8364297

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

April 11, 2023

THIS IS TO CERTIFY THAT ANNEXED IS A TRUE COPY FROM THE RECORDS OF THIS OFFICE OF THE FILE WRAPPER AND CONTENTS OF:

APPLICATION NUMBER: ***13/599,647***
FILING DATE: ***August 30, 2012***
PATENT NUMBER: ***10032171***
ISSUE DATE: ***July 24, 2018***

UNITED STATES PATENT AND TRADEMARK OFFICE · DEPARTMENT OF COMMERCE

Certified by

Kathi

Performing the Functions and Duties of the
Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

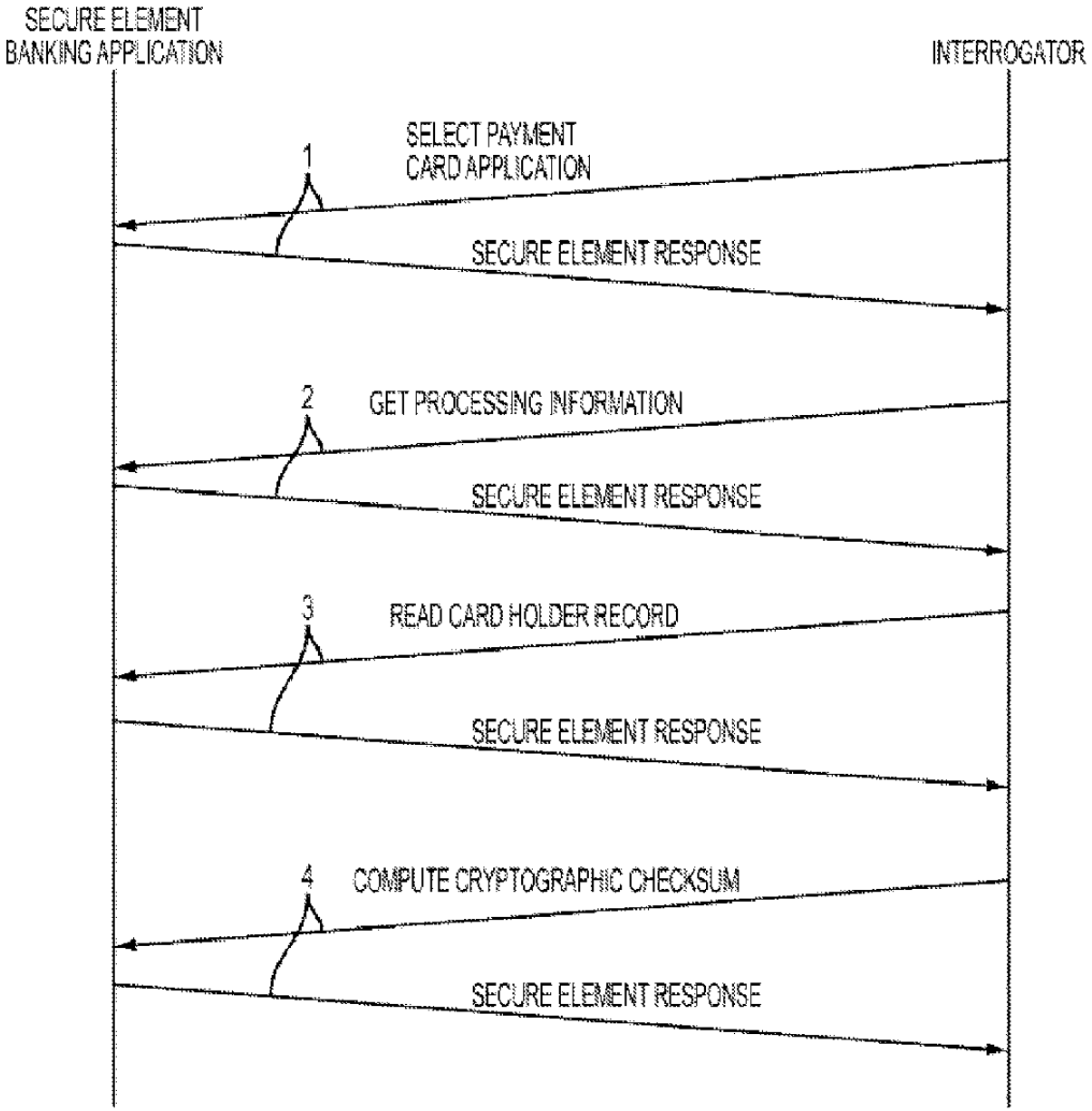

SECURE ELEMENT
BANKING APPLICATION
INTERROGATOR
1
SELECT PAYMENT
CARD APPLICATION
SECURE ELEMENT RESPONSE
2
GET PROCESSING INFORMATION
SECURE ELEMENT RESPONSE
3
READ CARD HOLDER RECORD
SECURE ELEMENT RESPONSE
4
COMPUTE CRYPTOGRAPHIC CHECKSUM
SECURE ELEMENT RESPONSE

FIG. 1

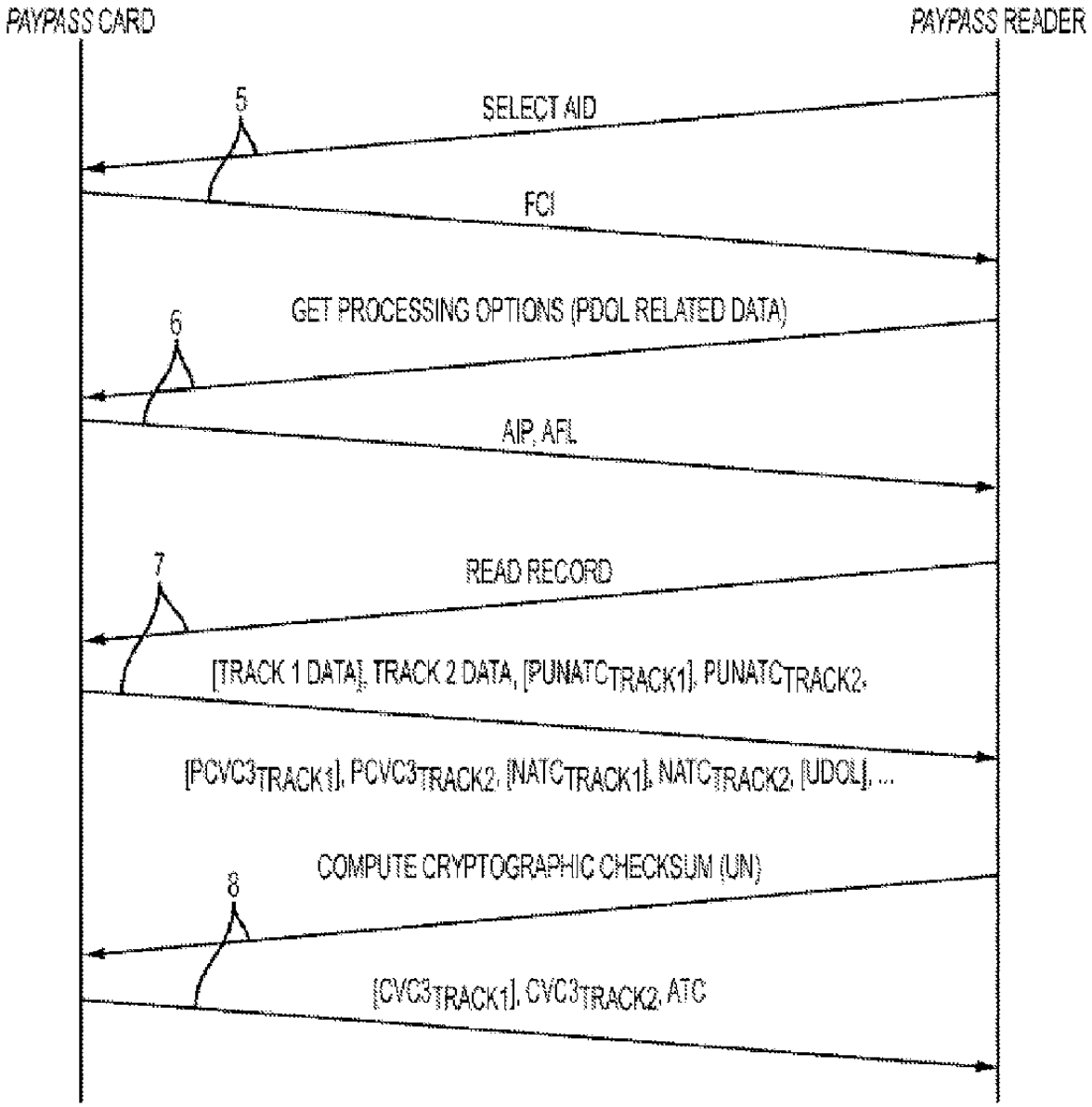

PAYPASS CARD
PAYPASS READER
5
SELECT AID
FCI
GET PROCESSING OPTIONS (PDOL RELATED DATA)
6
AIP, AFL
7
READ RECORD
[TRACK 1 DATA], TRACK 2 DATA, [PUNATC$_{TRACK1}$], PUNATC$_{TRACK2}$,
[PCVC3$_{TRACK1}$], PCVC3$_{TRACK2}$, [NATC$_{TRACK1}$], NATC$_{TRACK2}$, [UDOL], ...
COMPUTE CRYPTOGRAPHIC CHECKSUM (UN)
8
[CVC3$_{TRACK1}$], CVC3$_{TRACK2}$, ATC

FIG. 2

9
```
nUN:            3
UN:             00 00 08 99
ATC:            00 5E
CVC3TRACK1:     2 LEAST SIGNIFICANT BYTES OF
                    DES3(KDCVC3) [77 80 00 00 08 99 00 5E]
CVC3TRACK1:     FB C7
CVC3TRACK2:     2 LEAST SIGNIFICANT BYTES OF
                    DES3(KDCVC3) [99 D3 00 00 08 99 00 5E]
CVC3TRACK2:     B8 92
```

- SELECT PPSE COMMAND

10
```
>CARD:  00 A4 04 00 0E 32 50 41 59 2E 53 59 53 2E 44 44
        46 30 31 00
CARD>:  6F 23 84 0E 32 50 41 59 2E 53 59 53 2E 44 44 46
        30 31 A5 11 BF 0C 0E 61 0C 4F 07 A0 00 00 00 04
        10 10 87 01 01 90 00
```

- SELECT AID COMMAND

11
```
>CARD:  00 A4 04 00 07 A0 00 00 00 04 10 10 00
CARD>:  6F 17 84 07 A0 00 00 00 04 10 10 A5 0C 50 0A 4D
        61 73 74 65 72 43 61 72 64 90 00
```

- GET PROCESSING OPTIONS COMMAND

12
```
>CARD:  80 A8 00 00 02 83 00 00
CARD>:  77 0A 82 02 00 00 94 04 08 01 01 00 90 00
```

- READ RECORD COMMAND

13
```
>CARD:  00 B2 01 0C 00
CARD>:  70 7F 9F 6C 02 00 01 56 3E 42 35 34 31 33 31 32
        33 34 35 36 37 38 34 38 30 30 5E 53 55 50 50 4C
        49 45 44 2F 4E 4F 54 5E 30 39 30 36 31 30 31 33
        33 30 30 30 33 33 33 30 30 30 32 32 32 32 32 30
        30 30 31 31 31 31 30 9F 64 01 03 9F 62 06 00 00
        00 38 00 00 9F 63 06 00 00 00 00 E0 E0 9F 65 02
        00 0E 9F 66 02 0E 70 9F 6B 13 54 13 12 34 56 78
        48 00 D0 90 61 01 90 00 99 00 00 00 0F 9F 67 01
        03 90 00
```

- COMPUTE CRYPTOGRAPHIC CHECKSUM COMMAND

14
```
>CARD:  80 2A 8E 80 04 00 00 08 99 00
CARD>:  77 0F 9F 61 02 B8 92 9F 60 02 FB C7 9F 36 02 00
        5E 90 00
```

FIG. 3

THE *PAYPASS* READER GENERATES THE TRACK 2 DATA TO BE INCLUDED IN THE AUTHORIZATION MESSAGE AS FOLLOWS:

15

$CVC3_{TRACK2}$ IN BASE 10:47250
ATC IN BASE 10: 94

=> TRACK 2 DATA:	54	13	12	34	56	78	48	00	D0	90	61	01
	9	**094**	99	**899**	**250**			**3**	F			
		↑↑↑		↑↑↑	↑↑↑			↑				
		ATC		UN	$CVC3_{TRACK2}$			nUN				

THE *PAYPASS* READER GENERATES THE TRACK 1 DATA TO BE INCLUDED IN THE AUTHORIZATION MESSAGE AS FOLLOWS:

16

$CVC3_{TRACK1}$ IN BASE 10:64455
ATC IN BASE 10: 94

=> TRACK 1 DATA:	42	35	34	31	33	31	32	33	34	35	36	37	38	34	38	30
	30	5E	53	55	50	50	4C	49	45	44	2F	4E	4F	54	5E	30
	39	30	36	31	30	31	33	33	34	35	35	33	33	33	30	39
	34	32	32	32	32	32	38	39	39	31	31	31	31	33		

ASCII DUMP: B5413123456784800^SUPPLIED/NOT^0906101
3345533309422222899111113
↑↑↑ ↑↑↑ ↑↑↑ ↑
$CVC3_{TRACK1}$ ATC UN nUN

FIG. 4

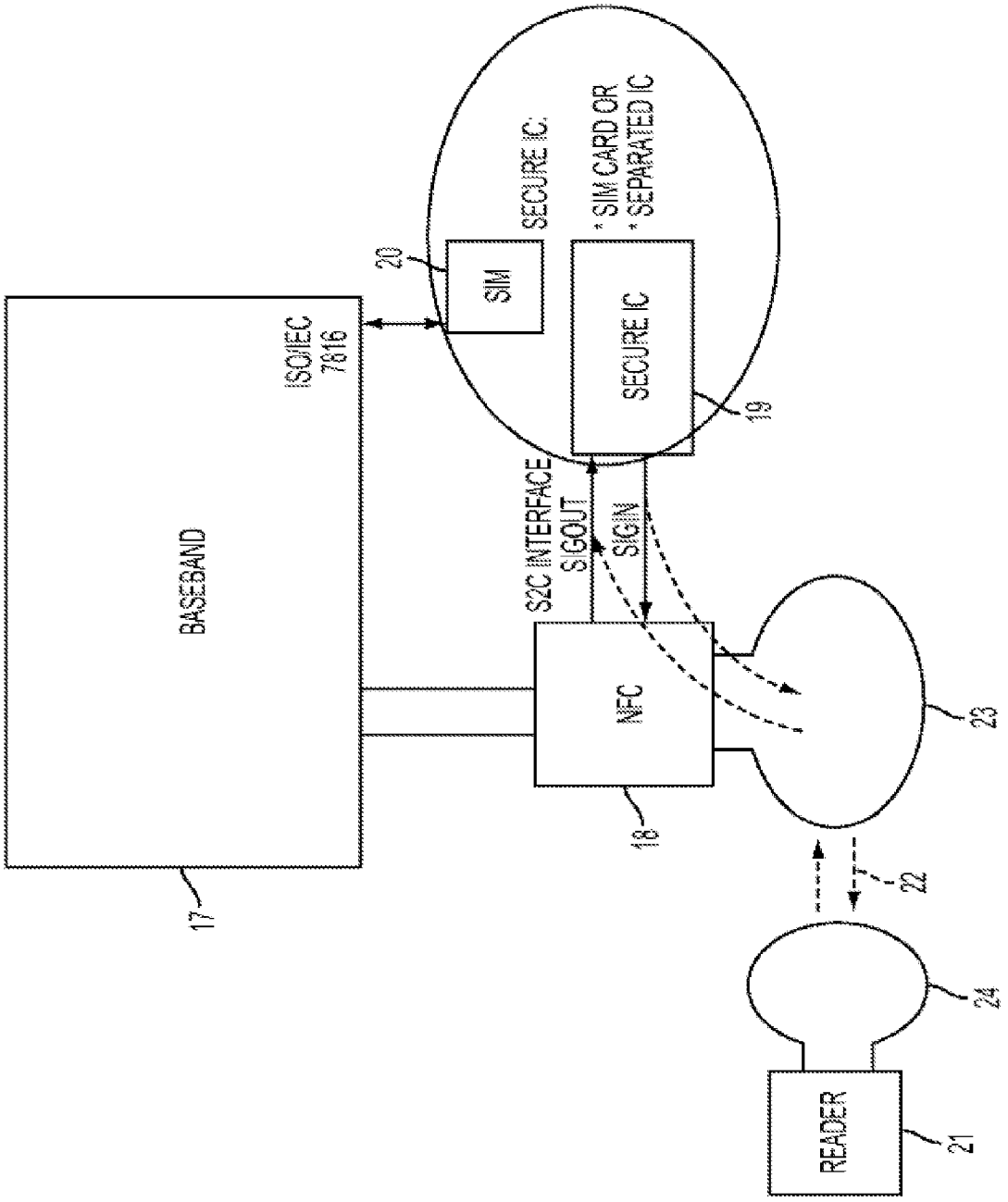

BASEBAND
17
ISO/IEC 7816
20
SIM
SECURE IC
* SIM CARD OR
* SEPARATED IC
SECURE IC
19
S2C INTERFACE
SIGOUT
SIGIN
NFC
18
23
22
24
READER
21

FIG. 5

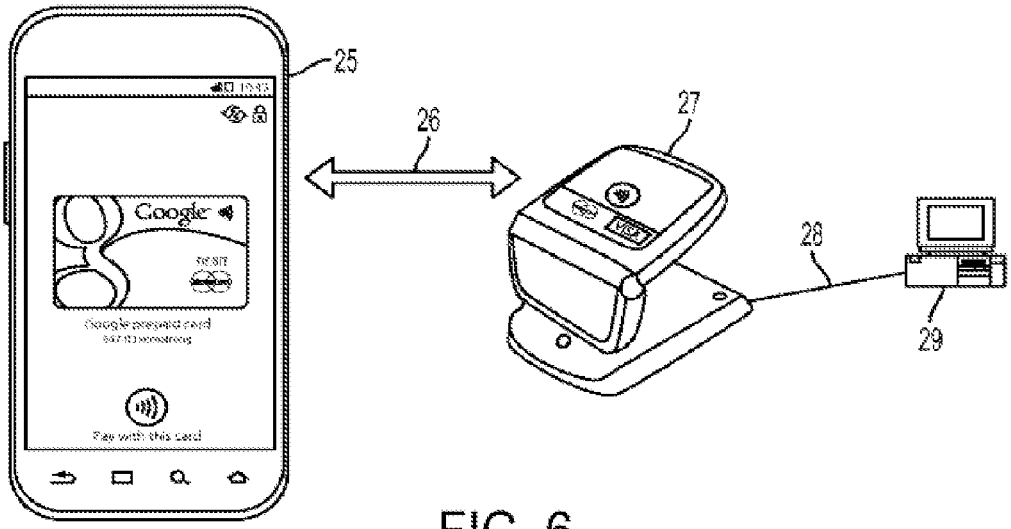

25
26
27
28
29
Google

FIG. 6

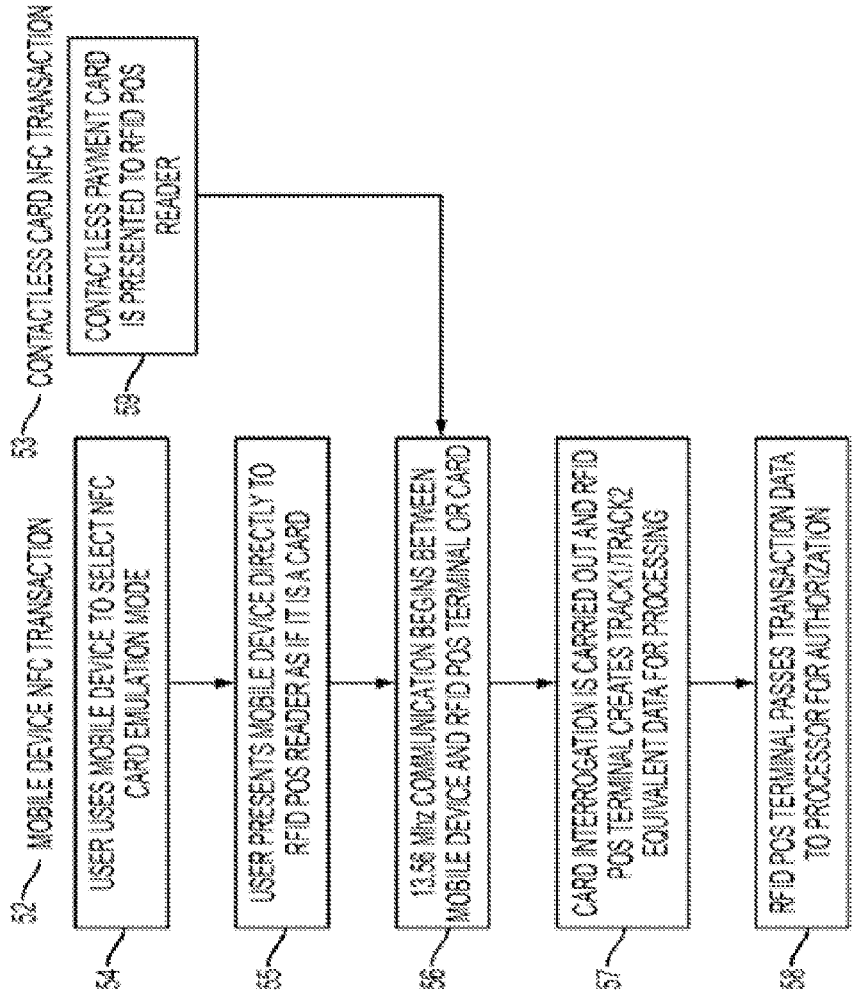

MOBILE DEVICE NFC TRANSACTION
52
USER USES MOBILE DEVICE TO SELECT NFC CARD EMULATION MODE
54
USER PRESENTS MOBILE DEVICE DIRECTLY TO RFID POS READER AS IF IT IS A CARD
55
13.56 Mhz COMMUNICATION BEGINS BETWEEN MOBILE DEVICE AND RFID POS TERMINAL OR CARD
56
CARD INTERROGATION IS CARRIED OUT AND RFID POS TERMINAL CREATES TRACK1/TRACK2 EQUIVALENT DATA FOR PROCESSING
57
RFID POS TERMINAL PASSES TRANSACTION DATA TO PROCESSOR FOR AUTHORIZATION
58
CONTACTLESS CARD NFC TRANSACTION
53
CONTACTLESS PAYMENT CARD IS PRESENTED TO RFID POS READER
59

FIG. 7

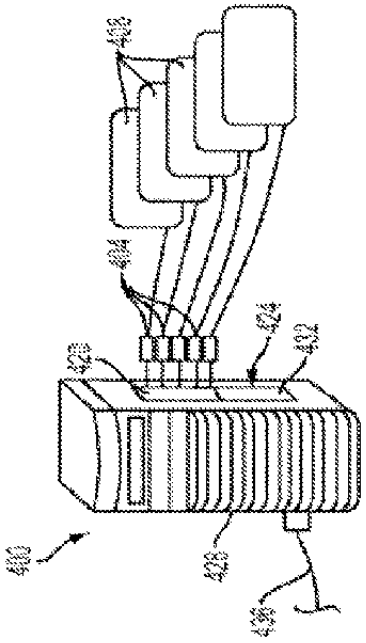


FIG. 8

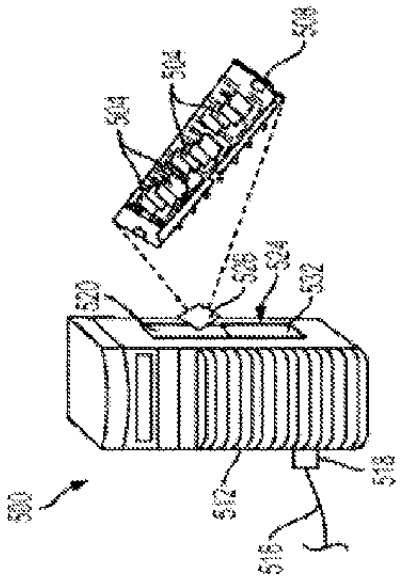


FIG. 9

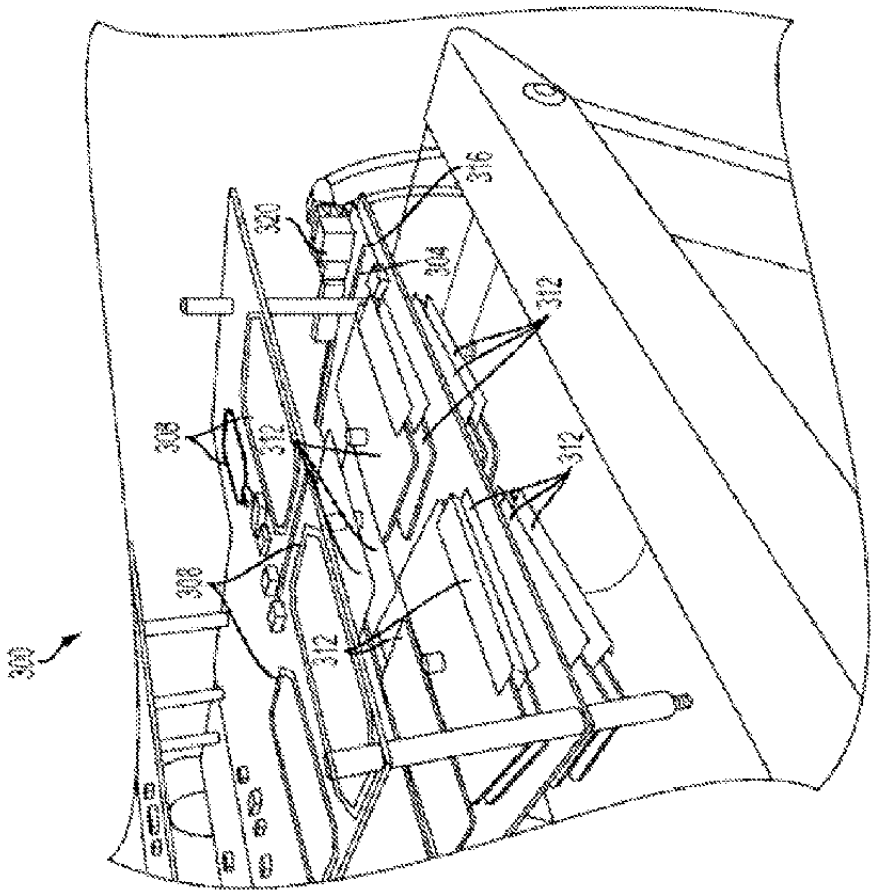


FIG. 10

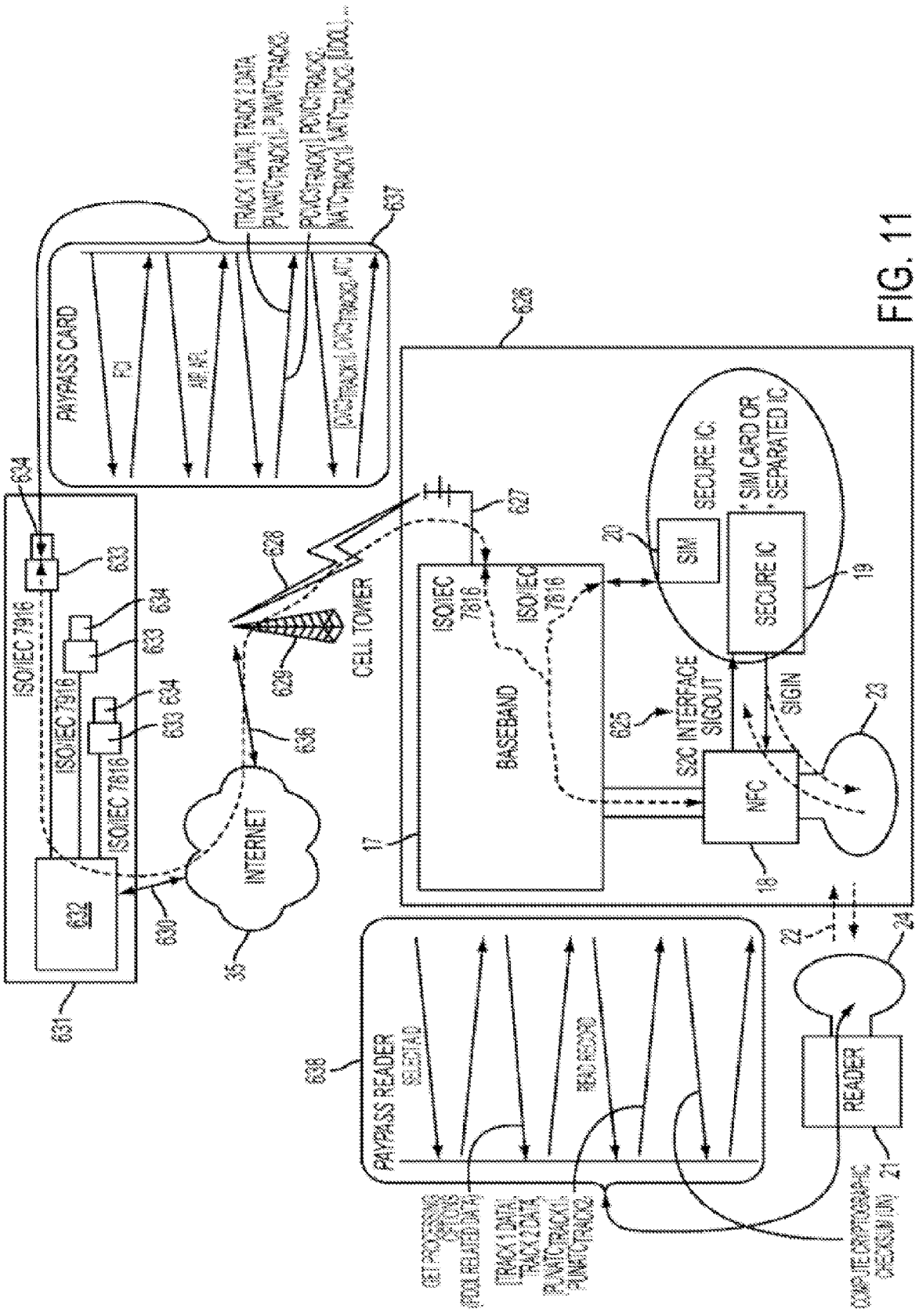

PAYPASS CARD
EDI
ABC INC.
TRACK 1 DATA, TRACK 2 DATA
PUNCTRACK1, PUNCTRACK2
PCVCTRACK1, PCVCTRACK2
MVTCTRACK1, MVTCTRACK2 (DDA, ...
DATA(TRACK1, DATA(TRACK2, ETC.
637
634
633
ISO/IEC 7816
632
630
631
INTERNET
635
636
628
CELL TOWER
627
626
BASEBAND
17
ISO/IEC 7816
ISO/IEC 7816
SIM
SECURE IC
SIM CARD OR SEPARATED IC
SECURE IC
20
19
625
S2C INTERFACE
SIGOUT
SIGIN
NFC
18
23
22
24
PAYPASS READER
SELECT AID
READ RECORD
GET PROCESSING OPTIONS (PDOL RELATED DATA)
TRACK 1 DATA, TRACK 2 DATA, PUNCTRACK1, PUNCTRACK2
COMPUTE CRYPTOGRAPHIC CHECKSUM (UN)
READER
21

FIG. 11

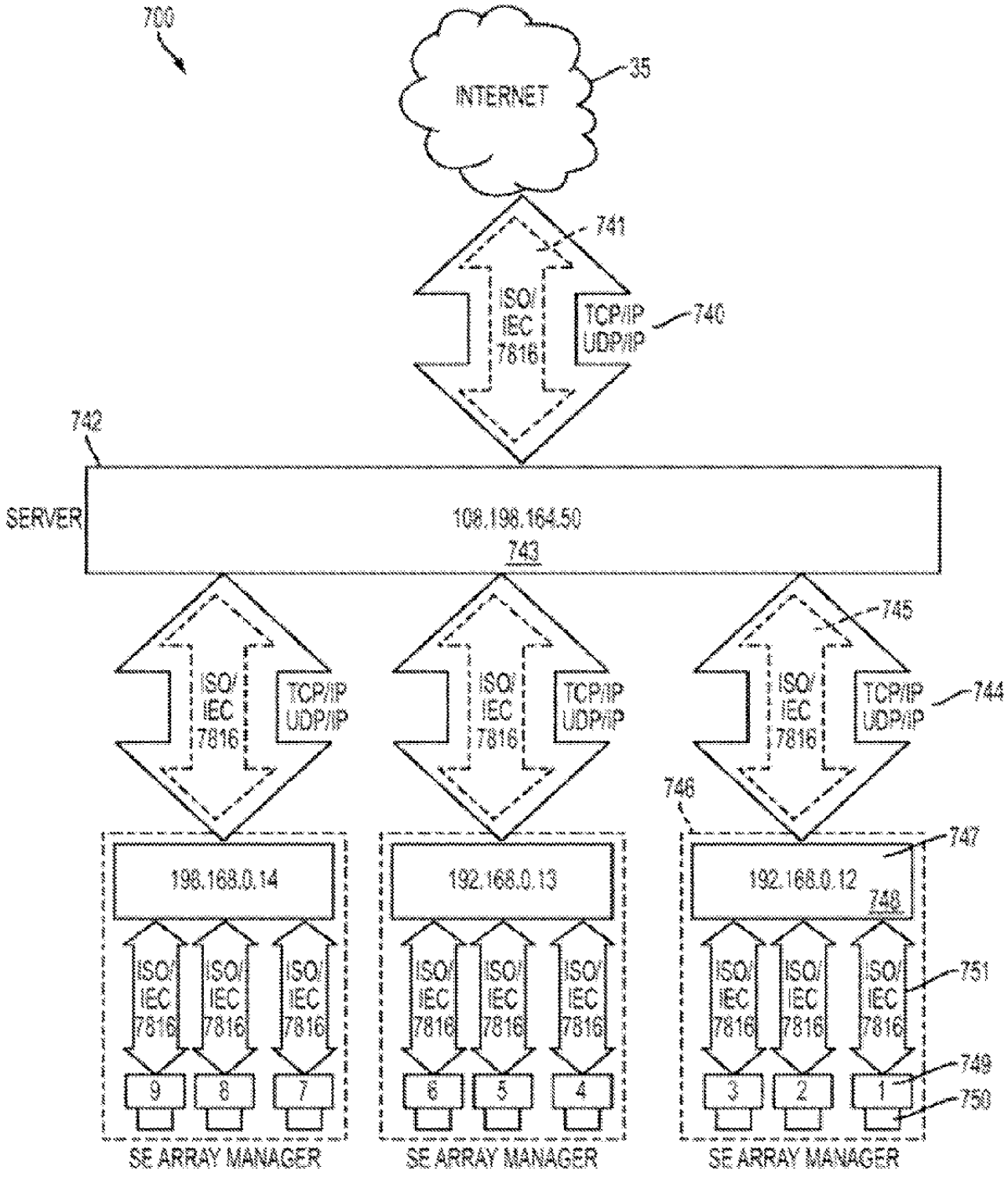

700
INTERNET
35
741
ISO/IEC 7816
TCP/IP UDP/IP
740
742
SERVER
108.198.164.50
743
745
744
746
747
192.168.0.14
192.168.0.13
192.168.0.12
748
751
749
750
9
8
7
6
5
4
3
2
1
SE ARRAY MANAGER
SE ARRAY MANAGER
SE ARRAY MANAGER

FIG. 12

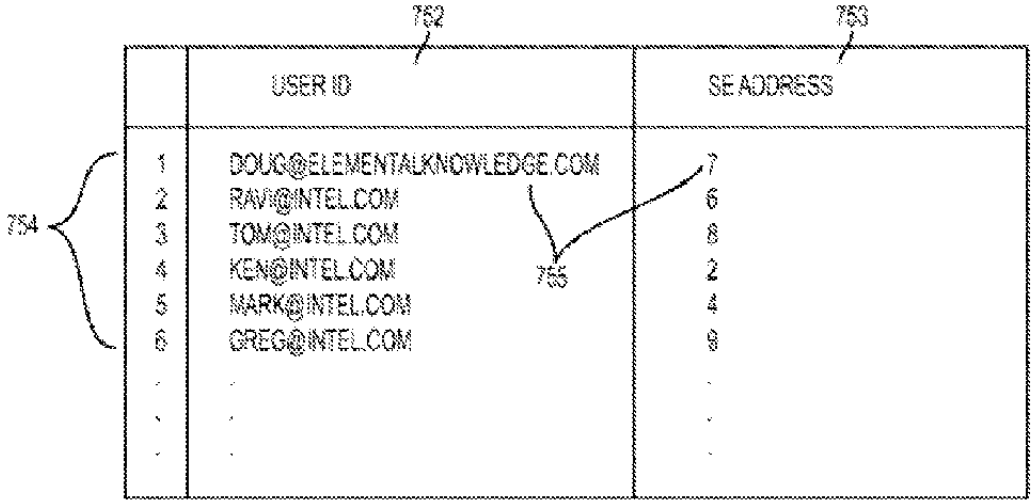

752
753
USER ID
SE ADDRESS
754
1 DOUG@ELEMENTALKNOWLEDGE.COM 7
2 RAVI@INTEL.COM 6
3 TOM@INTEL.COM 8
4 KEN@INTEL.COM 2
5 MARK@INTEL.COM 4
6 GREG@INTEL.COM 9
755

FIG. 13

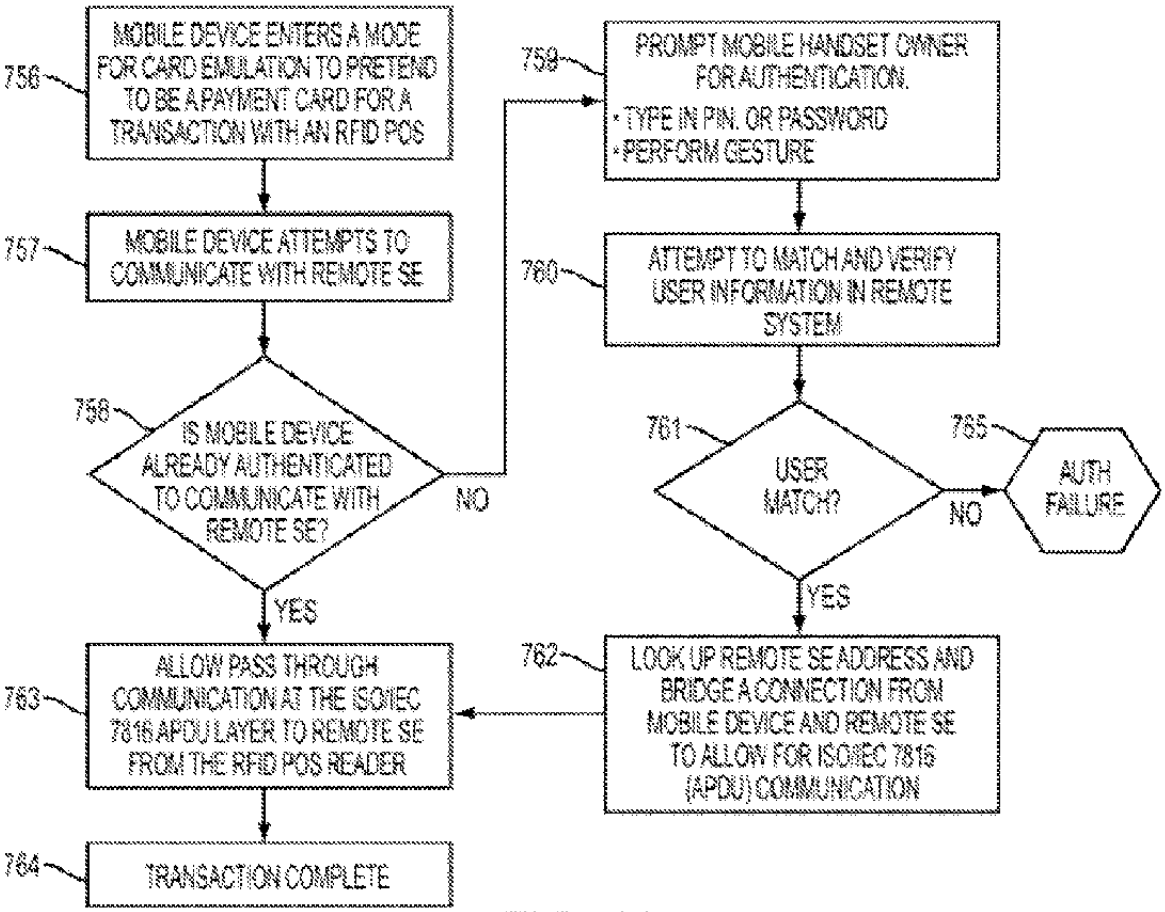

756
MOBILE DEVICE ENTERS A MODE FOR CARD EMULATION TO PRETEND TO BE A PAYMENT CARD FOR A TRANSACTION WITH AN RFID POS
757
MOBILE DEVICE ATTEMPTS TO COMMUNICATE WITH REMOTE SE
758
IS MOBILE DEVICE ALREADY AUTHENTICATED TO COMMUNICATE WITH REMOTE SE?
NO
YES
759
PROMPT MOBILE HANDSET OWNER FOR AUTHENTICATION.
• TYPE IN PIN, OR PASSWORD
• PERFORM GESTURE
760
ATTEMPT TO MATCH AND VERIFY USER INFORMATION IN REMOTE SYSTEM
761
USER MATCH?
NO
765
AUTH FAILURE
YES
762
LOOK UP REMOTE SE ADDRESS AND BRIDGE A CONNECTION FROM MOBILE DEVICE AND REMOTE SE TO ALLOW FOR ISO/IEC 7816 (APDU) COMMUNICATION
763
ALLOW PASS THROUGH COMMUNICATION AT THE ISO/IEC 7816 APDU LAYER TO REMOTE SE FROM THE RFID POS READER
764
TRANSACTION COMPLETE

FIG. 14

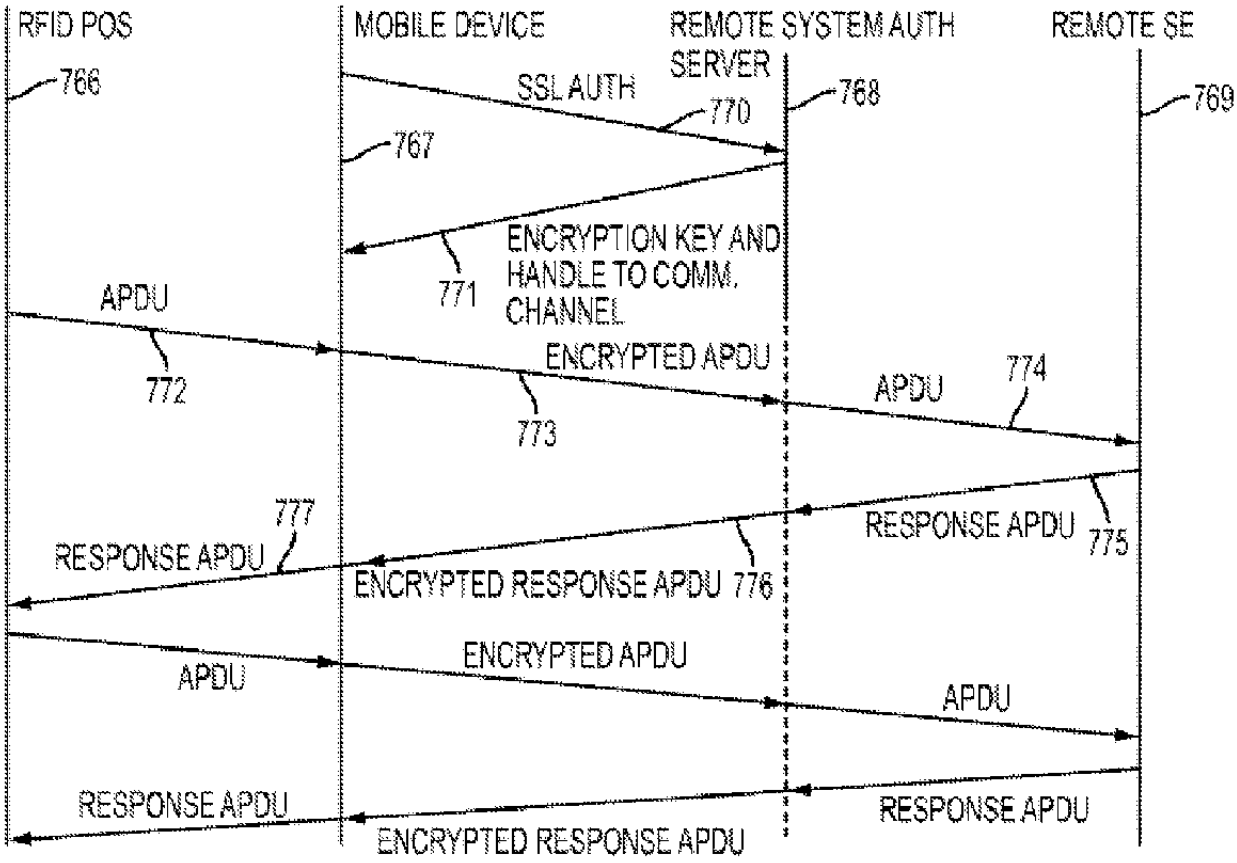

RFID POS
MOBILE DEVICE
REMOTE SYSTEM AUTH SERVER
REMOTE SE
766
SSL AUTH
770
768
769
767
ENCRYPTION KEY AND HANDLE TO COMM. CHANNEL
771
APDU
772
ENCRYPTED APDU
773
APDU
774
RESPONSE APDU
775
777
RESPONSE APDU
ENCRYPTED RESPONSE APDU
776
APDU
ENCRYPTED APDU
APDU
RESPONSE APDU
RESPONSE APDU
ENCRYPTED RESPONSE APDU

FIG. 15

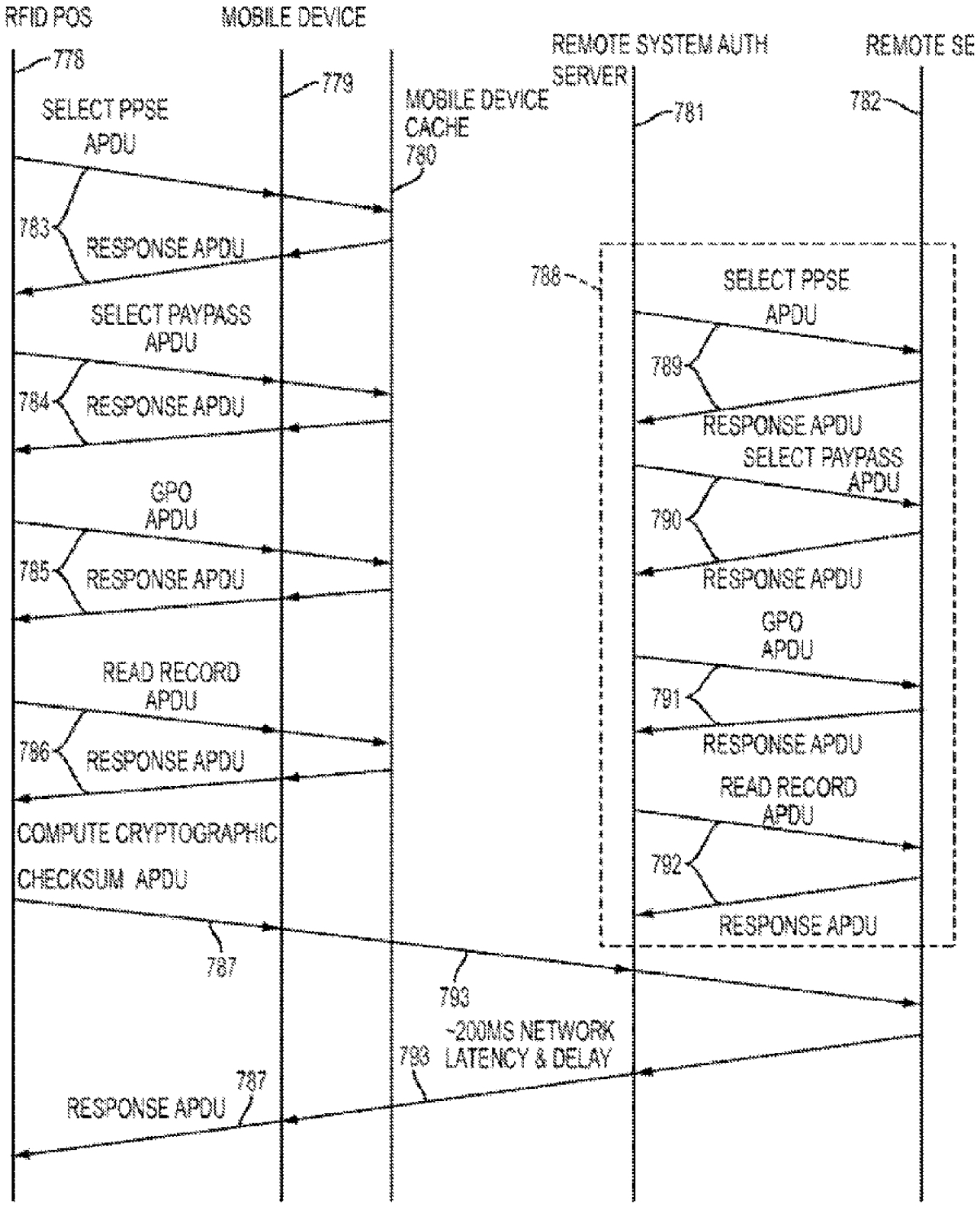

RFID POS
MOBILE DEVICE
REMOTE SYSTEM AUTH SERVER
REMOTE SE
776
779
MOBILE DEVICE CACHE 760
781
782
SELECT PPSE APDU
783
RESPONSE APDU
788
SELECT PPSE APDU
789
RESPONSE APDU
SELECT PAYPASS APDU
784
RESPONSE APDU
SELECT PAYPASS APDU
790
RESPONSE APDU
GPO APDU
785
RESPONSE APDU
GPO APDU
791
RESPONSE APDU
READ RECORD APDU
786
RESPONSE APDU
READ RECORD APDU
792
RESPONSE APDU
COMPUTE CRYPTOGRAPHIC CHECKSUM APDU
787
793
~200MS NETWORK LATENCY & DELAY
793
787
RESPONSE APDU

FIG. 16

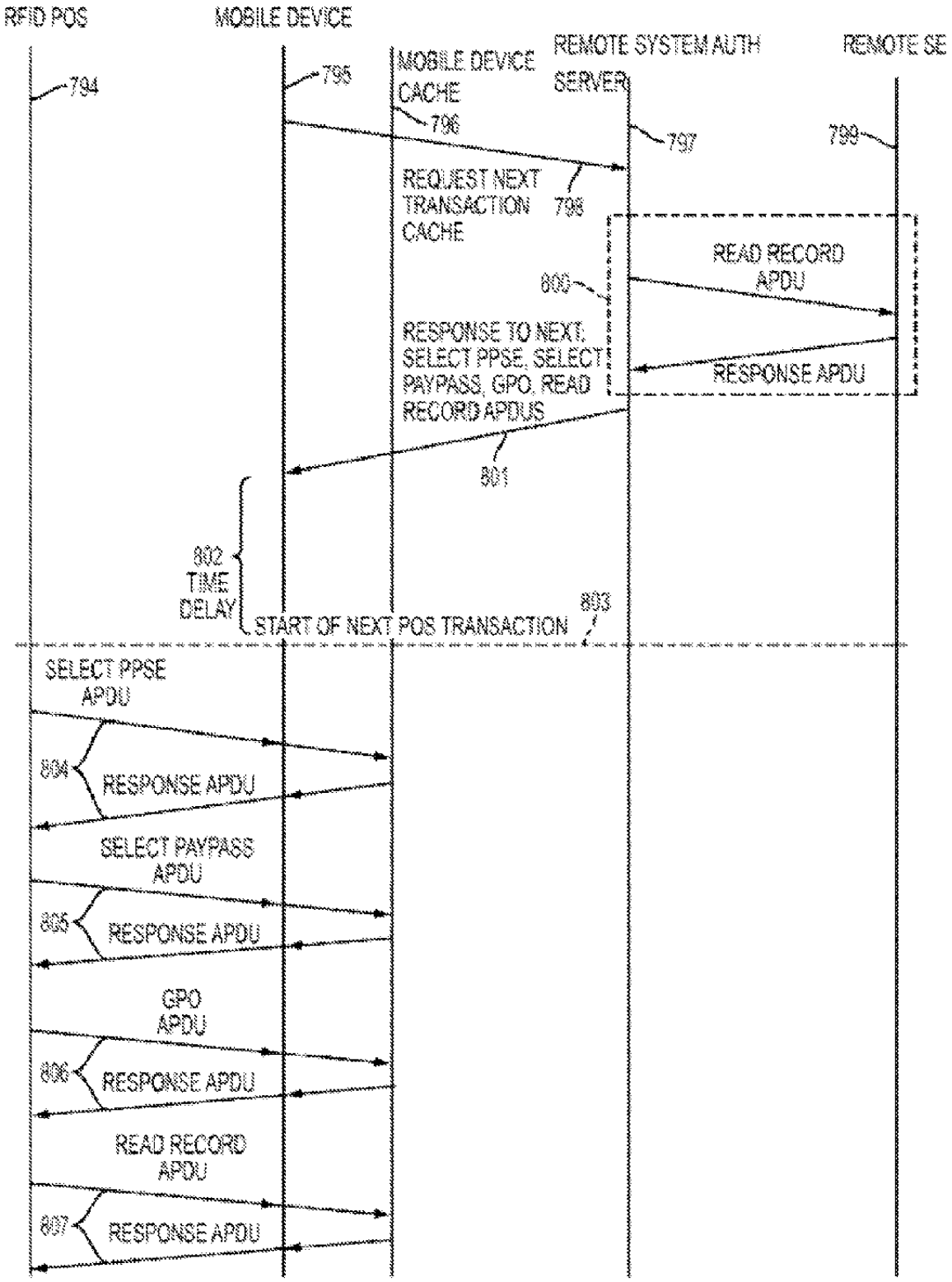

RFID POS
MOBILE DEVICE
MOBILE DEVICE CACHE
REMOTE SYSTEM AUTH SERVER
REMOTE SE
794
795
796
797
798
REQUEST NEXT TRANSACTION CACHE
796
READ RECORD APDU
800
RESPONSE TO NEXT SELECT PPSE, SELECT PAYPASS, GPO, READ RECORD APDUS
RESPONSE APDU
801
802 TIME DELAY
803
START OF NEXT POS TRANSACTION
SELECT PPSE APDU
804
RESPONSE APDU
SELECT PAYPASS APDU
805
RESPONSE APDU
GPO APDU
806
RESPONSE APDU
READ RECORD APDU
807
RESPONSE APDU

FIG. 17

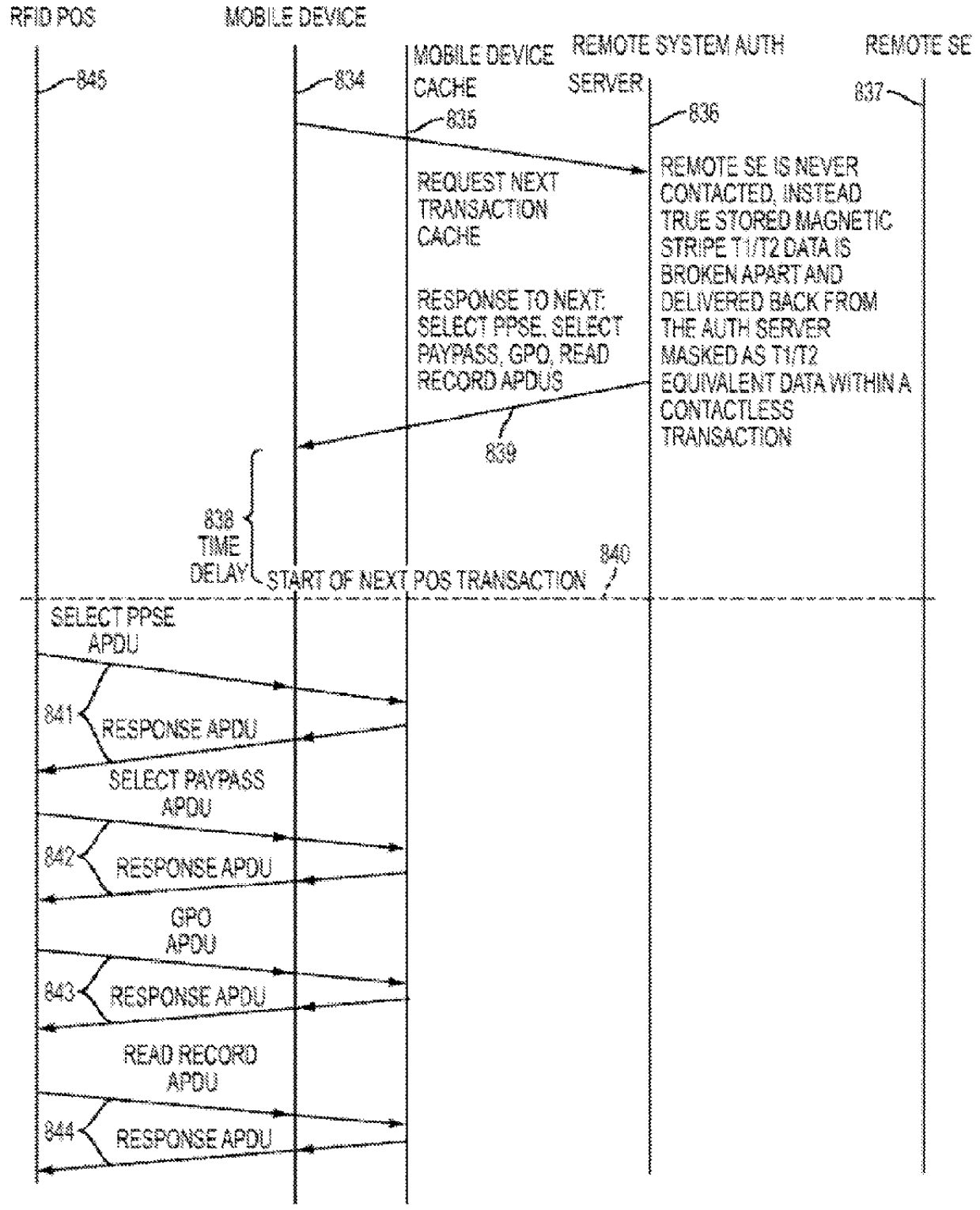

RFID POS
MOBILE DEVICE
MOBILE DEVICE CACHE
REMOTE SYSTEM AUTH SERVER
REMOTE SE
845
834
835
836
837
REQUEST NEXT TRANSACTION CACHE
REMOTE SE IS NEVER CONTACTED, INSTEAD TRUE STORED MAGNETIC STRIPE T1/T2 DATA IS BROKEN APART AND DELIVERED BACK FROM THE AUTH SERVER MASKED AS T1/T2 EQUIVALENT DATA WITHIN A CONTACTLESS TRANSACTION
RESPONSE TO NEXT: SELECT PPSE, SELECT PAYPASS, GPO, READ RECORD APDUS
839
838 TIME DELAY
840
START OF NEXT POS TRANSACTION
SELECT PPSE APDU
841
RESPONSE APDU
SELECT PAYPASS APDU
842
RESPONSE APDU
GPO APDU
843
RESPONSE APDU
READ RECORD APDU
844
RESPONSE APDU

FIG. 18

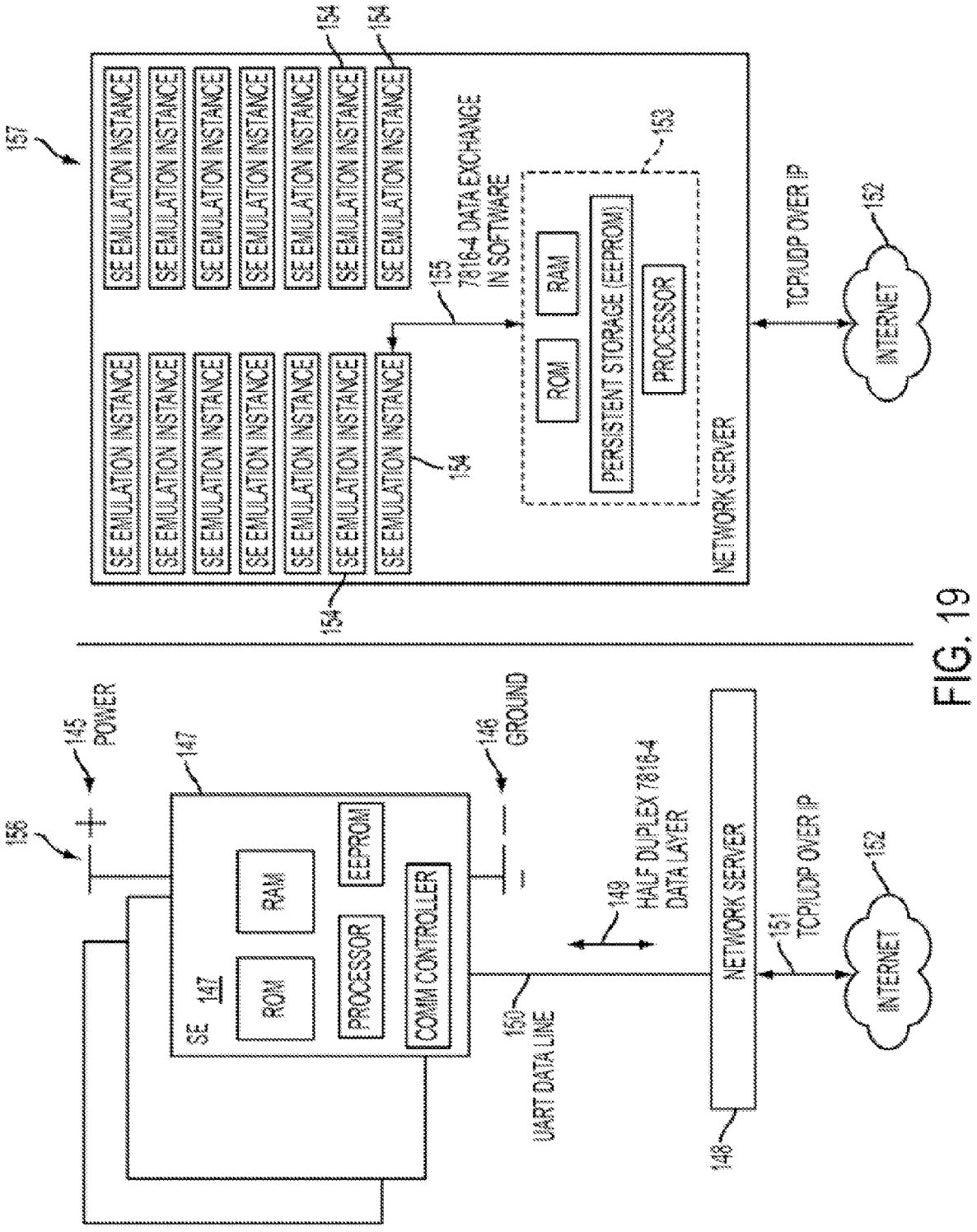

157
SE EMULATION INSTANCE
154
155
7816-4 DATA EXCHANGE IN SOFTWARE
ROM
RAM
PROCESSOR
PERSISTENT STORAGE (EEPROM)
153
NETWORK SERVER
TCP/UDP OVER IP
INTERNET
152
156
145
POWER
147
SE 147
ROM
RAM
PROCESSOR
EEPROM
COMM CONTROLLER
146
GROUND
149
HALF DUPLEX 7816-4 DATA LAYER
150
UART DATA LINE
148
NETWORK SERVER
151
TCP/UDP OVER IP
INTERNET
152

FIG. 19

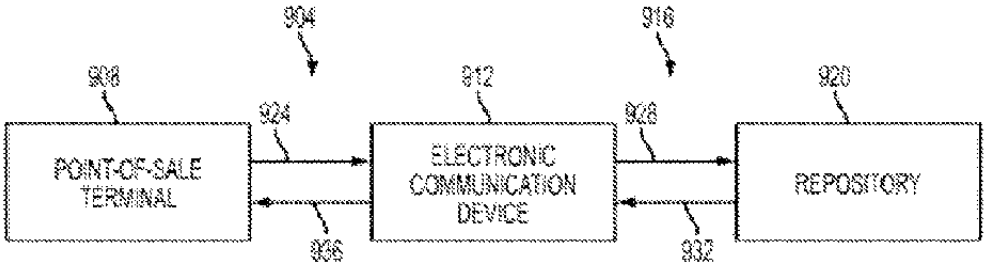

904
916
908
912
920
924
926
POINT-OF-SALE TERMINAL
ELECTRONIC COMMUNICATION DEVICE
REPOSITORY
936
932

FIG. 20

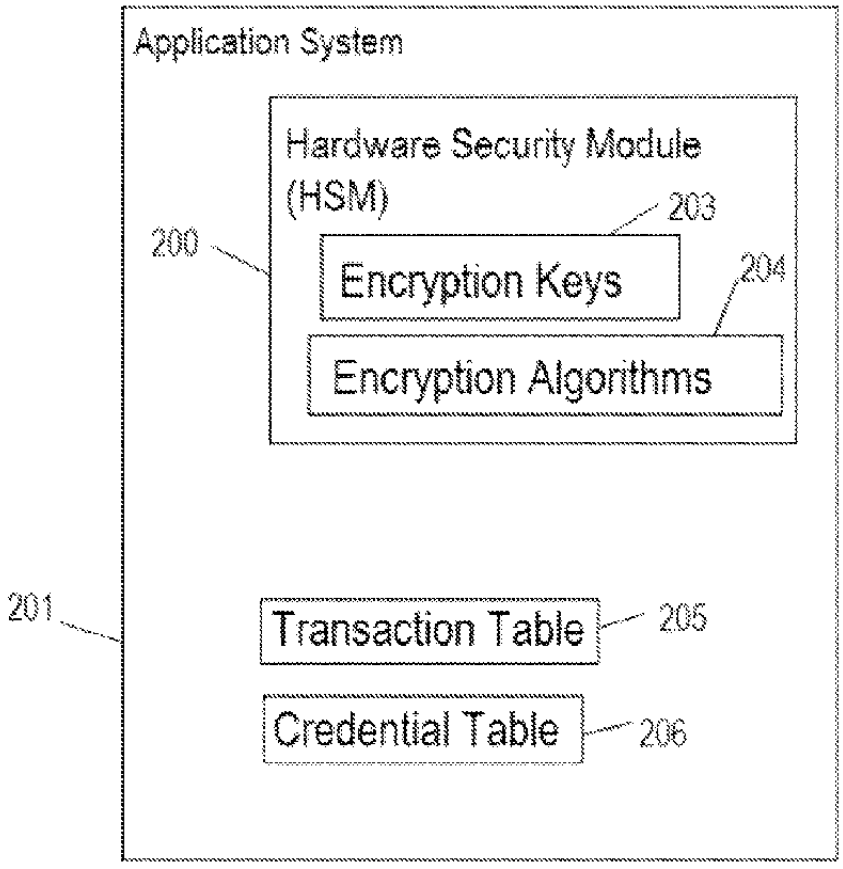

Application System
Hardware Security Module (HSM)
200
203
Encryption Keys
204
Encryption Algorithms
201
Transaction Table
205
Credential Table
206

Fig. 21

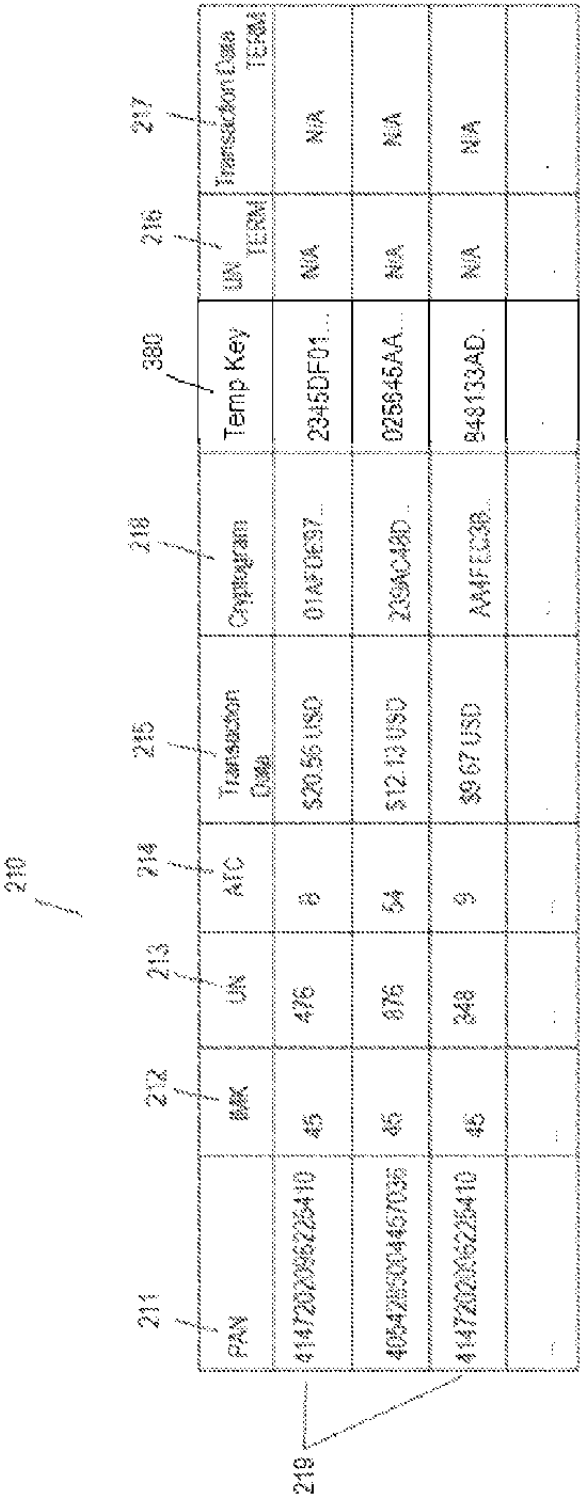

210
211
212
213
214
215
216
380
217
219
PAN
IMK
UN
ATC
Transaction Data
Cryptogram
Temp Key
UN TERM
Transaction Data TERM
4147202X0622264410
45
476
8
$20.56 USD
01AF0E37...
2345DF01...
N/A
N/A
4042EC0144C7036
45
876
54
$12.13 USD
209AC48D...
025645AA...
N/A
N/A
4147202X0622264410
45
348
9
$9.67 USD
AAFF1538...
948133AD...
N/A
N/A

Fig. 22

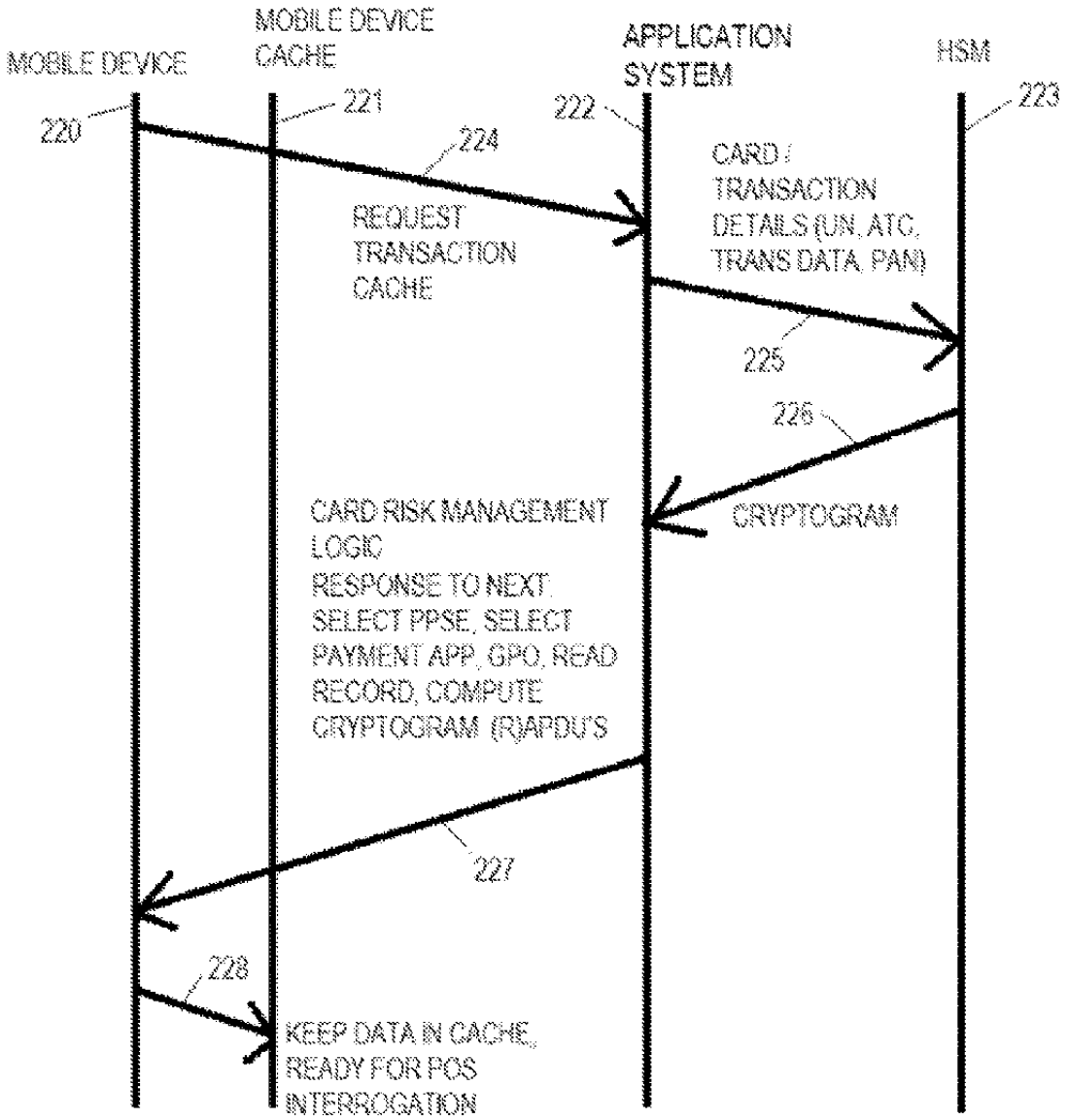

MOBILE DEVICE
MOBILE DEVICE CACHE
APPLICATION SYSTEM
HSM
220
221
222
223
224
REQUEST TRANSACTION CACHE
CARD / TRANSACTION DETAILS (UN, ATC, TRANS DATA, PAN)
225
226
CRYPTOGRAM
CARD RISK MANAGEMENT LOGIC
RESPONSE TO NEXT SELECT PPSE, SELECT PAYMENT APP, GPO, READ RECORD, COMPUTE CRYPTOGRAM (R)APDU'S
227
228
KEEP DATA IN CACHE, READY FOR POS INTERROGATION

Fig. 23

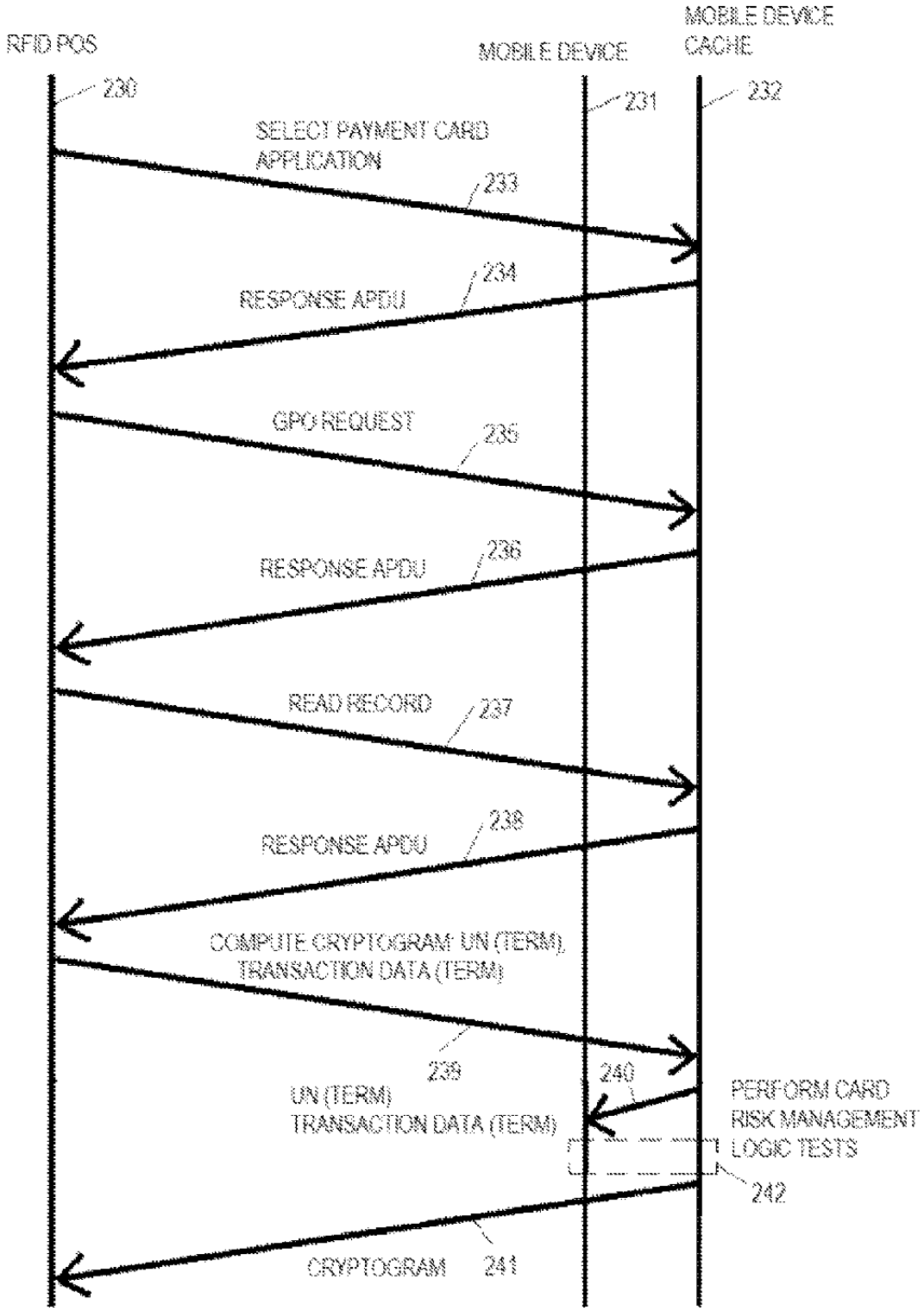

RFID POS
MOBILE DEVICE
MOBILE DEVICE CACHE
230
231
232
SELECT PAYMENT CARD APPLICATION
233
RESPONSE APDU
234
GPO REQUEST
235
RESPONSE APDU
236
READ RECORD
237
RESPONSE APDU
238
COMPUTE CRYPTOGRAM UN (TERM), TRANSACTION DATA (TERM)
239
UN (TERM)
TRANSACTION DATA (TERM)
240
PERFORM CARD RISK MANAGEMENT LOGIC TESTS
242
CRYPTOGRAM
241

Fig. 24

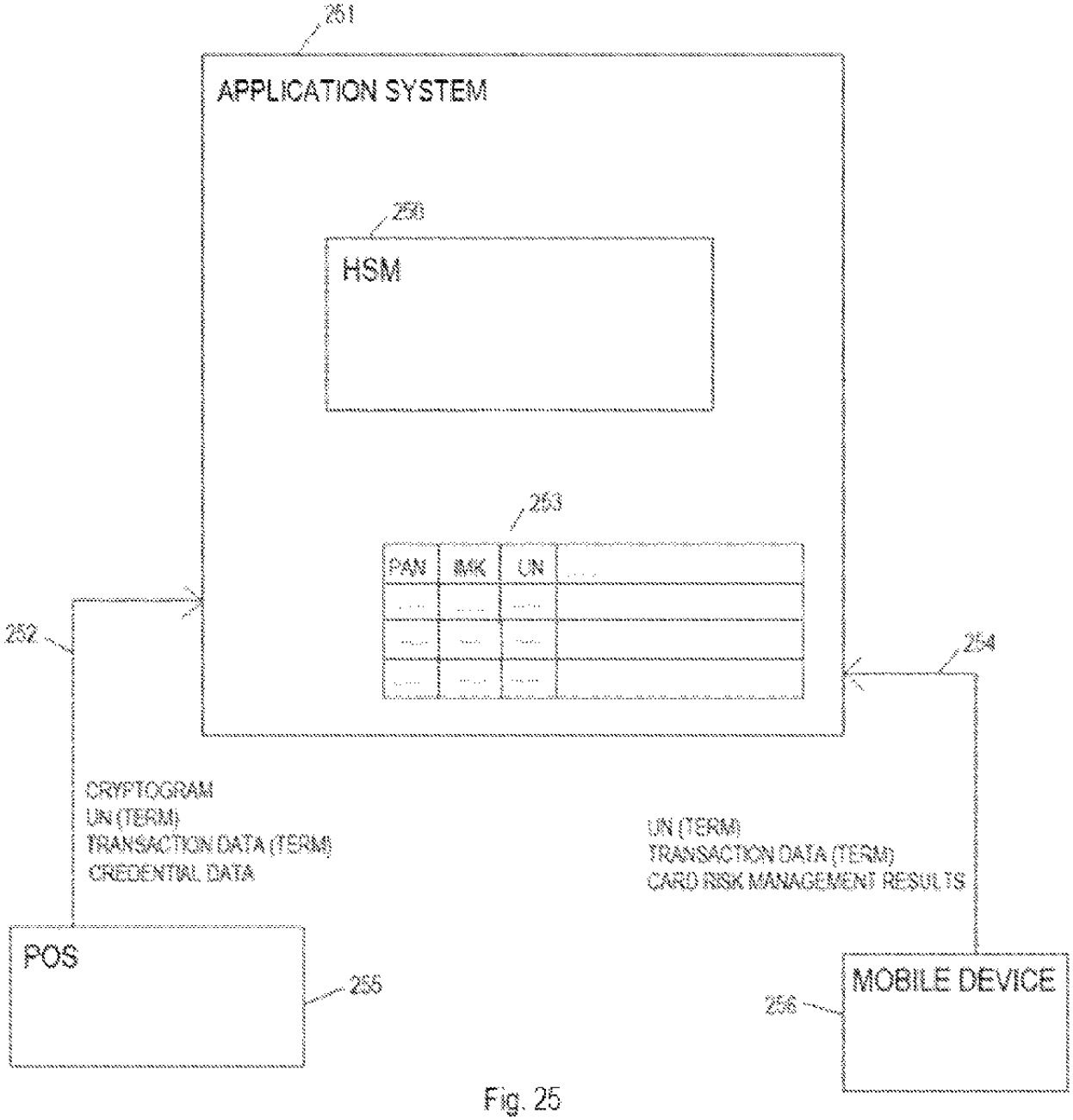

251
APPLICATION SYSTEM
250
HSM
253
PAN
IMK
UN
252
254
CRYPTOGRAM
UN (TERM)
TRANSACTION DATA (TERM)
CREDENTIAL DATA
UN (TERM)
TRANSACTION DATA (TERM)
CARD RISK MANAGEMENT RESULTS
POS
255
MOBILE DEVICE
256

Fig. 25

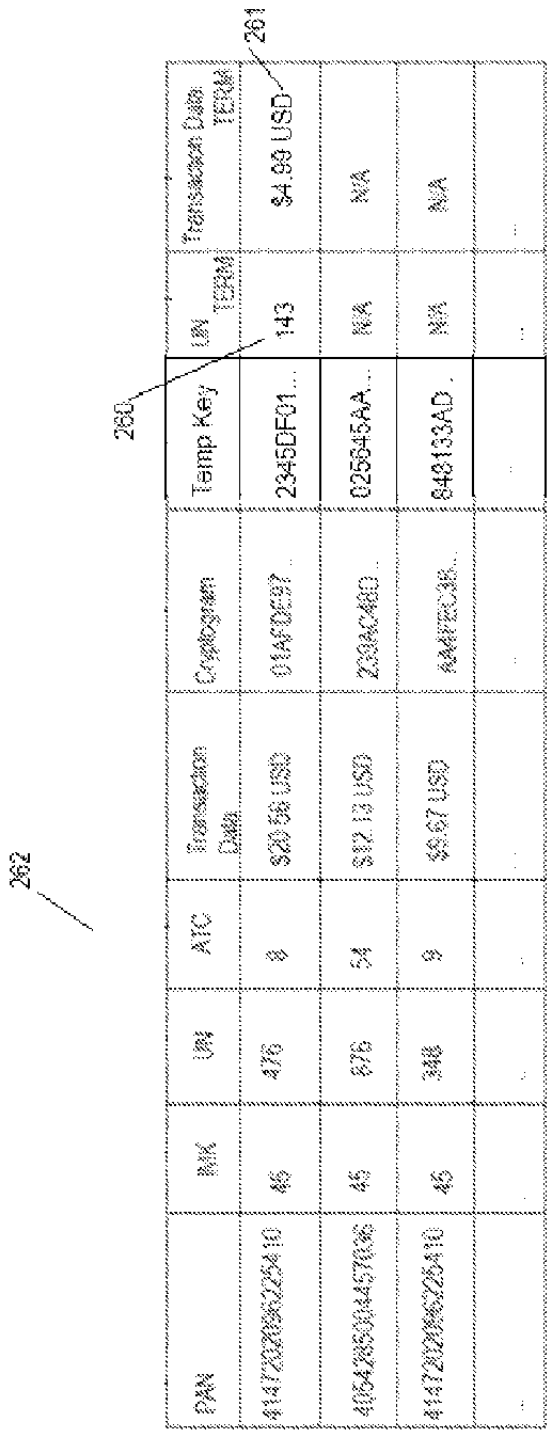

262
260
261
PAN
PAN
UN
ATC
Transaction Data
Cryptogram
Temp Key
UN TERM
Transaction Data TERM
4147208062264410
46
476
8
$20.56 USD
014F0E97...
2345DF01...
143
$4.99 USD
4064285004457066
46
676
54
$12.13 USD
Z33AC480...
025645AA...
N/A
N/A
4147208062264410
46
348
9
$9.67 USD
AAFFEC38...
848133AD...
N/A
N/A

Fig 26

Fig. 27

Mastercard, Ex1002, p. 23

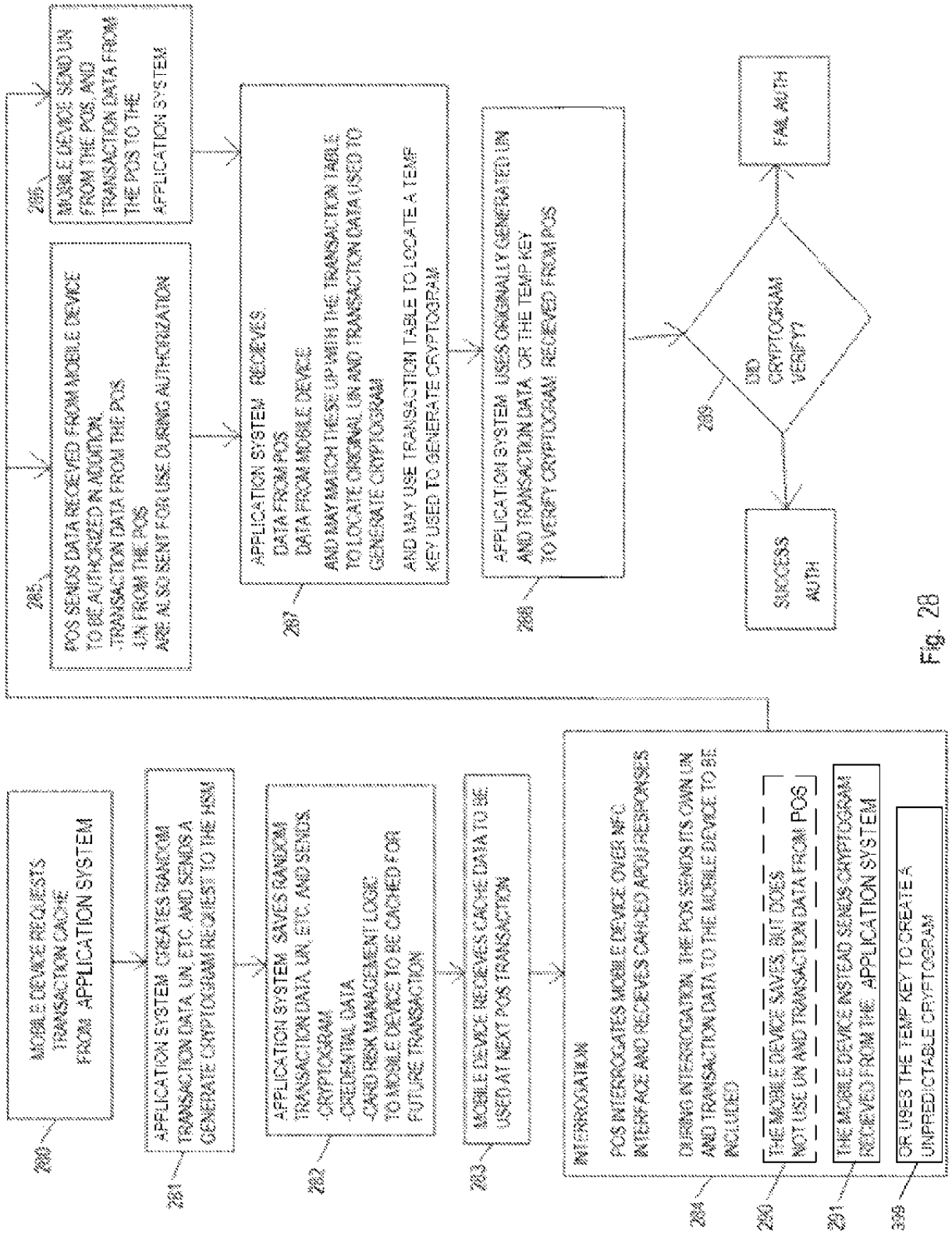

280
MOBILE DEVICE REQUESTS TRANSACTION CACHE FROM APPLICATION SYSTEM
281
APPLICATION SYSTEM CREATES RANDOM TRANSACTION DATA, UN, ETC. AND SENDS A GENERATE CRYPTOGRAM REQUEST TO THE HSM
282
APPLICATION SYSTEM SAVES RANDOM TRANSACTION DATA, UN, ETC. AND SENDS CRYPTOGRAM, CREDENTIAL DATA, CARD RISK MANAGEMENT LOGIC TO MOBILE DEVICE TO BE CACHED FOR FUTURE TRANSACTION
283
MOBILE DEVICE RETRIEVES CACHE DATA TO BE USED AT NEXT POS TRANSACTION
284
INTERROGATION
POS INTERROGATES MOBILE DEVICE OVER NFC INTERFACE AND RECEIVES CARDLET APDU RESPONSES
DURING INTERROGATION, THE POS SENDS ITS OWN UN AND TRANSACTION DATA TO THE MOBILE DEVICE TO BE INCLUDED
290
THE MOBILE DEVICE SAVES BUT DOES NOT USE UN AND TRANSACTION DATA FROM POS
291
THE MOBILE DEVICE INSTEAD SENDS CRYPTOGRAM RECEIVED FROM THE APPLICATION SYSTEM
309
OR USES THE TEMP KEY TO CREATE A UNPREDICTABLE CRYPTOGRAM
285
POS SENDS DATA RECEIVED FROM MOBILE DEVICE TO BE AUTHORIZED IN ADDITION, TRANSACTION DATA FROM THE POS, UN FROM THE POS ARE ALSO SENT FOR USE DURING AUTHORIZATION
286
MOBILE DEVICE SENDS UN FROM THE POS, AND TRANSACTION DATA FROM THE POS TO THE APPLICATION SYSTEM
287
APPLICATION SYSTEM RECEIVES DATA FROM POS DATA FROM MOBILE DEVICE AND MAY MATCH THESE UP WITH THE TRANSACTION TABLE TO LOCATE ORIGINAL UN AND TRANSACTION DATA USED TO GENERATE CRYPTOGRAM AND MAY USE TRANSACTION TABLE TO LOCATE A TEMP KEY USED TO GENERATE CRYPTOGRAM
288
APPLICATION SYSTEM USES ORIGINALLY GENERATED UN AND TRANSACTION DATA OR THE TEMP KEY TO VERIFY CRYPTOGRAM RECEIVED FROM POS
289
DID CRYPTOGRAM VERIFY
SUCCESS AUTH
FAIL AUTH

Fig. 28

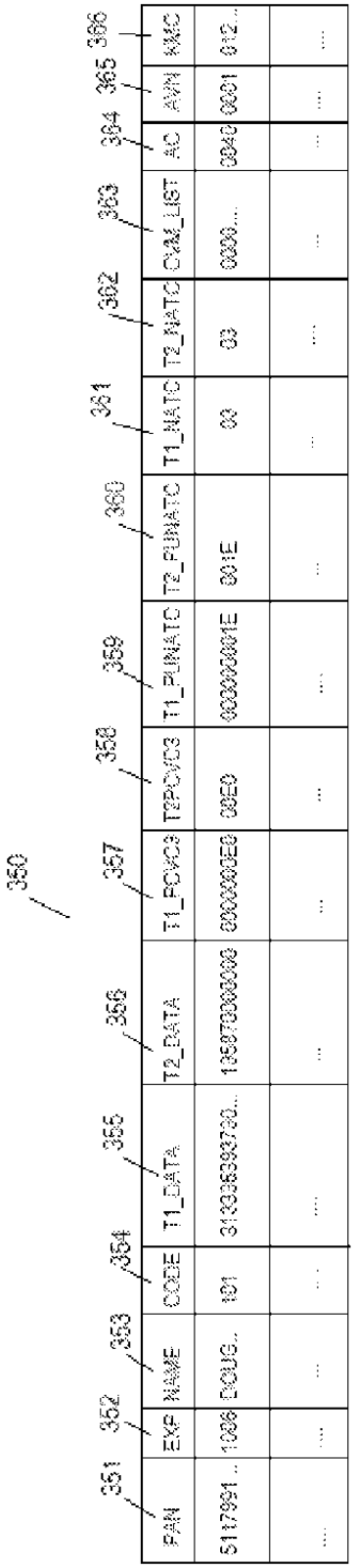

350
351
PAN
5117991...
...
352
EXP
1006
...
353
NAME
DOUG...
...
354
CCE2E
101
...
355
T1_DATA
3103383937...
...
356
T2_DATA
1359730000000
...
357
T1_PCVC3
0000000E0
...
358
T2PCVC3
00E0
...
359
T1_PUNATC
00000001E
...
360
T2_PUNATC
001E
...
361
T1_NATC
03
...
362
T2_NATC
03
...
363
CAK_LIST
0200...
...
364
AC
3040
...
365
AVN
0001
...
366
MAC
012...
...

Fig. 29

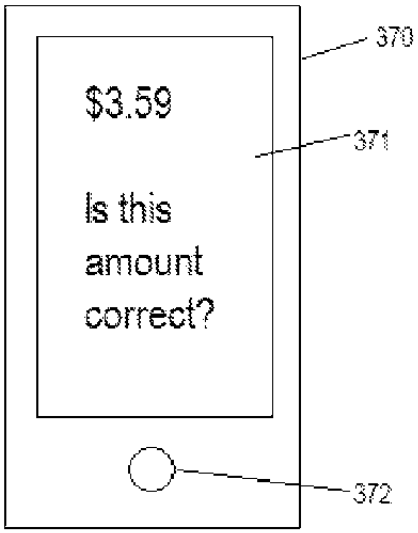

370
$3.59
371
Is this amount correct?
372

Fig. 30

APPLICATION

OF

C. DOUGLAS YEAGER

FOR

LETTERS PATENT OF THE UNITED STATES

FOR

SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM

Name C. Douglas Yeager
Address 7200 Spurlock Dr., Austin, TX 78731
Citizen of USA

Luedeka Neely Group, P. C.
P.O. Box 1871, Knoxville TN 37901

1.865.546.4305 (Tel)
1.865.523.4478 (Fax)

JPalmer@LNG-Patent.com

Attorney Docket: 67979.U2.US

COVER SHEET

SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM

CROSS REFERENCES TO RELATED APPLICATIONS

[0001] This application claims priority from and is related to U.S. Provisional Patent Application Serial No. 61/575,846 filed 08/30/2011, entitled: "Remote Hosted Secure Element Repository." This application claims priority from and is related to U.S. Provisional Patent Application Serial No. 61/573,476 filed 09/06/2011, entitled: "Remote Hosted Secure Element Repository." This application claims priority from and is related to U.S. Provisional Patent Application Serial No. 61/685,863 filed 03/26/2012, entitled: "Remote Hosted Secure Element Repository." This application claims a priority date of 08/30/2011 which is the filing date of U.S. Provisional Patent Application Serial No.61/575,846. Provisional Patent Application Serial Nos. 61/575,846 and 61/573,476 and 61/685,863 are incorporated by reference in their entirety herein.

Mastercard, Ex1002, p. 27

FIELD

[0002] This disclosure relates to the field of payment and authorization methods. More particularly this disclosure relates to using a mobile computing device in combination with a remotely hosted Secure Element representation to make payments, authorizations or exchange information with other devices.

Mastercard, Ex1002, p. 28

BACKGROUND

[0003] In some payment technologies such as smartcard payment, a microchip referred to as a "Secure Element" (SE) is embedded into a payment card, a payment fob (medallion), a cell phone, or other mobile devices that may be used for making payments. For the purpose of simplifying language in this document, a device that houses the SE will be referred to as a "card" or "card device". It is important to note that the "card" or "card device" may not physically resemble the shape or size of a typical payment card and may come in various form factors such as embedded into a mobile phone or embedded into a removable storage or removable device. Also, it is important to note that the SE may be an emulated software based SE and not strictly hardware based. For example, virtually any electronic device with a digital memory and processor or controller may be adapted to emulate and pretend to be an SE.

[0004] In order to extract information from the SE, an interrogator, also referred to in this document as a "reader," is required to interact electrically with the SE. The reader typically follows standards set forth by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and by application providers (such as VISA and MASTERCARD).

[0005] Secure element systems typically require that the user have physical possession of a card that matches the authorization capabilities of a merchant's system where a purchase is made. In many instances this is inconvenient. Therefore more flexible and convenient systems and methods for authorizing financial transactions are needed.

SUMMARY

[0006] Provided herein, in one embodiment, is a method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction. This embodiment includes a step of using a remote permanent cryptographic key to calculate an expected cryptogram that is expected to include at least a portion of the digital credential data. In this embodiment the remote permanent cryptographic key is persistently stored at a remote source that is remote from the mobile device and the mobile device does not store or access a duplicate local permanent cryptographic key persistently stored locally to the mobile device. This embodiment also includes a step of performing an interrogation between the point-of-sale terminal and the mobile device. This performing an interrogation step includes sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device requesting the digital credential data. This performing an interrogation step also includes sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal including the expected cryptogram as the at least a portion of the digital credential data, such that the financial transaction is authorized.

[0007] A further embodiment provides another method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction. This embodiment includes a step of performing an interrogation between the point-of-sale terminal and the mobile device. This performing an interrogation step includes sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device, the at least one POS command communication that includes (a) a request for the digital credential data that is expected to include an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data, and, at least in part, from a permanent cryptographic key and (b) the unpredictable data. This performing an interrogation step further includes sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal, with the at least one device response communication including at least a

portion of the digital credential data that includes an unexpected cryptogram, substituted in place of the expected cryptogram, such that the financial transaction is authorized.

[0008] A further embodiment provides a method for acquiring digital credential data by a point-of-sale terminal from a secure mobile device for authorization of a financial transaction. This embodiment includes a step of performing an interrogation between the point-of-sale terminal and the secure mobile device. In this embodiment the performing an interrogation step includes sending through a communication channel at least one POS command communication from the point-of-sale terminal to the secure mobile device, the at least one POS command communication comprising (a) a request for the digital credential data that is expected to comprise an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data, and, at least in part, from a permanent cryptographic key and (b) the unpredictable data. In this embodiment the performing an interrogation step also includes sending through the communication channel at least one device response communication from the secure mobile device to the point-of-sale terminal, where the at least one device response communication includes at least a portion of the digital credential data that includes the expected cryptogram. Then, in a step that follows the step of performing an interrogation, a secure mobile device transmitting step is provided, which includes sending over a second communication channel the unpredictable data from the secure mobile device to a remote application system. Further in this embodiment, in a step that follows the step of performing an interrogation, a point-of-sale terminal transmitting step is provided, which includes sending over a third communication channel an authorization request from the point of sale terminal to the remote application system, where the authorization request includes the expected cryptogram and the unpredictable data. Further, in a step that follows the secure mobile device transmitting step and the point-of-sale terminal transmitting step, a corroborative authorizing step is provided. The corroborative authorizing step includes verifying a correctness of the expected cryptogram by the application system and verifying a correctness of the unpredictable data by the application system by comparing the unpredictable data sent over the second communication channel with the unpredictable data sent over the third communication channel. The corroborative authorizing step further includes sending through the third communication channel an authorization response from

the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable data and at least in part by the verifying of the correctness of the expected cryptogram, such that the financial transaction is authorized.

Mastercard, Ex1002, p. 32

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] Various advantages are apparent by reference to the detailed description in conjunction with the figures, wherein elements are not to scale so as to more clearly show the details, wherein like reference numbers indicate like elements throughout the several views, and wherein:

[0010] Fig. 1 illustrates an embodiment of a command and response APDU (Application Protocol Data Unit) flow between a reader and an SE;

[0011] Fig. 2 illustrates an embodiment of a command and response APDU flow between a reader and an SE with specific details about the MASTERCARD PayPass application that may be installed on the SE;

[0012] Fig. 3 illustrates certain raw data related to an embodiment of a transaction between a reader and an SE;

[0013] Fig. 4 illustrates an embodiment of a format for which a reader may be required to deliver the results of a previous interrogation;

[0014] Fig. 5 illustrates an embodiment of a diagram of a mobile device that contains NFC capabilities;

[0015] Fig. 6 illustrates an embodiment of a diagram for how a mobile device that contains NFC capabilities and how that device may be used with an RFID POS reader;

[0016] Fig. 7 illustrates an embodiment of an interaction flow between a typical RFID POS reader and a mobile device with NFC or a contactless card;

[0017] Fig. 8 illustrates an embodiment of a repository that uses hardware representations of secure elements;

[0018] Fig. 9 illustrates an embodiment of a somewhat schematic representation of a repository that uses virtual hardware representations of secure elements;

[0019] Fig. 10 illustrates an embodiment of a repository that uses hardware representations of secure elements;

[0020] Fig. 11 illustrates an embodiment of a diagram of a mobile device that contains NFC capabilities and how that device may allow access to secure elements.

[0021] Fig. 12 illustrates an embodiment of a diagram of an addressable array of remote hosted SEs;

[0022] Fig. 13 illustrates an embodiment of a User ID SE address lookup table;

[0023] Fig. 14 illustrates an embodiment of an authorization flow for using a remote hosted SE;

[0024] Fig. 15 illustrates an embodiment of a data flow diagram including authorization between a mobile device and a remote hosted SE;

[0025] Fig. 16 illustrates an embodiment of an example of caching being used during a MASTERCARD PayPass transaction between a RFID POS and a remote SE;

[0026] Fig. 17 illustrates an embodiment of an example of 100% transaction caching being used during a VISA PayWave transaction;

[0027] Fig 18 illustrates an embodiment of an example of using a remote authorization server to deliver static T1/T2 data without the use of a Remote SE to a mobile handset;

[0028] Fig. 19 illustrates an embodiment of how a system may be created to simulate a remote hosted bank of SEs;

[0029] Fig. 20 illustrates an embodiment of communications and communication channels between a point-of-sale terminal, an electronic communication device, and a repository;

[0030] Fig. 21 illustrates an example of an application system that uses a hardware security module;

[0031] Fig. 22 illustrates an embodiment of data elements from a sequence of transactions prior to the processing of the transactions;

[0032] Fig. 23 illustrates an embodiment of a mobile device acquiring transactional data to store in a mobile device cache;

[0033] Fig. 24 illustrates an embodiment of an interrogation between a point-of-sale and a mobile device;

[0034] Fig. 25 illustrates an embodiment of transactional data flow from a mobile device and point-of-sale to an application system after an interrogation;

[0035] Fig. 26 illustrates an embodiment of data elements from a transaction during or after the processing of a transaction;

[0036] Fig. 27 illustrates an embodiment of a verifying transactional data;

[0037] Fig. 28 illustrates an embodiment of an entire authorization data flow between a mobile device and point-of-sale;

[0038] Fig. 29 illustrates an embodiment of data elements that may be used to form a digital credential; and

[0039] Fig. 30 illustrates an embodiment of a request on a mobile device for card-holder validation of a transaction.

DETAILED DESCRIPTION

[0040] In the following detailed description of the preferred and other embodiments, reference is made to the accompanying drawings, which form a part hereof, and within which are shown by way of illustration the practice of specific embodiments of systems and methods for acquiring digital credential data and for securing authorization for a financial transaction. It is to be understood that other embodiments may be utilized, and that structural changes may be made and processes may vary in other embodiments.

[0041] Prior to card issuance, an SE is typically injected with personalization or "credential" data that is generated from a "Hardware Security Module" (HSM). The HSM securely contains the cryptographic keys and algorithms that relate to a particular banking application and more specifically may contain a set of individual digital credentials. An HSM typically is accessed in a secure environment and never allows direct access to master keys which are used to create diversified keys or to encrypt or decrypt input data that may be provided to the HSM.

[0042] A significant advantage of extracting and delivering data that are contained within an SE is provided by an ability to know beyond reasonable doubt that the data string being delivered indeed came from a particular SE or card. This knowledge creates a more secure transaction with lower risk to the merchant, card issuing bank, and card associations. Traditionally the methods for extracting information from a banking card involve swiping the magnetic stripe on a card through a magnetic stripe reader, or extracting the information with a separate contact or contactless reader connected to a point-of-sale (POS) terminal. Because of inherent security that is provided by these methods of extracting the information on the card, a merchant may receive a lower transaction fee for that particular transaction. On the other hand, reading or entering account numbers, expiration dates, and card verification codes off of a card during a phone call or internet shopping experience is less secure, and may result in a higher transaction fee.

[0043] It is important to note that acquiring transactional data from an SE (such as Track1/Track2 data that are equivalent to data located on a card magnetic stripe) is

significantly different than simply using a duplicate of transactional data (such as a copy of Track1/Track2 data). A typical magnetic stripe on a card is a static data set because it never changes Track1/Track2 data between transactions or "swipes". For this reason, the data on the stripe may simply be copied or duplicated for use without having physical access to the payment card. Simply copying the card digits printed on the front and back of the card presents this same security risk. In other words, the data on a magnetic stripe may be copied and even programmed to another mobile device and used to make transactions continuously from the copy with no technical limitation. In the same way, card numbers that are simply copied from the face or front or back of the card and programmed to a mobile device and may also be continuously used to make transactions without a technical limitation.

[0044] In contrast to the acquisition of transactional Track1/Track2 data from a magnetic stripe on a card, the acquisition of transactional Track1/Track2 data from a SE is "singular." In other words, those data have a life span of a single transaction or a single "swipe" and then the data are no longer valid. Moreover the Track1/Track2 data acquired during normal usage of an SE cannot be created by any other entity except the SE which has been programmed with at least one secret key owned by the bank that loaded the key(s) and their accessing system to that SE.

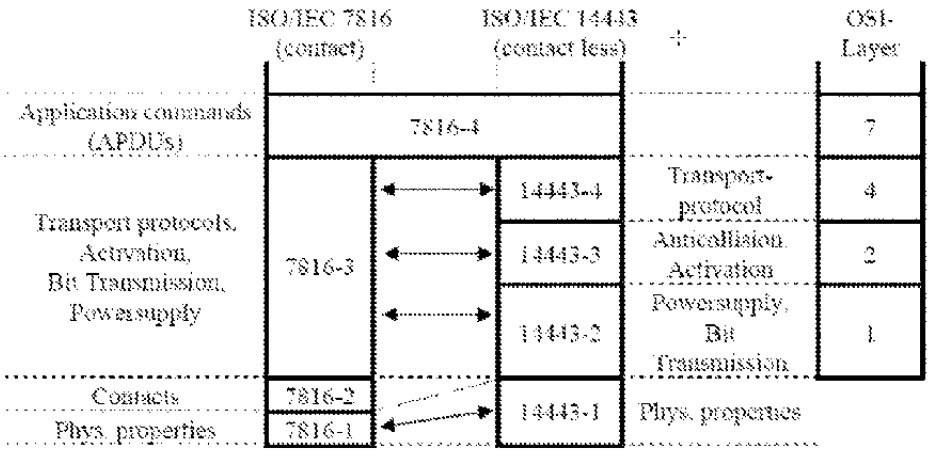
[0045] Knowing this difference, various embodiments disclosed herein are directed specifically to SE transactions because the security of these types of transactions makes the architecture much more credible and secure under current industry banking and processing standards.

[0046] Cards containing an SE are typically presented to an RFID (Radio Frequency Identification) reader device as the interrogator that extracts the information from the card and delivers the data to the POS terminal and then forwarded by the POS terminal on to a card processor for authorization. Mobile phones that contain NFC (Near Field Communication) functionality with embedded SEs have the ability to pretend to be (or emulate) a card that contains an SE. In this case the mobile phone may be presented to the RFID reader just as a card would be presented, and the information may be extracted from

the SE that is on the mobile phone and delivered to POS, which then forwards the data on to a card processor for authorization.

[0047] Fig. 1 describes a protocol level communication between a reader and an SE. The protocol layer is a standard protocol referred to as APDU. APDU stands for Application Protocol Data Unit and typically the protocol is defined by ISO/IEC specification 7816. This specification (commonly referred to as "ISO 7816" is a broad specification with different sections directed toward different "layers" of communication protocols, as seen in Table 1.

Table 1



Communications referred to herein as being according to ISO7816-4 correspond to Open Systems Interconnection (OSI) layer 7. The OSI model is a product of the Open Systems Interconnection effort at the ISO. OSI layer 7 is a high-level software applications layer. The APDU section of the 7816-4 specification describes two forms of APDU communications abbreviated as C-APDU ("command APDU") and R-APDU ("response APDU"). "Commands" are sometimes referred to as "queries" because they originate from an "interrogator," which has a querying connotation.

Mastercard, Ex1002, p. 38

[0048] The APDU data typically are transmitted over the air on 13.56 MHz radio waves between the reader and the SE. There is no hardware requirement limitation on this process; the APDU commands are just data moving from one entity to another. Various embodiments disclosed herein use the standard APDU commands to interact with the SE regardless of whether the SE is the mobile device's own embedded SE, or is a remote SE embedded into a different mobile device or a card. Communications 1, 2, 3 and 4 show the sequential commands of a typical command and response between and SE and a reader. Usually multiple steps are involved with accessing a SE, which involves multiple APDU commands and responses. Fig. 1 shows the general interrogation steps to access digital credential data specifically for a MASTERCARD PayPass Mag Stripe application running on an SE, according to "Mag Stripe.pdf" (Ver. 3.3) presently available at http://www.PayPass.com/approved-products.html. The term "digital credential data" as used herein refers to at least a portion of all data, including any data that are required to calculate the data, that are necessary to authorize approval of a transaction at a POS terminal.

[0049] Fig. 2 describes the detailed commands and responses expected when a reader interrogates a MASTERCARD PayPass Mag Stripe Ver. 3.3 application running on a SE. This sequence is provided in the MASTERCARD PayPass card specification. Shown in Fig. 2 are communications 5, 6, 7, 8 and 9 with details including abbreviations and acronyms explained subsequently herein.

[0050] Fig. 3 describes example transactions at the ISO/IEC 7816-4 Application Protocol Data Unit (APDU) protocol level between a reader and a card. The transaction processing depicted in Fig. 3 is representative of the MASTERCARD PayPass Mag Stripe application card specification v. 3.3. The notation ">CARD" denotes commands to the card and the notation "CARD>" denotes responses from the card. Communication 9 defines some of the initial parameters used in the transaction which include an unpredictable number issued by the reader, a transaction counter maintained on the SE. Communication 10 describes the command that the reader issues to the SE to find out what applications exist on the SE. This example shows that the MASTERCARD PayPass application responds as an active one. Next, communication 11 shows how the reader commands the SE to properly select the

PayPass application for further processing. Communication 12 shows how the reader receives the type of processing options that the PayPass application supports. Communication 13 shows how the reader commands and then receives the PayPass application specific credential information about its card holder including card account number, holder name, expiration date, and more. Communication 14 shows how the reader receives the dynamic aspects of the transaction that will be inserted into the Track 1 and Track 2 data. This command uses a shared key on the SE, the unpredictable number from the reader, and the transaction counter on the SE to determine a new number sequence for each transaction called a cryptogram. After the SE calculates the cryptogram, it sends it back to the reader in the response APDU. These data are obtained through the MASTERCARD PayPass card specification that was referenced earlier in this document. All details including abbreviations and acronyms are explained in detail through that card specification document.

[0051] Fig. 4 describes how the reader 21 in Fig. 5 formats the response data received from the SE into accepted Track1 and Track2 data strings that are used in existing processing systems. Communication 15 shows a Track2 data string built from the card interrogation in Fig. 3. The CVC3(Track2) UN and ATC numbers will all vary with each transaction or interrogation of the SE. Communication 16 shows a Track1 data string built from the card interrogation in figure 3. CVC3(Track1), ATC, and UN numbers will all vary with each transaction or interrogation of the SE. These data are obtained through the MASTERCARD PayPass card specification that was referenced earlier herein. All details including abbreviations and acronyms are explained in detail through the cited MASTERCARD card specification document.

[0052] Fig. 5 describes the inner architecture of a mobile device that supports NFC functionality. Examples of such devices are described in U.S. Patent 8,151,345 issued to C. Douglas Yeager from U.S. Patent Application Number 12/019,318. U.S. Patent 8,151,345 and U.S. Patent Application Number 12/019,318 are incorporated by reference in their entirety herein. A base band processor 17 of a mobile device typically runs an OS (Operating System) to control all aspects and interfaces on the device including communication access

to the SIM, NFC controller, Secure IC 19. The NFC controller acts as a router to determine where the communication is routed. The baseband controller has the option:

a. To communicate through the NFC controller to the reader and antenna 23 to communicate with an external card or device 24 over 13.56 MHz radio 22. There are 2 modes of this:

    i. The external card or device is a passive tag. This is reader mode

    ii. The external card or device is a mobile device in peer to peer mode.

b. To communicate through the NFC controller to the embedded Secure IC

c. To configure the NFC controller into card emulation mode in which case the NFC controller routes information from the external antenna 23 directly to the Secure IC 19 or a SIM 20.

Both options a. and b. could use APDU data to exchange information between the baseband processor 17 and the applications located in the internal SE 19 or to a remote SE. It is important to note that the SIM 20 or Secure IC (SE 19) may also be created with software and emulated within the baseband processor 17. The interrogation example mapped out in fig. 3 and 4 could easily be implemented on this system in all three modes a., b., and c. above. This suggests that the baseband processor 17 could perform the identical interrogation on the internal secure element 19.

[0053] Fig. 6 describes a typical interaction between a mobile device with NFC functionality and an RFID POS reader. The mobile device 25 is set to NFC mode in which it is emulating or pretending to be a card. The mobile device 25 is then presented to the RFID reader 27 and communication begins over the 13.56 MHz baseband 26. The reader then interrogates the card similar to Fig. 1 and Fig. 2, and Fig. 3 and compiles the standardized credential data into Track1 and Track2 equivalent data like in Fig. 4. The term "equivalent" is used in some industry documentation to refer to Track1/Track2 data that were not generated by a magnetic-head reader from a magnetic stripe on a card, but instead are created in a purely

digital data form, such as by an RFID reader. The term "Track Data" is used herein to refer to data comprising all or portions of the Track 1 and/or Track 2 data as defined in ISO7813. The data are then delivered to the connected POS computer 29 that then routes the data properly to the processor with other transactional information for authorization. In some embodiments Track Data are delivered to a field in a transaction authorization system using keyboard emulation. Some software applications expect data to be entered using a keyboard, and the application may check features of the data entry process, such as cadence and elapsed time, to verify that the data are entered via a keyboard. "Keyboard emulation" refers to a process of delivering data by a device or software representation of a device that is not a physical keyboard in manner that tricks the operating system into believing that a key has been pressed. Effectively the keyboard emulation system provides an entry as if it were a keystroke in a form field that correctly has the focus of the cursor.

[0054] Fig. 7 describes a typical transaction flow between an NFC enabled mobile device 52 or a contactless card 53. Step 54 describes setting up the mobile device to perform a transaction with an RFID POS reader. Step 55 describes presenting the mobile device within field range of the RFID POS reader. Step 59 describes presenting a contactless payment card to an RFID POS reader. Step 56 describes the RFID POS reader interrogating either the mobile device or the contactless card over the 13.56 MHz radio. Step 57 describes how the RFID POS reader constructs the Track1/Track2 data from the interrogation. Step 58 describes how the formatted data are delivered to the POS and on to the processor for authorization.

[0055] The systems and methods described herein above may be extended to facilitate transactions at a point-of-sale terminal where it is not necessary for the user (e.g., the purchaser) to have physical possession of a card with a magnetic stripe or possession of a secure element at the point-of-sale terminal. Such systems typically employ a "Remote Hosted Secure Element" (RHSE). An RHSE is a repository for a plurality of "secure element representations" each of which is provided for one or more mobile devices or mobile device owners. The repository storing the plurality of secure element representations is typically remote from the point-of-sale terminal. As used herein the term "remote" refers to locations

that are geographically far apart. One indication of remoteness is that the two locations are not within a distances such that most persons at one or the other of the remote locations would consider walking to the other location, or at least would not be able to do so within one day. This frame of reference is provided merely to explain the meaning of the term "remote" and does not imply that actually walking between remote locations has anything to do with embodiments disclosed herein. To further explain remoteness using as an example the situation where many point-of-sale terminals are serviced by one repository, it is entirely possible that one or more of the point-of-sale terminals may be within walking distance of the repository. However, when that is not the case for most of the point-of-sale terminals having access to the repository, then all of these point-of-sale terminals are considered to be remote from the repository. As used herein the term "local" refers to locations that are geographically proximate to each other. One indication of a local relationship between two locations would be the locations are separated by a distance of less than one foot.

[0056] The plurality of secure element representations (or the "array of secure element representations") is typically hosted in a secure environment such that it is protected from cyber attack. The secure element representations may be (a) actual SE hardware (referred to herein as a "hardware representation"), or may be (b) virtual hardware secure element representations such as a computer model that simulates the operation of a hardware SE element (referred to herein as a "virtual hardware secure element representation"), or may be (c) data in a database (typically a secure database), such as static Track Data or data dynamically or statically generated by an HSM (Hardware Security Module), where the data in the database are elements of data that are typically stored in an SE memory (referred to herein as a "database secure element representation"). The term "software representation" is used herein to refer to either (i) a virtual hardware secure element representation or to (ii) a database secure element representation. As the terms are used herein, a "secure element," a "remote secure element," an "SE," or a "remote SE" may be a hardware representation, or a virtual hardware secure element representation, or a database secure element representation. Each form of representation, or a combination of just two of these three forms of representation, may be advantageously employed in certain embodiments such as described in the context of various figures and descriptions provided herein.

[0057] In a case where an array of secure element representations are present as actual SE hardware, a repository may be created with a network server that is connected to a wide-area network (such as the internet) and one or more SE readers that are each addressable by the network server. The one or more SE readers receive ISO 7816 protocol commands for communication to an SE using a communications protocol such as TCP/UDP/IP data packets. The one or more SE readers are each in communication with one or more SE's. Software and hardware that interacts with each card reader has the ability to query (command) each SE at a particular network address that corresponds to a particular remote mobile device. As a result data that are to be passed to a particular SE from a remote mobile device are translated (if necessary) and routed over a TCP/UDP/IP network to the correct hardware SE reader and hence to the SE. Responses from the SE are relayed to that particular remote mobile device. These readers and SEs are not limited to one particular form factor or any particular communications protocol.

[0058] In a case where an array of secure element representations are present as virtual hardware secure element representations, the one or more SE readers may interact with the virtual hardware secure element representations in substantially the same manner as the one or more SE readers interact with hardware representations (i.e., actual SE hardware). A software representation allows a completely contained system that gives the same remote mobile device functionality as the previous completely hardware based case. An example of a virtual hardware secure element representation is the jcop.exe software that is presently sold and supplied by NXP semiconductor within the JCOP tools suite. The jcop.exe software provided is not a secure element, but rather a self-contained smart card operating system contained within an executable file that is meant to run on a host computer as a process. When jcop.exe runs, it opens a communications port that is accessible through the host computer operating system. The communications port that jcop.exe opens up accepts and responds to 7816-4 protocol and effectively simulates real SE hardware. The JCOP tools suite that contains jcop.exe additionally is a development platform to develop Java Card applications. JCOP tools give the user the ability to program and test application-specific software. This is accomplished using a combination of a virtual machine (the Java Card Virtual Machine, one version of which is contain in the jcop.exe referenced above) and a

well-defined runtime library, which largely abstracts the applet from differences between smart cards. Using this technique one can run and debug both the Java Card code for the application that will eventually be embedded in a smart card, as well as a Java application that will be in systems that will use the smart card, all working jointly in the same environment.

[0059] In the case where the SEs in an array of SEs are database secure element representations, a SE card reader is not needed to interrogate the SE representations. . In such systems the data may be acquired by using an electronic processor to translate the ISO 7816-4 protocol queries (commands) from the remote device into standard database queries and then translating the database responses into ISO 7816-4 responses for transmittal to the remote device. An array of SEs may include combinations of one or more types of secure element representations. That is, an array may include hardware representations and/or virtual hardware representations and/or database secure element representations.

[0060] The SE hardware implementation may be the preferred case by the financial transaction industry simply because of the more secure nature of controlling the removable SE that may be manufactured with secure data residing on the SE chip in a secure facility and then shipped to the remote system facility to be plugged in and activated and verified.

[0061] Fig. 10 illustrates a repository 300 that employs hardware representations of secure elements. The repository 300 includes at least one secure element reader 304, and in the embodiment illustrated the repository 300 includes one secure element reader 304 having four RFID antennas 308. In the embodiment of Fig. 10, the secure element reader 304 is a contactless (RFID) reader operating under ISO 14443A or B protocols. A repository (such as the repository 300) typically includes a plurality of secure element representations, and in the embodiment of Fig. 10 the repository 300 includes eleven secure element hardware representations 312 each of which is integrated into one of eleven bank-issued transaction cards. In the embodiment of Fig. 10 the secure element reader 304 is disposed adjacent to the plurality of secure element hardware representations 312. As used herein the term "adjacent to" refers to a spatial condition where two devices are very close to each other, such as being in the same electronics cabinet, or at least in the same room. A data server 316

is provided to communicate with the plurality of secure element representations 312 through the secure element reader 304.

[0062] In typical embodiments a data server (e.g., the data server 316) is a hardware/firmware device that includes a multitasking processor, such as a multithreading processor, or a parallel processor, or a time-shared processor, to communicate with a plurality of secure element representations (e.g., the secure element hardware representations 312) through a secure element reader (e.g., the secure element reader 304). Typically such communication is conducted according at least one part (e.g., part 1, part 2, part 3 or part 4) of the ISO7816 specification to extract at least a portion of the digital credential data from a the paired secure element representation. In some cases only the bus communication protocol of the ISO layer may be used, in other embodiments the data section (i.e., part -4) may be used, and in some cases several or all of the sections (i.e., parts -1 through part -4) of ISO7816 may be used. In the embodiment of Fig. 10 the secure element reader 304 includes a multiplexor in order to sequentially address the secure hardware element representations 312. Typically the multiplexor is part of the hardware at the reader circuitry level. In other embodiments the multiplexor may be provided in software. The multiplexing function allows a single secure element reader to rotate through multiple ports or antennas in order to address and communicate with a plurality of secure element representations. Such a configuration allows a data server (e.g., the data server 316) to conduct a plurality of command/response time-wise overlapping sessions with the plurality of secure element representations (e.g., the secure element hardware representations 312) without causing confusion about which card is being interrogated and which card is responding. The data server 316 also includes a network interface processor that communicates with the internet over an internet connection 320. The use a plurality of secure element hardware representations to store multiple different secure elements in a common processing environment in order to conduct a plurality of command/response time-wise overlapping sessions with the plurality of secure element hardware representations provides utility (as an SE repository) that is unexpected from the usual application a secure hardware representation, such as a single bank-issued card that is read by an SE reader at a point-of-sale terminal.

[0063] Fig 8 illustrates an embodiment of a repository 400 that employs a plurality of contact readers 404 operating under ISO 7816. A separate dedicated reader is provided for each of a plurality of secure element hardware representations 408. In the embodiment of Fig. 8 the secure element hardware representations 408 are bank-issued cards containing a secure element chip that is accessible by a Universal Serial Bus (USB) connector, and the contact readers 404 are USB readers. A first portion 420 of a CPU 424 in a computer 428 is a multitasking data server to conduct a plurality of command/response time-wise overlapping sessions with the plurality of secure element hardware representations 408 through the plurality of contact readers 404. The USB standards typically limit the number of USB ports on a computer to 127 ports. A different bus architecture may be used to overcome that limitation, or a single USB reader may be configured to address multiple cards through electronic or even mechanical switching mechanisms. In the latter case the switching mechanism acts as a portion of a multitasking data server. In some embodiments (such as, for example, embodiments that employ contact readers as illustrated in the Fig. 8) a plurality of secure element representations may be disposed proximate to a secure element reader. As used herein the terms "proximate to" and "local" refers to a spatial condition where two devices are close to each other, but may not be adjacent to each other. For example, two devices that are in the same building (but not the same room) are considered to be proximate to each other. The term "proximate to" encompasses devices that are "adjacent to" each other.

[0064] Continuing with Fig. 8, a second portion 432 of the CPU 424 is a network interface processor that communicates with the internet over an internet connection 436. The internet connection 436 to the second portion 432 of the CPU 524 provides addressability of the plurality of secure element hardware representations 408 over the internet. The use a plurality of secure element hardware representations to store multiple different secure elements in a common processing environment in order to conduct a plurality of command/response time-wise overlapping sessions with the plurality of secure element hardware representations provides utility (as an SE repository) that is unexpected from the usual application a secure hardware representation, such as a bank-issued card.

[0065] Fig. 9 illustrates a repository 500 that employs virtual hardware secure element representations. A plurality of instances of virtual hardware secure element representations (shown symbolically as elements 504) is provided in a memory 508 of a computer 512. These virtual hardware secure element representations 508 may be multiple instances of the Java Card software previously described. Each instance is programmed as if it were a different secure element. Typically each instance is a separately-running thread of a standard jcop.exe program. Each instance may be run from a DOS command line such as:

jcop.exe –port 50000

Running that command opens up a TCP/IP PORT number 50000 and, presuming that the computer is on the internet (such as per internet connection 516), the program listens for telnet terminal type data on the telnet port, shown symbolically as element 518. It is expecting ISO7816-4 data communications and will respond just like a real SE with response ISO7816-4 data. Thus, when that program is running on the computer 512, another DOS window may be opened on a different computer to communicate with that instance of jcop.exe by executing the following command line:

telnet 192.168.0.14 50000

where the 192.168.0.14 is the IP address of the computer 512 where the simulation program (jcop.exe) is running, and where 50000 is the port number that it is running on. A local I/O bus 520 is controlled by a CPU 424 in the computer 512 so that when the telnet window on the second computer connects to that IP address and port number on the first computer 512, standard command/response communications may be established by sending 7816-4 formatted data and getting the response from the designated virtual hardware secure element representation 504 back into the telnet window of the second computer.

[0066] In the embodiment of Fig. 9, a first portion 520 of the CPU 524 operates as a secure element reader using a local I/O bus 528 to communicate with the virtual hardware secure element representations 504. The instances of virtual hardware secure element representations 504 are a plurality of secure element representations proximate to the secure element reader (I/O bus 528). A second portion 532 of the CPU 524 is a data server to

conduct a plurality of command/response time-wise overlapping sessions with the plurality of secure element representations (e.g., the virtual hardware secure element representations 504) through the first portion 520 of the CPU 524 that is operating as the secure element reader. The second portion 532 also includes a network interface processor that communicates with the internet over the internet connection 516. In the embodiment of Fig. 9 the secure element reader (i.e., the first portion 520 of the CPU 524) is disposed adjacent to the plurality of virtual hardware secure element representations 504. In other embodiments a secure element reader may be disposed proximate to the plurality of virtual hardware secure element representations. The internet connection 516 to the second portion 532 of the CPU 524 provides addressability of the plurality of secure element representations (504) over the internet. The use of multiple instances of the JCOP environment to store multiple different virtual hardware secure elements in a common processing environment in order to conduct a plurality of command/response time-wise overlapping sessions with the plurality of virtual hardware secure element representations provides utility (as an SE repository) that is unexpected from the usual application of the JCOP programming environment.

[0067] Fig. 11 describes an inner architecture of a mobile device 626 that supports NFC functionality and how that device may allow access to its attached secure elements as well as access to a secure element where the mobile device is remote from the secure element. A base band processor 17 is provided in the mobile device and the baseband processor 17 typically runs an OS (Operating System) to control all aspects and interfaces on the device including communication access to the SIM 20, NFC controller 18, Secure IC 19, or data that are eventually that are eventually sent to the internet 35. The NFC controller 18 acts as a router to determine where the communication is routed. When a mobile NFC device is presented to an RFID POS, the mobile device may emulate a card (pretend to be a payment card). When this happens the NFC controller 18 which is controlled by the baseband processor 17 in the mobile device may be configured to route interrogation commands and responses (such as communications 1, 2, 3, 4, 5, 6, 7, and 8 depicted in Figs. 1 and 2) from the reader (interrogator) 21 to a secure element for processing and response. Thus an SE application that is used in a payment transaction may be configured to respond to interrogation commands the same or similar to the sequences described in Fig. 1 and Fig. 2.

The commands and responses illustrated in Fig. 1 and Fig. 2 are comprised of a string of data that conforms to ISO/IEC 7816 specification. The baseband controller may choose to route the commands from the reader 21 to any secure element it chooses for processing. Some of the options include:

a. Routing ISO/IEC 7816-4 data through the NFC interface 18 to an embedded secure IC over its proprietary connected SE interface 625

b. Routing ISO/IEC 7816-4 data through the NFC interface 18 through the baseband processor 17, to an attached SIM card 20

c. Routing ISO/IEC 7816-4 data through the NFC interface 18 through the baseband processor 17, to an attached SD, miniSD, or microSD card that contains an SE

d. Routing ISO/IEC 7816-4 data through the NFC interface 18 through the baseband processor 17, over a data connection 627, 628, 629, 636, 35, 630 to a remote data server 632 using TCP/UDP/IP

[0068] All options a., b., c., and d. use APDU data to exchange information between the RFID reader 21 and the applications located in an SE located in the mobile device 626 or in a remote SE 634. It is important to note that the remote SE 634 may also be created with software and emulated within the remote system 631. The interrogation example mapped out in Figs. 3 and 4 may be implemented on this system in all 4 modes a., b., and c., and d. above. Thus the remote system SE 634 may perform the identical interrogation on a remote secure element 634

[0069] It is important to note that at the ISO/IEC 7816-4 (APDU) level, an entire interrogation similar to those described in Fig. 1, and Fig. 2 may be carried out from a RFID POS reader 21 through an NFC enabled mobile device 626, through a data connection over the internet 35 to a remote system 631 that contains the actual SE 634. An example of reader commands is illustrated in element 638 as a PayPass reader. The PayPass reader 638 shows an exemplary sequence of ISO/IEC 7816-4 APDU commands and responses that may be

pushed through the reader 21 and end up at the remote SE 634. Element 637 shows an example of APDU commands that are received by the remote SE 634 and the appropriate response that is issued as defined by the 7816-4 application for MASTERCARD PayPass. Elements 638 and 637 show how Figure 2 may be broken up so that the PayPass card may be hosted on a remote SE 634 on a remote system 631 and show that the PayPass reader may be an RFID POS 621.

[0070] The remote system 631 has a connection to the internet 630 and connections to an array or plurality of SE readers 633 that are each connected to an SE 634. A server or set of servers 632 may be used for pairing the connections originating at the mobile NFC device 626 to the correct SE 634 within the remote system 631. The server or set of servers 632 may, for example, be one or more computers each of which has access to control one or more of the SE readers 633.

[0071] The data connection described in Fig. 11 (i.e., the path 627, 628, 629, 636, 35, 630) is a TCP/UDP/IP connection that is offered by most cellular carriers over a cellular network and cellular towers 629 using a cellular link 628. The TCP/UDP/IP connection may run socket software that allows for raw data to be transmitted from one end of the data connection 626 and the other 631 and vice versa. The data packets within the socket software may be configured to exchange data that contains ISO/IEC 7816-4 data.

[0072] In alternate embodiments a stationary device may be used in place of the mobile device 626 depicted in Fig. 11.

[0073] Fig. 12 describes a remote system 700 that is capable of bridging a data (TCP/UDP/IP) connection through the internet 35 to a single addressable SE reader 749 and SE 750. Communications 740 and 741 show how a data link (TCP/UDP/IP) 740 may be used to pass ISO/IEC 7816-4 APDU data 741 to a remote server 742. In this example the remote system is identified on the internet through the IP address 743. The remote system is comprised of a remote server 742 that routes the connection to an internet network of attached SE Array Managers 746. The TCP/UDP/IP data 740 that enters this remote system and is routed to the internal SE Array Manager 746 over TCP/UDP/IP 744 contains data that

uses the protocol for ISO/IEC 7816-4 APDU data 741 and 745. Each SE Array Manager 746 contains an internally unique IP address 748 within a TCP/UDP/IP socket server 747. Each TCP/UDP/IP socket server 747 is responsible for receiving ISO/IEC 7816-4 APDU data 745 and routing as it as ISO/IEC 7816-4 APDU data 751 to the appropriate addressable SE reader 749 and SE 750.

[0074] Fig. 12 further illustrates one method to create a communication channel from the remote system to the mobile device over TCP/UDP/IP using socket server and client methods. Identification data from the mobile device may be used to set up a socket connection all the way through the remote server 742 to the TCP/UDP/IP socket server 747. The data that are sent over the socket server and client may be formatted to be ISO/IEC 7816-4 APDU data. The APDU command may enter the socket server 747 and be routed to the appropriate SE reader 749 and SE 750 and the response APDU may be sent from the SE 750 and SE reader 749 back to the remote mobile device through the SE Array Manager socket server 748, the remote system socket server 742, and through the internet 35 and be received by the socket client on the remote mobile device.

[0075] Fig. 12 also depicts a plurality of remote SEs that are each addressable and may be accessed by a plurality of remote mobile devices independently. The descriptions herein above describe how a single remote mobile device may connect to a remote system and specifically a single remote SE to complete a transaction. This same process may occur through this same system concurrently with different SE's in the system from different remote mobile devices.

[0076] Fig. 13 depicts a table in a database that may be used to identify which remote SE within a remote system described in Fig. 12 that a user and particular mobile device may be attached to. Unique row identifiers 754 are provided in the table. Each row contains related data. The other columns of this table are the User ID 752 and the SE Address 753. The SE address is the unique address within the remote system for a particular SE. The table of Fig. 13 further illustrates a relationship 755 between two fields that form a row in the database. This table in Fig. 13 may be used to properly match a remote user or remote mobile device with the address of a particular SE.

[0077] In order to connect to the remote system and create the connection to the correct SE for that user or mobile device, it is generally necessary that the mobile device must be validated by the remote system. At a minimum, validating a mobile device by a repository involves pairing a particular secure element or secure element representation to a specific mobile device. Generally this involves establishing at the repository a digital database that lists at least one secure element representation identifier for each of a plurality of mobile device identifications.

[0078] Fig. 14 describes one process flow for allowing a data connection between a mobile device and remote hosted secure element. Step 756 describes how a mobile device that supports NFC is initiated and presented to a RFID POS reader in order to make a payment transaction. The phone is placed into a mode that is referred to as card emulation mode where the NFC interface on the phone pretends to be contactless RFID card. The phone has a bit more control to select which card is presented to the POS. The subject of this patent describes how the NFC mobile device has the ability to use a SE for the transaction that is not physically located in the mobile device. This may be done be creating a data connection to a remote SE for which is used for the payment transaction. In step 757, while the phone is being placed into card emulation mode, the connection to the remote SE that will be used for emulation is attempting to connect. As illustrated in step 758 there is a chance that the connection is already open in which case the flow in Fig. 14 will simply allow the ISO/IEC 7816-4 APDU data to pass directly through the connection to the remote SE and back 763 successfully completing the transaction 764. There is also a chance that the connection to the remote SE does not exist and needs to be created, as described subsequently in step 762.

[0079] Typically systems require that a mobile device "authenticate" itself with a remote hosted secure element. The method of authentication to the remote system that is described in Fig. 14 may, for example, be initiated and completed using HTTPS/SSL (Hypertext Transfer Protocol Secure / Secure Socket Layer (SSL) or Transport Layer Security (TLS)) web services. Authentication may also be initiated and completed using a telephone link, such as a cell-phone connection. In some embodiments authentication is facilitated through a remote system authorization server. As used herein the term "remote authorization server"

refers to an electronic computer or set of computers configured for the purpose of approving or disapproving access to a particular secure element by a particular mobile device or stationary device. In some embodiments a remote system authorization server may be configured to access secure element representations that may be either proximate to the remote authorization server or that may be proximate to the remote authorization server, and in such embodiments the remote system authorization server is considered to be a remote repository having a plurality of secure element representations. The mobile device connecting to the remote system is able to pass various credentials to the remote system such as user ID, passwords, PIN, "gesture signal," unique electronic communication device identity number, and so on securely to the remote system for mobile device validation 759. In steps 760 and 761 the system attempts to match and verify the user information in the remote system. Where a gesture signal is used, the verification includes an assessment as to whether the gesture signal is a valid gesture signal (i.e., a gesture signal that is expected by the remote system). Upon a successful match the remote system is said to "validate" the remote device, and the remote system opens up a communication channel (step 762) to the appropriate SE within the remote system and creates a handle to that communication channel that may be used to access it from the remote mobile device. When a communication link is established between a mobile device (or a stationary device) and a particular SE in a repository, the device and the particular SE may be described as being "paired" with each other. Once the mobile device is paired with a particular SE the remote system (repository) may securely pass back over HTTPS/SSL a shared encryption key and handle to the communication channel that may be used for continued communication over that communication channel through a TCP/UDP/IP data socket 762. If the authorization fails (step 765), the connection to the remote SE is not opened, and the process ends. When the remote device receives the shared encryption key and handle to the communication channel to a particular SE on the remote system, the ISO/IEC 7816-4 APDU commands from the RFID POS may be passed to this remote hosted SE through a socket connection and the data may be encrypted with the shared encryption key. The remote system may decrypt the data and send it to the correct SE within the remote system. The remote system may then send the response APDU from the SE back to the remote mobile device in a similar manner. The

remote mobile device may forward this response APDU back through the NFC interface to the RFID POS reader.

[0080] Some electronic communication devices (such as a mobile device) have memory for storing at least a portion of digital credential data as cached data. Such electronic communication devices are configured to send the cached data as at least a portion of a device response communication. When such an electronic communication device authenticates with a secure element representation, cache data can be copied from or extracted from data within a single secure element representation that is specifically matched or "paired" to an electronic communication device and may be provided to the electronic communication device, such as in Fig. 17, element 801. In such embodiments the electronic communication device may be paired with the single secure element representation for the purpose of extracting or copying cache data and may not be paired for any subsequent command/response communications. Such cache data are a "cached portion" of a set of digital credential data, and in some embodiments this cached portion is all of the digital credential data that are needed to complete a transaction. In some embodiments the cache data may include an ISO 7816-4 protocol response communication. In some embodiments the cache data may also include ISO7816-4 protocol command communication for the purposes of matching or analyzing it against other incoming ISO7816-4 protocol command communication data to determine which ISO7816-4 protocol response communication from the cache to use.

[0081] Fig. 15 illustrates an authorization and communication process in more detail. The vertical line 766 represents the RFID POS entity. The vertical line 767 represents the mobile device. The vertical line 768 represents a remote system authorization server, and the vertical line 769 represents the remote hosted SE. As shown in Fig. 15, the mobile device 767 may interact with a remote authorization server (e.g., remote authorization server 768) in order to facilitate the access of digital credential data from a remote hosted SE (e.g., remote SE 769).

[0082] In the example of Figure 15, a communication channel is opened between the RFID POS 766 and the remote SE 769. Authorization over SSL is initiated where credentials 770

are sent to the remote authorization server 768. The remote authorization server 768 verifies the credentials and sends back a successful response 771 which contains a handle to a communication channel and an encryption key. The mobile device 767 may then open a channel to the remote SE 769. At that point APDU command and response APDUs may be sent securely between the RFID POS reader 766 and the remote SE 769 and back through the mobile device 767. An APDU command 772 is sent from the RFID POS reader 766 to the mobile phone 767, which may encrypt that APDU as command 773 and forwards an APDU command 773 on to the remote system 768 and on to the remote SE 769 as APDU command 774. In some embodiments the command communications 773 and 774 comprise at least a portion of the command communication 772 from the RFID POS 766 to the mobile device 767. In some embodiments the mobile device 767 may know ahead of time what the RFID POS 766 will command the mobile device 767 in the APDU command 772 in advance of actually interacting with the RFID POS 766. In such cases the command 773 may have been sent already sent by the mobile device 767 before the command 772 was received by the mobile device 767 from the RFID POS 766. The return APDU response from the SE is delivered back to the RFID POS through the communication channel using the handle provided by the response 771, via communications 775, 776, and 777.

[0083] With some data networks that pass TCP/UDP/IP information there are network delays and latencies that contribute to delays for round trip information exchange with a destination. With many embodiments disclosed herein, data are intended to go round-trip from a mobile device to a remote SE. Many payment applications that communicate with an SE may require a plurality of commands and responses to the SE for each transaction carried out by an interrogation from the POS RFID reader. Each or some of these command and responses to the SE may be subject to network delays and latency. Prolonged delays during a transaction with the RFID POS may cause an unsatisfactory user experience. Here is an example of a delay that was recorded during evaluation of an embodiment described herein:

a. Card transaction with a MASTERCARD PayPass plastic card and a RFID POS reader was measured to take ~200ms

b. Card transaction with a remote SE programmed with the MASTERCARD PayPass application over a 3G network managed by Verizon through a mobile handset was measured to take ~600ms

[0084] The remote SE took ~400ms longer in the above example due to network latency and delay during the SE interrogation.

[0085] A local cache (a memory located in the mobile device for data caching) may be implemented for use in some embodiments. Many of the responses to a 7816-4 APDU commands or queries are static and unchanging in a payment application on a SE. For this reason, a cache system may be configured to respond locally for these static information requests with the known 7816-4 APDU data responses, and to only generate real-time commands the remote SE in the event that the response 7816-4 APDU data are dynamic or changing with each transaction. This should limit the number of round trip data requests to the remote SE. Because each round trip request to the remote SE is subject to network delay and latency, a relatively significant total transaction time savings may be realized. The main advantages of implementing a caching system in the current invention is to save over-all time to perform a full transaction with a payment card application between a RFID POS reader through a mobile device to a remote SE.

[0086] Fig. 16 illustrates an example of caching being used during a MASTERCARD PayPass transaction between a RFID POS and a remote SE. The vertical line 778 represents the RFID POS entity. The vertical line 779 represents the mobile device. The vertical line 781 represents the remote system authentication server, and the vertical line 782 represents the remote hosted SE. The vertical line 780 represents the caching system in the mobile device.

[0087] The MASTERCARD PayPass card specification indicates that the response to the Select PPSE APDU 83 will always be the same:

a. APDU to the card for Select PPSE APDU:

```
00 A4 04 00 0E 32 50 41 59 2E 53 59 53 2E 44 44 46
30 31 00
```

b. APDU response from the card for Select PPSE APDU is ALWAYS:

```
6F 23 84 0E 32 50 41 59 2E 53 59 53 2E 44 44 46 30
31 A5 11 BF 0C 0E 61 0C 4F 07 A0 00 00 00 04 10 10
87 01 01 90 00
```

In some embodiments the fact that the APDU response from the card for Select PPSE APDU is ALWAYS a prescribed sequence is used to advantageously cache this response and then the caching system 780 may respond to this APDU without making a command all the way to the remote SE over the data network.

[0088] The MASTERCARD PayPass card specification indicates that the response to the Select PayPass AID APDU 84 always be the same:

a. APDU to the card for Select PayPass AID APDU:

```
00 A4 04 00 07 A0 00 00 00 04 10 10 00
```

b. APDU response from the card for Select AID APDU is ALWAYS:

```
6F 17 84 07 A0 00 00 00 04 10 10 A5 0C 50 0A 4D 61
73 74 65 72 43 61 72 64 90 00
```

This prescribed response to this APDU may also be cached and the caching system 780 may respond to this APDU without making a command all the way to the remote SE over the data network.

[0089] Furthermore, the MASTERCARD PayPass card specification indicates that the response to the GPO (Get Processing Options) APDU 785 always be the same:

a. APDU to the card for GPO APDU:

```
80 A8 00 00 02 83 00 00
```

b. APDU response from the card for GPO APDU is ALWAYS:

```
77 0A 82 02 00 00 94 04 08 01 01 00 90 00
```

This means that the response to this APDU may be cached and the caching system 780 may also respond to this APDU without making a command all the way to the remote SE over the data network.

[0090] The MASTERCARD PayPass card specification indicates that the response to the Read Record APDU 786 is to always be the same for a particular card that has been personalized, but will be different from personalized card to a different personalized card:

a. APDU to the card for Read Record APDU:

```
00 B2 01 0C 00
```

b. APDU response from the card for Read Record APDU is ALWAYS for a specific card:

```
70 7F 9F 6C 02 00 01 56 3E 42 35 34 31 33 31 32 33
34 35 36 37 38 34 38 30 30 5E 53 55 50 50 4C 49 45
44 2F 4E 4F 54 5E 30 39 30 36 31 30 31 33 33 30 30
30 33 33 33 30 30 30 32 32 32 32 32 30 30 30 31 31
31 31 30 9F 64 01 03 9F 62 06 00 0C 00 38 00 00 9F
63 06 00 00 00 00 E0 E0 9F 65 02 0C 0E 9F 66 02 0E
70 9F 6B 13 54 13 12 34 56 78 48 0C D0 90 61 01 90
00 99 00 00 00 0F 9F 67 01 03 90 00
```

This means that the response to this APDU may be cached and the caching system 780 may respond to this APDU without making a command all the way to the remote SE over the data network, UNLESS the card on the SE has changed to a different card, in which case the caching system should send this command to the remote SE for processing.

[0091] The MASTERCARD PayPass card specification indicates that the request and the response to the Compute Cryptographic Checksum APDU 787 will always be different for each transaction. This means that this APDU will always need to be processed by the actual remote SE through the data network. Communication 793 indicates the estimated or example of network processing time for this single APDU command and response 787. The over-all example in Fig. 16 illustrates how there is potentially only a single command and response that need to happen in real time over the data network 793 as a result of implementing a caching system.

[0092] In this specific example in Fig. 16, communications 788 illustrate one method to maintain the proper state of the remote SE 882 when a caching system is used. It is important that the remote SE 782 maintain the same processing state as the system is expecting when introducing a caching system. For this reason, it is important to actually issue the APDU commands to the remote SE in order to bring that SE to the appropriate system state. The dashed line illustrates how these ghost commands may be issued by the remote system in order for the SE to maintain an up-to-date state. The communications 789, 790, 791, and 792 mirror the APDU commands and responses 783, 784, 785, and 786 managed by the caching system 780.

[0093] Fig. 17 illustrates a slightly different caching concept using a VISA payWave transaction as an example. In this figure, the entire transactional sequence with all APDU commands and responses is cached at a separate time 802 prior to the actual transaction. In this example illustrated in Fig 17, the RFID POS 794 does not initiate the initial request to the remote authentication server 797. Instead, it is initiated by the mobile device application at some prior time from the actual RFID POS transaction. When the mobile device 795 makes a request to the remote system authentication server 797, the remote system authentication server 797 either retrieves caching information from a database, or from making a request to a HSM (Hardware Security Module) or other storage system or, if needed, makes commands with a remote SE 799 as indicated by the dotted box in the figure with a read record request 800 to the remote SE 799. The remote SE 799 may be a hardware representation of a secure element or a software representation of a secure element. This

example is particularly pertinent in the event that the response to the read record request 800 is dynamically changing data with each individual transaction with the SE. When all known responses to the remote SE transactional command(s) are gathered, the entire set of caching information may be passed back to the mobile device 795 as shown in communication 801. In communication 801 the SE responses to Select PPSE, Select PayPass, GPO, and Read Record APDU is passed back to the mobile device all at once.

[0094] Fig. 17 illustrates an unspecified time delay 802 after communication 801 until the actual start of the RFID POS transaction 803. During this time delay 802 the cached APDU command and response data may be stored safely in non-persistent memory or RAM in a cached format 796. An alternative is to store this data safely through encryption techniques in a persistent manner.

[0095] Communications 804, 805, 806, and 807 illustrate the real time transaction with an RFID POS at a later time 802 than the previous interaction with the remote authentication server 797. In this example each and every response APDU command that the RFID POS requested was replied to locally by the mobile device cache 796.

[0096] The configuration of Fig. 18 closely represents an embodiment which employs secure element software representations where the secure element software representations are in the remote system authorization server 836. Much of the transaction scenario in Fig. 18 is identical to Fig. 23 including the time delay 838 (802 in Fig. 23) prior to the actual transaction 840 (803 in Fig. 23) and the delivery of the transactional data from the server 836 (801 in Fig. 23). This type of data substitution is possible with existing contactless APDU commands as defined in the VISA payWave card specification. That card specification allows for a transaction with an RFID POS to be made using these commands:

a. Select AID: communication 11 Fig. 3

b. GPO: communication 12 Fig. 3

c. Read Record: communication 13 Fig. 3

[0097] The read record command for VISA payWave indicates there may be 3 data elements with the tags:

a. Tag 57: Track 2 Equivalent Data

b. Tag 5F20: Cardholder Name

c. Tag 9F1F: Track 1 Discretionary Data

[0098] Specifically Tag 57 is a required tag that presents Track 2 Equivalent Data to the POS transaction. This format of the data is processed by the RFID POS and converted into ISO7813 data format. An example of this data conversion is this:

a. Raw Tag 57 data:

i. 54 13 12 34 56 78 48 00 D0 90 61 01 90 94 99 89 92 50 3F

b. Converted to ISO 7813 format:

i. ;5413123456784800=09061019094998992503?

[0099] In this instance the data conversion is almost a direct conversion, just adding the start sentinel ';', the end sentinel '?' and substituting "=" the "D" and removing the trailing padding 'F' gives the ISO7813 equivalent data. ISO 7813 data are used to send out for authentication processing for both magnetic stripe cards and contactless cards. Because of this, the actual data in Tag 57 may be gathered and populated from a regular magnetic stripe card as described in Fig. 26 tasks in the remote system auth server 836.

[00100] Extrapolating this concept displayed in Fig. 18 further, it is possible to substitute any Track 2 data into tag 57 of the read record APDU response. Some substitution examples are:

a. Mastercard data: 54 13 12 34 56 78 48 00 D0 90 61 01 90 94 99 89 92 50 3F

b. VISA data: 44 13 12 34 56 78 48 00 D0 90 61 01 90 94 99 89 92 50 3F

c. AMEX data: 34 13 12 34 56 78 48 00 D0 90 61 01 90 94 99 89 92 50 3F

d. Any propriety data format (McDonalds Arch Card): 64 13 12 34 56 78 48 00 D0 90 61 01 90 94 99 89 92 50 3F

[00101] Fig. 19 illustrates two embodiments of SE repositories, repository 156 and repository 157, to illustrate some similarities between hardware representations of an SE 147 and a software representation of an SE 154. In both cases the mobile device that is accessing the secure element representation is remote from repository 156/157, and the secure element representation is accessed over an internet 152 or other global network. In the hardware based SE side (i.e., repository 156 on the left side) of the figure, the hardware representation of the SE 156 is a "chip" that may be mounted to a circuit board or located in a physical plastic card or a SIM module. Each such form factor has both power 145 and ground 146 lines, and also includes a data line 150 that is configured to be half duplex communication over various serial data rates 149. The SE 147 is a fully functional processor chip that includes ROM, RAM, communications controller, EEPROM or persistent memory and a processor. It is addressable by and communicated with by a Network Server 148 provided the correct conversion hardware is in place to do so. Such conversion hardware is depicted in Fig. 12 where the SE array manager 746 sits in between the network server 742 and the SE's 750. One job performed by the SE array manager 746 is to translate TCP/UDP/IP communication packets from the network server 742 into 7816-4 data packets for the SE's and vice versa.

[00102] In Fig. 19, the Network Server 148 serves as a communication server for communicating with the SEs and as a network interface with the internet 152. The APDU data communication (typically standard SE communication) between the Network Server 148 and the SEs 147 is extended to the Internet 152 over TCP/UDP/IP protocol. In Fig. 27, for clarity of illustration, details are depicted for only one hardware representation of SE 147.

[00103] The right side of Fig. 19 shows a repository 157 where the function of the SE are handled as multiple software representations 154 (SE Emulation Instances) in a single computer or a bank of several computers. In this configuration, there is no separate hardware

that is the SE. In the embodiment of Fig. 19. the functions of the SEs are provided as software representations depicted as SE Emulation Instances 154 that are established entirely in software and contained inside a Network Server 153. The communication format of APDU 7816-4 structure 155 may also be provided by the software of the Network Server 153. A general purpose computer or server typically has all the necessary components (such as ROM, RAM, Persistent Memory, and a processor) that are necessary to provide the SE software representations. The software architecture within the Network Server 153 may be arranged as such to divide and address many different SE software representations 154 within a single computer. In the same manner the hardware based SEs 147 are exposed to the Internet over TCP/UDP/IP, the software representations of the SEs 154 are also be exposed to the Internet.

[00104] Fig. 19 illustrates that either of the depicted architectures (i.e., the hardware representations 147 and the software representations 154) are functionally interchangeable and are interoperable from the external world over the Internet. Fig. 19 also suggests that a repository (such as repository 157) using software representations of SEs may be more easily scalable than a repository (such as repository 156) using many hardware representations. The use of virtual hardware representations may be a good compromise between the security of hardware representations and portability and scalability of database secure element representations.

[00105] Fig. 20 illustrates communications channels and communications between a point-of-sale terminal and an electronic communication device and a repository, according to some embodiments. There is a first communication channel 904 between a point-of-sale terminal 908 and an electronic communication device 912. The first communication channel may, for example, include a near field communication channel or an internet connection. The electronic communication device 912 may be a mobile device or a stationary device. There is a second communication channel 916 between the electronic communication device 912 and a repository 920. The second communication channel 916 may include, for example, a cell-phone connection or an internet connection. A POS command communication 924 may be sent over the first communication channel 904 and a device

command communication 928 may be sent over the second communication channel 916. A repository response communication 932 may be sent over the second communication channel 916 and a device response communication 936 may be sent over the first communication channel.

[00106] Fig. 21 illustrates an arrangement of an application system 201 (a variant of remote system auth server) that contains a Hardware Security Module (HSM) 200. The application system also includes a system of one or more computers that all may have access to the transaction table 205 and the credential table 206 within the application system. The application system contains data that should be kept in a secure manner and as a result may have both network accessibility and physical accessibility limitations built in to it. The application system can be further detailed as a "software representation" of a plurality of secure element representations as the application system has access to all the information used to create APDU responses for any particular SE representation in its repository data. An added feature of the application system that extend its capabilities beyond a "software representation" of a plurality of secure element representations is that because it has access to the HSM that stores keys used to create the data in each SE representation, it can be configured for authorizing or verifying the output data (digital credential data) for any of the SEs contained in its repository data as well. An HSM is a device commonly used in the banking and processing industry. The HSM is responsible for securely containing encryption keys 203 (cryptographic keys) that are used to authorize card payments, or create digital credential data for new cards. Encryption algorithms 204 that use these keys are also contained on the HSM. An example of an HSM used in the industry at the time of this filing is currently distributed by SafeNet Inc. and is named the Luna EFT Mark II Edition. An example, from the MasterCard PayPass MSD v3.3 card specification document, of an encryption key that may be stored on the HSM is called an Issuer Master Key (IMK). The HSM can then, for example, use the embedded algorithms 204 to create a "diversified key for card verification code creation" (KDcvc3) from the IMK that is used for each individual card that is issued based on a certain algorithm that is also stored in the HSM. The HSM is designed to protect individual encryption keys, and to use embedded encryption algorithms to calculate encryption output based on an encryption input request from an application

system. The encryption algorithm must be located within the HSM because the algorithm must have direct access to the protected encryption keys 203. The application system will provide additional input data to be used in the encryption algorithms to the HSM. The application system will also expect output data from the encryption algorithms from the HSM. The input data to the HSM may be stored in the transaction table 205 and the credential table 206. An HSM is commonly a separate device within the application system that is connected to other devices within the application system through a communication channel. The communication channel may be a network connection such as an RJ45 cable or in some cases is a hardware bus connection such as a PCI connector within a computer casing. An example of using this arrangement may be that the application system contains:

a. Encrypted data (cryptogram)

b. Unpredictable number (UN)

c. Application Transaction Counter (ATC)

d. Transaction data such as a dollar amount

e. A key identifier (but the not key itself)

in its transaction table and credential table. The application system would like to verify encrypted data (a) was created from a particular encryption key (e), unpredictable number (b), ATC (c), and transaction data (d). The application system knows which key was used to create the cryptogram (a), but opts, for security reasons, not to have access to the key itself. The application system then uses the cryptogram (a), unpredictable number (b), ATC (c), transaction data (d), and a key identifier (e) as input for the HSM and sends the input to the HSM. The HSM then uses the input data from the application system and locates the proper encryption algorithm and encryption key to use. The HSM then creates the output response from the algorithm using the encryption key and sends the output to the application system. The output in this example would be a simple "verified" or "not verified" message.

Mastercard, Ex1002, p. 66

[00107] The application system 201 is an embodiment of a "software representation" of a repository of a plurality of secure element representations and has access to all the information that is used to create APDU responses generated by any particular database SE representation in its repository data. This repository data is represented in the credential database table 206. This would include credential data such as PAN, expiration date, card holder name, contactless application type, automated transaction counter, card record, etc. This gives the application system the ability to formulate APDU responses to APDU commands that are issued from the point-of-sale to an SE during an interrogation. So if a mobile device requests a transaction cache for a particular SE or card identified by a card id or PAN, for example, the application system has the ability, using the data in the credential table, transaction table, and HSM, to formulate all the responses that the mobile device may need at a later point in time when the mobile device is being interrogated by the point-of-sale. This set of responses could be in the format of APDU responses and passed to the mobile device to be cached for use later. Alternatively, just the data required for the mobile device to formulate the responses may be passed to the mobile device cache. The application system also may have access to the encryption key for creating cryptograms in the HSM, in which case the keys themselves could be sent to a mobile device to allow the mobile device to calculate a cryptogram that may be requested by a point-of-sale.

[00108] Examples of SE responses are shown in Fig. 3 next to the 'CARD>:' prompt indicating data from the SE to the point-of-sale. The application system may know the specific responses based on a number of factors. In figure 3, the responses are for a PayPass 3.3 MSD transaction, because the application system knows the particular card id or PAN is associated to this PayPass 3.3 MSD transaction, and the PayPass card specification for 3.3 MSD dictates specifically elements 10, 11, and 12 exactly as shown in figure 3, so the response APDU data as shown in 10,11, and 12 can be sent verbatim over a communication channel to the mobile device cache when requested by the mobile device.

[00109] Figure 3, element 13 after the 'CARD>:' prompt shows the format of the read record command response, but the data inside the response may change from one card id or PAN to another because it is credential data that is stored in the read record command

Mastercard, Ex1002, p. 67

response. Fortunately the application system has access to all the credential data that comprises the response to the read record command such as displayed, in part in figure 2, element 7:

a. Track 1 and Track 2 data comprised of PAN, Exp Date, card code, issuer discretionary data

b. Substitution bitmaps for Track 1 and Track 2 (PUNATC, PCVC3)

c. Number of ATC digits used in bitmaps (NATC)

d. Application Version Number

From this data, the application system can create the proper APDU response to the read record command that is formatted just like figure 3, element 13 and send it specifically for the card credential the mobile device has requested to the mobile device for caching over a communication channel. For a MasterCard PayPass MSD v. 3.3 credential, table 2 shows a technical breakdown of how the data in the read record response is formulated from data in the application system in proper APDU response BER-TLV format.

Table 2

70 7F

T	L	V	
9F 6C	02	00 01 -Application Version Number	
56 3E		42 35 34 31 33 31 32 33 34 35 36 37 38 34 38 30 30 5E 53 55 50 50 4C 49 45 44 2F 4E 4F 54 5E 30 39 30 36 31 30 31 33 33 30 30 30 33 33 33 30 30 30 32 32 32 32 32 30 30 30 31 31 31 31 30	Track 1 Data
9F 64	01	03 T1_NATC	
9F 62	06	00 00 00 38 00 00 T1_PCVC3	
9F 63	06	00 00 00 00 E0 E0 T1_PUNATC	
9F 65	02	00 0E T2_PCVC3	
9F 66	02	0E 70 T2_PUNATC	
9F 6B	13	54 13 12 34 56 78 48 00 D0 90 61 01 90 00 99 00 00 00 0F	Track 2 Data
9F 67	01	03 T2_NATC	

90 00

Application Version Number, Track 1 Data, T1_NATC, T1_PCVC3, T1_PUNATC, T2_PCVC3, T2_PUNATC, T2_NATC, and Track 2 Data are all accessible by the application system in the credential table.

[00110] As used herein the term "cryptogram" refers to encrypted data that may or may not be able to be un-encrypted. Encrypted data that cannot be un-encrypted is many times called a "hash." A cryptogram is typically calculated from a series of input data that comprises some data and a cryptographic key, where the cryptographic key is used to encrypt some data. As used herein the term "cryptographic key" refers to a key used, at least in part, to calculate a cryptogram. A cryptogram is calculated based on an algorithm or calculation formula. As use herein the term "calculation formula" refers to an algorithm or formula that is specified by a card specification as the method to calculate a cryptogram. A calculation formula typically may be known by any entity. The output result of the calculation formula that uses the input data and a cryptographic key is a cryptogram. Examples of cryptograms at the time of this filing are defined by the following card specifications in table 4.

Table 4

Card specification	Cryptogram Designator or Name
MasterCard PayPass MSD	CVC3
Visa Contactless MSD	dCVV
Discover ZIP MSD	dCVV
EMV, Visa QVSDC, VISA VSDC, MasterCard MCHIP	AC, TC, AAC, ARQC

A "cryptogram" as used herein may be classified as "dynamic" meaning that it is always changing from one interrogation (transaction) to the next over the life a digital credential (SE representation). As used herein the term "life of", as in, the life of a digital credential, the life of a card, the life of a SE, the life of a SE representation, refers to the life beginning when it is used its first interrogation and ending when it is used in its last interrogation. One indication of this dynamic aspect of a cryptogram is to perform two sequential independent interrogations between a mobile device and a point-of-sale terminal where the same digital credential is used on the mobile device, and the point-of-sale terminal receives two sets of digital credential data with each including a single cryptogram, one with each interrogation. If the cryptogram received by the point-of-sale terminal is different from one interrogation to the next, it is dynamic.

[00111] The details of an interrogation between a point-of-sale and a digital credential, card, SE representation, and mobile device are defined in "card specifications" and implemented in point-of-sale terminals. Examples of these card specifications at the time of this filing are MasterCard PayPass - Mag Stripe v3.3, Contactless EMV, Discover Network RF Contactless Specification – Supplement Guide For Functional Support, AMEX ALIS v1.7, and Visa Contactless Payment Specification v2.0.2. Used herein the term "card specification" refers to a specification or reference within the specification to other specifications and so on that a point-of-sale terminal must adhere to in order to interrogate a

card, SE, mobile device as expected by that card specification. A point-of-sale terminal, as the interrogator, controls the interrogation. The card specification that defines the details of an interrogation may also define the details of a cryptogram request, calculation, and delivery from the card, SE, or mobile device to the point-of-sale as part of the interrogation sequence. Card specifications may include references to other specifications and those other specifications to even more specification wherein the card specification may be defined by the card specification in conjunction with other supporting documents sited within a card specification. Card specifications typically consist of an application layer that defines an interrogation sequence and calculations that are to be performed by both the card, SE, mobile device and also the interrogator or point-of-sale. Both a mobile device and a point-of-sale are expected to be operating under the direction of a card specification during an interrogation.

[00112] The card specification may define a cryptogram to be calculated by the card, SE or mobile device based, at least in part, on unpredictable data sent from the point-of-sale during the interrogation. In this context, it is said that the cryptogram delivered by the mobile device is "expected" because the card specification indicates it will be calculated, at least in part, from the unpredictable data delivered by the point-of-sale during the interrogation and that is what the card specification expects.

[00113] Also, the card specification may define a cryptogram to be calculated by the card, SE, or mobile device based, at least in part, on a cryptographic key, where the cryptographic key is a "permanent cryptographic key". In this context, it is said that the cryptogram delivered by the mobile device is "expected" because the card specification indicates it will be calculated, at least in part, from a permanent cryptographic key and that is what the card specification expects. Used herein the term "permanent cryptographic key" refers to a cryptographic key that is unchanging (or static) throughout the life of a card, SE, mobile device, or digital credential.

[00114] As used herein the term "temporary cryptographic key" refers to a cryptographic key that changes (or is dynamic) from one interrogation to the next over the life of a digital credential (e.g., an SE representation). A temporary cryptographic key may be selected or changed randomly from its use in one interrogation to the next. It is

unpredictable from one interrogation to the next. A temporary cryptographic key may be recorded or stored in assigned to an individual transaction (interrogation) as shown in the "TEMP KEY" column 380 in the transaction table 210. As used herein,if not otherwise explicitly stated, the term "cryptographic key" means a "permanent cryptographic key". As used herein, if not otherwise explicitly stated, the term "encryption key" means a "permanent cryptographic key".

[00115] As used herein the term "persistent" or "persistently stored" refers to of data that are stored in a storage container (such as non-volatile read-only-memory) where the data "persists", and is not erased in the event of a power failure or outage to that storage container. Another example of a persistent storage container is a hard drive, or flash memory.

[00116] Used herein the terms "transient," "transiently stored," "non-persistent," and "non-persistently stored" refers to data that are stored in a storage container where the are erased or otherwise rendered not accessible after a power failure to the storage container. An example of a transient storage container is RAM (Random Access Memory).

[00117] Cryptograms used herein may be "expected" to be calculated, at least in part, from unpredictable data passed from a point-of-sale to a mobile device during an interrogation that is dictated by a card specification. Used herein the term "predetermined cryptogram" refers to a cryptogram that is formulated without the use of unpredictable data passed from the point-of-sale terminal to a mobile device during an interrogation; wherein the interrogation is defined by a card specification; and the card specification indicates the cryptogram to be calculated, at least in part, by the unpredictable data. This may include a predetermined cryptogram being entirely made up of a string of random data. This may also include a predetermined cryptogram being calculated based on other unpredictable data instead of the unpredictable data from the point-of-sale. As used herein "predetermined cryptogram" also refers to a type of unexpected cryptogram.

[00118] Cryptograms used herein are many times may be "expected" to be calculated, at least in part, from a permanent cryptographic key that during an interrogation between a

mobile device and a point-of-sale. Used As used herein the term "unpredictable cryptogram" refers to a cryptogram calculated, at least in part, from a temporary cryptographic key for use in an interrogation between a mobile device and a point-of-sale; wherein the interrogation is defined by a card specification; and the card specification indicates a cryptogram to be calculated, at least in part, by a permanent cryptographic key. As used herein "unpredictable cryptogram" also refers to a type of unexpected cryptogram.

[00119] Used herein the terms "unexpected cryptogram", "unexpected predetermined cryptogram", and "unexpected unpredictable cryptogram" refer to a cryptogram that is sent from a mobile device to a point-of-sale during an interrogation; wherein the interrogation is defined by a card specification implemented on the point-of-sale; and the cryptogram is calculated from a different calculation formula than is defined in the card specification. For example, the "different calculation formula" includes a predetermined cryptogram. As used herein the term "predetermined cryptogram" refers to a cryptogram that is calculated without the use of unpredictable data passed from the point-of-sale terminal to a mobile device during an interrogation; wherein the interrogation is defined by a card specification; and the card specification indicates the cryptogram to be calculated, at least in part, by the unpredictable data. A predetermined cryptogram may be entirely made up of a string of random data. A predetermined cryptogram may also be calculated based on other unpredictable data instead of the unpredictable data from the point-of-sale. As used herein "predetermined cryptogram" is an example of an unexpected cryptogram.

[00120] As a further example, the "different calculation formula" includes an unpredictable cryptogram. As used herein the term "unpredictable cryptogram" refers to a cryptogram calculated, at least in part, from a temporary cryptographic key instead of a permanent cryptographic key for use in an interrogation between a mobile device and a point-of-sale; wherein the interrogation is defined by a card specification; and the card specification indicates a cryptogram to be calculated, at least in part, by a permanent cryptographic key. As used herein "unpredictable cryptogram" is an example of an unexpected cryptogram. An unexpected cryptogram can also be said to deviate from the card specification.

[00121] As a further example, the "different calculation formula" may include using a temporary cryptographic key in place of a permanent cryptographic key in the case of an "unexpected unpredictable cryptogram", or may include using a random value in place of the cryptogram in the case of an "unexpected predetermined cryptogram". As a controlled consequence of the "different calculation formula", the value of the unexpected cryptogram may be different than that of an expected cryptogram; however, it is to be of the same general data format as the expected cryptogram. For example, if the expected cryptogram is 3 bytes long, then the unexpected cryptogram will be 3 bytes long, however the data within the respective cryptograms may not match.

[00122] The response for the compute cryptographic checksum command (figure 3, element 14), is created by a method employed in figures 22, 23, 24, 25, 26, 27, 28, 29 and 30 called "Cryptogram Substitution" using a predetermined cryptogram or unpredictable cryptogram and in some embodiments sent for each transaction to the mobile device cache over a communication channel when requested by the mobile device. In other embodiments cryptogram substitution is used with unexpected cryptograms created on the mobile device and sent to a remote application system. For a MasterCard PayPass MSD v. 3.3 credential, table 3 shows a technical breakdown of how the data in the read compute cryptographic checksum response is formulated from data in the application system in proper APDU response BER-TLV format.

Table 3

77 0F

T	L	V	
9F 61	02	B8 92	T2_CVC3
9F 60	02	FB C7	T1_CVC3
9F 36	02	00 5E	ATC

90 00

The ATC is the automated transaction counter that increments with every point-of-sale interrogation, and can be stored in the transaction table or credential table and updated with each interrogation by a mobile device. The CVC3 is cryptogram that is expected to be calculated with this algorithm from the MasterCard PayPass MSD v3.3 card specification:

First KDcvc3 is created:

Z_L := DES3(IMK_{CVC3})[Y]
Z_R := DES3(IMK_{CVC3})[Y ⊕ ('FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF')]

and define :

KD_{CVC3} := (Z_L || Z_R).

KDcvc3 calculation may be preformed inside the HSM because the HSM contains IMK. The application system will pass Y, which is defined as the PAN and PAN sequence number concatenated as an input to the HSM in conjunction with the IMK id to use. The HSM will respond back with the KDcvc3 as output. The KDcvc3 in this example would be considered a permanent cryptographic key because it will not change over the life of the digital credential, as none of the inputs to the calculation of KDcvc3 change over the life of the credential.

Next T2_IVCVC3 is created:

O :=PayPass- MagStripe(3.3) Annex B alg(KDcvc3)[Track 2 Data]

The least two significant bytes of the output data are defined to be T2_IVCVC3.

Finally, the CVC3 cryptogram for track 2 is calculated:

O := DES3(KD_{CVC3})[T2_IVcvc3 || UN || ATC]

The least two significant bytes of the output data are defined to be CVC3

CVC3 calculation may be preformed inside the HSM because the HSM contains the IMK which is used to create KDcvc3, which is used to create IVCVC and CVC3. So the application system will pass UN and ATC as inputs in conjunction with the IMK id to use. The HSM will respond back with the CVC3 cryptogram as output. The CVC3 is a dynamic cryptogram as the input to the calculation of the cryptogram change with each interrogation.

Mastercard, Ex1002, p. 75

This is known because with each interrogation the digital credential is expected to increment the ATC (Automated Transaction Counter) and also have different UN value.

[00123] This card specification expects KDcvc3 cryptographic key to be a permanent cryptographic key. In the event that an unpredictable cryptogram is to be calculated instead, in this example, the permanent key of KDcvc3 is not used and is replaced by a temporary cryptographic key that may consist of a random value that changes, and may be erased or altered after a single interrogation. The temporary cryptographic key that is used can be recorded in the application system transaction table for future reference during cryptogram verification. Proceding with the following formula using the termperary cryptographic key instead of the permanent cryptographic key will yield an unpredictable cryptogram.

[00124] The UN input value in this algorithm is intended (expected) to be an unpredictable number from the point-of-sale that was acquired during interrogation. In order to calculate an unexpected predetermined cryptogram instead, in one embodiment this UN number will be created randomly and used as input to the cryptogram algorithm. The UN number used will be recorded in the application system transaction table for future reference during cryptogram verification. The predetermined cryptogram can now be used to formulate a response to the "compute cryptographic checksum" request without consulting the application system during the interrogation. In this embodiment, the mobile device may share access to the predetermined cryptogram during the scope of the authorization process.

[00125] In another embodiment of substituting a predetermined cryptogram, random data could simply be used to create the predetermined cryptogram. In this embodiment, the mobile device may share access to the predetermined cryptogram during the scope of the authorization process.

[00126] In another embodiment of substituting an unpredictable cryptogram, a temporary cryptographic key could be used to allow the mobile device to calculate and create the unpredictable cryptogram. The temporary cryptographic key would be recorded in the application system transaction table for future reference during cryptogram verification. In

this embodiment, the mobile device may share access to the temporary cryptographic key with the application system during the scope of the authorization process.

[00127] Alternatively, although less secure, in another embodiment of the application system could deliver the permanent cryptographic key to the mobile device to be stored transiently to allow the mobile device to calculate and create an expected cryptogram that can be used to formulate the "compute cryptographic checksum" response without consulting the application system.

[00128] The concept of transaction (command/response) caching is disclosed herein. A cache is a component that transparently stores data so that future requests for that data may be served faster. The data that are stored within a cache may be values that have been computed earlier or duplicates of original values that are stored elsewhere. If requested data are contained in the cache ("cache hit"), this request may be served by simply reading the local cache, which is comparatively faster that accessing the remote source. Otherwise ("cache miss"), the data have to be recomputed or fetched from its original storage location, which is comparatively slower. Hence, the more requests that may be served from the local cache, the faster will be the overall system performance. Caching implies that the cache values may be temporary and the original values from the remote source can be easily accessible time after time if needed in order to update, or replace the cached values. Used herein the term "non-persistent cache" and "transient cache" refers to the cached data to be transient or non-persistent. Unless otherwise stated the term "cache" also refers to the cached data to be transient or non-persistent.

[00129] The mobile device cache is setup to hold the cached data in preparation for the next interrogation from the point-of-sale that will happen at a later time. It is important to note that the data transmitted to the mobile device cache may hold the literal APDU formatted data, or may simply hold the data required to formulate a correctly formatted APDU response. The important aspect is that the cache holds all the data required to properly create APDU responses to the APDU commands.

[00130] Used herein the term "card data" or "credential data" may refer to the data used to create a proper APDU response to credential specific APDU commands such "read record" 7, and data used in "compute cryptographic checksum" 8. It is common for an application system in a software representation of a plurality of remote secure element repository to have access to all the data to properly create a valid APDU response.

[00131] Fig. 16 illustrates a caching system for each transaction or interrogation between a point-of-sale 778 and a mobile device 779 for a MasterCard PayPass transaction. The advantage of caching secure element responses is to lessen the effect of network latency and speed up an interrogation. In the example contained Fig. 16, network latency is reduced from a potential 800ms to a potential 200ms because of the caching technique applied. This is a significant effect in the application of NFC or RFID because the as the total interrogation timeframe shrinks, the likelihood of a successful interrogation sequence goes up because it is less likely the communication channel between the point-of-sale and the mobile device will be interrupted from the mobile device moving out of the field generated by the point-of-sale. Notice that not all interrogation command and responses 787 and 793 in Fig. 16 are handled from the mobile device cache 780. The non-cached command and response, lead to the 200ms network latency of the entire transaction in figure 16.

[00132] Fig. 17 illustrates a caching system for each transaction or interrogation between a point-of-sale 794 and a mobile device 795 for a Visa PayWave transaction. In this figure the concept of 100% transaction caching is employed. It illustrates how all of the responses for an interrogation from a point-of-sale may be cached at some point of time ahead 802 of the actual mobile device and point-of-sale interrogation. This causes network latency of the interrogation to be 0ms (zero) because no data is queried during the interrogation over the network from the remote system auth server's remote repository. This is a tremendous advantage over the system in Fig. 16, which in-turn had a tremendous advantage to the system that does not employ transaction caching at all.

[00133] Depending on the interrogation sequence selected by the point-of-sale, it may not always be possible to implement a system set forth in Fig. 17. Many point-of-sale

interrogation sequences carried out at the time of this filing are based on card specifications such as:

a. MasterCard, PayPass, MChip

b. American Express, Express Pay

c. Discover Zip

d. Visa QVSDC, VSDC

e. Contactless EMV

Employ a method of creating an expected cryptogram by the mobile device that is calculated, at least in part, from unpredictable data generated on the point-of-sale and delivered to the mobile device during the interrogation sequence. Because creating an expected cryptogram requires a calculation to be preformed that includes a permanent cryptographic key, the secure element or system with access to this key must be used to carry out the expected cryptogram calculation. Because the secure element representation is stored in a remote repository and contains the permanent cryptographic key, this expected cryptogram calculation would incur network latency to perform the calculation during the interrogation, as shown in figure 16, element 793.

[00134] During point-of-sale interrogation with a mobile device, the point-of-sale may request a cryptogram and supply some data to be used in cryptogram calculation to the mobile device in the same APDU command request. The APDU response to this request by the mobile device, which is also in the same interrogation sequence, is expected to contain the cryptogram itself, calculated, at least in part, using the input data from the point-of-sale, and also other input data. After receiving the cryptogram in the APDU response from the mobile device, the point-of-sale then sends the cryptogram, the input data it used to request the cryptogram, and possibly other information about the credential data from the mobile device to a remote processor for an authorization request. As part of the authorization

request process, the cryptogram is verified based on the input data that was used to create it, some of which was generated by the point-of-sale.

[00135] Because many of these cryptograms referenced by external card specifications use transaction data or unpredictable number data created by the point-of-sale as part of the input during the calculation of the expected cryptogram, the step of calculating the cryptogram requires the secure element at the time of interrogation because the secure element contains the permanent cryptographic key required to create the cryptogram. If the secure element is contained in a remote repository, network latency must be factored into the total interrogation time in order for the secure element to calculate the cryptogram using data from the point-of-sale.

[00136] If data created by the point-of-sale is not part of the input to the creation of the expected cryptogram, such as in Visa Contactless MSD cryptogram (dCVV), then the cryptogram can be calculated by the remote repository, transferred to the mobile device, and cached for use at a later time during point-of-sale interrogation. This scenario creates no network latency and allows for one hundred percent transaction caching during the interrogation, because the secure element representation need not be accessed during the actual interrogation time. Used herein the term "one hundred percent (100%) transaction caching" refers to the ability for the mobile device to complete the interrogation with a point-of-sale terminal without the requirement to contact the secure element during the interrogation, and instead have all the data on hand local to the mobile device to complete the interrogation.

[00137] Most cryptogram algorithms referenced by external card specifications require input data from the point-of-sale during the interrogation, so many of the following figures address this problem and how it can be solved in the context of one hundred percent transaction caching. The method of "Cryptogram Substitution" and creating a pre-defined cryptogram are defined and described in the figures 21, 22, 23, 24, 25, 26, 27, 28, 29, and 30 explain a solution to the problem of creating a response to a cryptogram request the expected cryptogram is calculated, at least in part, by unpredictable data sent by the point-of-sale to the mobile device.

[00138] Fig. 22 illustrates how one embodiment of an application system could create cryptograms using random, predetermined, or "made up" input data. A transaction table 210 is defined in which each row represents a transaction between a mobile device and a point-of-sale. The state of the data in this table currently shows transaction data that have been delivered to a mobile device cache, but have not been verified through a point-of-sale. In order to comply with the request of a point-of-sale to a mobile device during an interrogation, the mobile device must deliver cryptogram in the proper data format that the point-of-sale expects. The data that is contained in the actual cryptogram that is delivered to the point-of-sale from the mobile device may not be accurately calculated with the input data from the point-of-sale, but it does not matter at this point as the point-of-sale alone does not verify the cryptogram, it simply receives the cryptogram and relays it for verification to the application system, which has access to the input data used to create the original pre-determined cryptogram. This is why the predetermined cryptogram 218 can may be calculated based on randomly selected terminal input data UN 213, and Transaction Data 215. The other inputs to create the predetermined cryptogram are based on credential data of each secure element such as the Application Transaction Counter 214, the Issuer Master Key id 212, and the account Personal Account Number 211. After gathering all predetermined cryptogram input data, the application system sends the input to the HSM and receives the predetermined cryptogram as an output response. The application system may optionally store the predetermined cryptogram 218 into the table 210, for use during verification later.

[00139] The actual unpredictable number 216 and transaction data 217 sent by the point-of-sale terminal during interrogation is not known at this point in time because the interrogation has not actually happened yet. However, it is still possible to create a predetermined cryptogram, in this manner, to be delivered to a mobile device for use in a mobile device cache to use during a point-of-sale interrogation that includes a properly formatted predetermined cryptogram. This predetermined cryptogram is formatted properly, but will not be calculated based on the input data from the point-of-sale interrogation. Because it is formatted properly, it will still be accepted by the point-of-sale and sent to off for verification in an authorization request. Also note that there may be multiple transactions in processing at a single point of time, 219 shows two different rows representing two

different transactions currently being processed for the same PAN 211. The application system has the ability to process each of the transactions independently because there is a row in the table to discern each one separately.

[00140] Note that because the same application system that is creating the cryptogram will also be verifying the same cryptogram, another embodiment of predetermined cryptogram creation is simply make up a predetermined cryptogram from random data without performing a calculation from input data at all. This embodiment requires the application system to store the random predetermined cryptogram 218 into the table 210 for verification later. This embodiment also does not require an HSM to create the cryptogram as it is simply created randomly.

[00141] Note that in another embodiment, it is possible to create a temporary cryptographic key for each transaction. This key may be shared with the mobile device allowing the mobile device to calculate an unpredictable cryptogram using, at least in part, the unpredictable data received from the point-of-sale during the interrogation. This embodiment requires the application system to store the temporary key 380 into table 210 for use during unpredictable cryptogram verification later.

[00142] These methods of substituting a predetermined cryptogram and of substituting an unpredictable cryptogram are vital to the concept of 100% transaction caching with the existing point-of-sale infrastructure. The existing point-of-sale infrastructure is pre-set for each interrogation sequence and expects data to be formatted according to each interrogation sequence that is programmed in the point-of-sale. Changing the interrogation sequence(s) is out of the control of the mobile device, and so this method of creating a predetermined cryptogram or unpredictable cryptogram as defined using data, at least in part, from Fig. 22 may be required for 100% transaction caching which creates no network latency during the interrogation between the point-of-sale and the mobile device. Because the predetermined cryptogram is created without input from the point-of-sale, the calculation time to create a predetermined cryptogram may also removed from the overall interrogation time. In the case of an unpredictable cryptogram, this calculation time persists and cannot be removed from the overall interrogation time.

[00143] Fig. 29 illustrates a representation of a table of digital credentials 350 (digital credential data) that may be stored inside the application system. This table, in conjunction with the transaction table, and in some embodiements the HSM allows the application system to perform as a repository of a plurality of secure element software representations. The credential data used to create data inside an SE and also allow it to formulate its proper APDU responses is contained in this table for a plurality of credentials (SEs). For a MasterCard PayPass MSD v3.3 credential, the example shown in this table, the columns of data list personal account number (PAN) 351, expiration date 352, name of card holder 353, card code 354, track 1 data 355, track 2 data 356, track 1 cvc3 bitmap 357, track 2 cvc3 bitmap 358, track 1 UN and ATC bitmaps 359, track 2 UN and ATC bitmaps 360, track 1 number of ATC digits 361, track 2 number of ATC digits 362, CVM list 363, AC 364, application version number 365, and the master key identifier 366.

[00144] Fig. 23 illustrates a method for a mobile device 220 to request a transaction cache 224 prior to being interrogated by a point-of-sale. Used herein the term "transaction cache" refers to data required to formulate proper mobile device responses during an interrogation with a point-of-sale, which may comprise digital credential data. As discussed in figure 17 and figure 18, figure 23 is very similar and describes a method for a mobile device 220 to receive a cache of transaction data (transaction cache) 227 over a communication channel to be used during a point-of-sale interrogation at a later point in time. Before an interrogation with a point-of-sale, the mobile device will request a transaction cache to be used during the point-of-sale interrogation from the application system 222 over a communication channel. This transaction cache data may comprise the randomly generated unpredictable data such as UN and transaction data from the application system, the other credential based inputs 225 to cryptogram calculation and sends them to the HSM 223 over a communication channel. The HSM then may calculate the predetermined cryptogram 226 and return it to the application system. The predetermined cryptogram may then be used to formulate the cache response to a "request cryptogram" APDU command from a point-of-sale. In a further embodiment, the application system could avoid the step of contacting the HSM and simply make up a random sequence of bytes to be used as a predetermined cryptogram to be used in place of the expected cryptogram. This

predetermined cryptogram is a sequence of random data and is shared with the mobile device, so the mobile device could have, just as well, created the random bytes as the predetermined cryptogram and shared them with the application system. In a further embodiment, the application system could avoid the step of contacting the HSM and simply make up a temporary cryptographic key from a random sequence of bytes to be shared with and used by the mobile device while creating an unpredictable cryptogram to be used in place of the expected cryptogram. This temporary cryptographic key is a sequence of random data and is shared with the mobile device, so the mobile device could have, just as well, created the random bytes as the temporary cryptographic key and shared them with the application system.

[00145] For an example, the MasterCard PayPass interrogation from the point of sale incorporates an APDU command request called "compute cryptographic checksum" 14 as seen in figure 3. The command APDU follows a particular format and may look like this:

80 2A 8E 80 04 00 00 08 99 00

The digits 00 00 08 99 in the APDU command above from the point-of-sale indicate the unpredictable number to be used as an expected cryptogram calculation input. This unpredictable number is a random sequence of numbers that changes with each interrogation the point-of-sale initiates. The format of this APDU command request is discussed in more detail inside the MasterCard PayPass MSD v3.3 card specification. The immediate APDU response from the mobile device is expected to follow a particular format and may look like this:

77 0F 9F 61 02 B8 92 9F 60 02 FB C7 9F 36 02 00 5E 90 00

The digits B8 92 represent the cryptogram. It is identified by the preceding BER-TLV formatted tag 9F 61 (track 2 CVC3), and length value of 02. It was expected to have been calculated from the unpredictable number issued by the preceding point-of-sale APDU command request in combination with other inputs such as the ATC. A correct expected cryptogram must be calculated using the permanent cryptographic key that is securely stored inside the SE. Because figure 23 implements 100% transaction caching, it is not impossible

for the expected cryptogram to be calculated after receiving the unpredictable number from the point-of-sale, because in that event, the mobile device would need to access the network to contact the remote repository as in figure 16, elements 787 and 793 in order to perform the expected cryptogram calculation. The method of substituting a predetermining a cryptogram, or an unpredictable cryptogram in place of the expected cryptogram, in this case, needs to be applied in order to create this response. With this method applied, the "compute cryptographic checksum" response from the mobile device can be successfully delivered interrogation with the point-of-sale without contacting the remote SE representation during the interrogation. In this case, the cached response may look like this instead:

77 0F 9F 61 02 A4 56 9F 60 02 FB C7 9F 36 02 00 5E 90 00

Where, in one embodiment, the digits A4 56 is the predetermined cryptogram, and NOT calculated using, at least in part, the expected unpredictable number from point-of-sale. Where, in another embodiment, the digits A4 56 is the unpredictable cryptogram, and NOT calculated, at least in part, using the expected permanent cryptographic key rather using a temporary cryptographic. This is an example of "Cryptogram Substitution" technique. The point-of-sale does not have the means or keys to check the received cryptogram for correctness, so it will accept the cryptogram answer because it is of the proper format. The point-of-sale will rely on the authorization request later to verify the correctness of the cryptogram.

[00146] In this manner, with some embodiments the entire transaction cache data comprising elements that make up the response to "compute cryptographic checksum" 227 may be returned to the mobile device from the application system over a communication channel prior to point-of-sale interrogation. The transaction cache can be used during interrogation from a point-of-sale to successfully cache the responses to 100% of the interrogation requests without requiring network access to the remote repository and SE during the complete interrogation time. Please also note that the data supplied in the transaction cache response 227 may be literally APDU formatted responses. It may also simply contain all the data required to formulate proper APDU responses without requesting more information from the application system during interrogation time. In this case the

mobile device must employ some logic to properly formulate the APDU responses. This logic may also be delivered with transaction cache data 227.

[00147] From time to time, such as during a contactless EMV interrogation sequence from the point-of-sale, the point-of-sale may request one of a plurality of cryptograms. In this case, the response to more than one cryptogram type request must be delivered in the transaction cache response 227 over a communication channel. In this case, the mobile device must employ some logic as to which cryptogram response is being requested and direct the mobile device cache appropriately to deliver the correct cryptogram response. This logic may also be delivered with transaction cache data 227.

[00148] Also, from time to time, such as during a contactless EMV interrogation sequence, a response during the interrogation with the point-of-sale based on "card risk management" decisions may be implemented. Card risk management is described by the card having enough logic and information about the transaction at the point-of-sale to approve or decline the transaction without consulting an application system or remote processing server. An example of performing card risk management logic using unpredictable data is:

A point-of-sale interrogates a secure element or mobile device and during the process, it indicates to the mobile device it will not be forwarding credential data immediately for authorization of a transaction. This is sometimes called an "offline transaction". At that point during the interrogation, the point-of-sale sends the mobile device unpredictable data, such as a transaction amount that is a portion of the unpredictable data, and requests an approval cryptogram from the SE or mobile device. The SE or mobile device has the ability at that point to make "card risk management" decision as to accept or decline the transaction based on the transaction amount. If the transaction amount is above a "ceiling limit" it may opt to decline the transaction.

The response from a mobile device to a point-of-sale that indicates the decision it has made regarding the card risk management logic is typically formulated with a cryptogram wherein the cryptogram calculation formula is different depending on the type of response to the

point-of-sale. So "declining" message from the mobile device may include a different cryptogram that was calculated by a different calculation formula than the cryptogram that is designated for an "approved" message. The card specification will define the different calculation formulas

[00149] Element 227, in addition to delivering transaction cache information, may also contain logic and data to make decisions regarding card risk management during the interrogation with the point-of-sale.

[00150] Element 227, although it may be less secure, in another embodiment could contain the permanent cryptographic key that is used to create an expected cryptogram.

[00151] Element 227 in a further embodiment could contain a temporary cryptographic key that is used to create an unpredictable cryptogram.

[00152] Element 227 could also contain data required to be used with the encryption key to create the cryptogram such as ATC. This would allow the mobile device to create a cryptogram without consulting the application system and effectively cache a response to a cryptogram request from a point-of-sale during an interrogation. Sharing the permanent cryptographic key with the mobile device would be an alternative to using a predetermined cryptogram to achieve a similar system performance result with the context of 100% transaction caching. Also sharing a temporary cryptographic key with the mobile device wherein the mobile device calculates an unpredictable cryptogram would be an alternative to using a predetermined cryptogram to achieve a similar system performance result with the context of 100% transaction caching. During an authorization step, the verification of correctness method that pertains to the mobile device calculated cryptogram and unpredictable cryptogram compared to a predetermined cryptogram may be different as the mobile device may use the unpredictable data passed from the point-of-sale in the cryptogram calculation. The mobile device may store the transaction cache data and card risk management logic securely in a mobile device cache 221 which can be non-persistent memory or RAM, or possibly encrypted memory.

[00153] Fig. 24 illustrates an interrogation between a point of sale 230 and mobile device 231 sometime after the mobile device has received the mobile device cache data 227 from the application system 222. This interrogation may be carried out over near field communication (NFC) on both the point-of-sale and mobile device. The data protocol layer within this interrogation may be configured for ISO7816-4 and follow APDU command and response formats. Figure 24 is very similar to the lower half of figure 16, with the exception of cryptogram request 239 and response 241 on figure 24 and 787 and 792 of figure 16. The APDU response in figure 24, element 241 is formulated as a response from the mobile device using the mobile device cache 232 and contains a predetermined cryptogram or an unpredictable cryptogram. Both unpredictable number (UN) and transaction data from the point-of-sale terminal passed to the mobile device 239 are not actively used to create the predetermined cryptogram response 241, however, they are used to create an unpredictable cryptogram response. They are both kept by the mobile device 240 to be transmitted to the application system later over a communication channel. If there are card risk management tests to be performed to determine which predetermined cryptogram or unpredictable cryptogram response 241 is used, they are performed by the mobile device at this time 242. Prior to the cryptogram request 239, the interrogation sequence from the point-of-sale may contain additional requests such as select payment card application 233, which is followed by a response 234 from the mobile device cache, GPO request 235, which is followed by a response 236 from the mobile device cache, and read record request 237, which is followed by a response 238 from the mobile device cache.

[00154] Fig. 25 illustrates an authorization request after an interrogation between a mobile device and a point-of-sale has been preformed, such as in fig. 24. Typically the point-of-sale 255 will formulate an authorization request which may be in the form of ISO8583 format. This format will contain data that pertains to the interrogation such as the cryptogram received from the mobile device, the unpredictable number and transaction data passed to the mobile device for cryptogram calculation, and other credential data. The authorization request will be passed to the application system 251 over a communication channel 252. This communication channel may not go directly to the application system, but may go first to an acquiring gateway, then to an issuing processor, and eventually to the

application system 251. This communication channel may be referred to herein as "the interchange". The interchange is a private network that is used exclusively by the payment card industry for the purpose of authorization requests. After the authorization request is received by the application system, the authorization request may be matched to a particular transaction that is listed in the transaction table 210 based on the PAN 211 that is listed in the credential data of the authorization request. The application system will make the authorization decision for the authorization request.

[00155] The application system has access to the HSM 250 as well as the transaction table 253 that is also shown in figure 22, element 210. It may contain the original randomly created UN 213 and transaction data 215 used to create the predetermined cryptogram. It may contain the predetermined cryptogram. It may also contain a temporary cryptographic key that allows the mobile device to create an unpredictable cryptogram. The cryptogram that was received over the interchange communication channel 252 may be a predetermined cryptogram that may have been originally delivered to the mobile device in the response to a request for transaction cache data (figure 23, element 227). The cryptogram that was received over the interchange communication channel 252 may also be an unpredictable cryptogram that was created by the mobile device using a temporary cryptographic key.

[00156] In parallel to the data being sent from the point-of-sale to the application system, the mobile device 256, after the interrogation, sends the unpredictable number and transaction data it received from the point-of-sale terminal, the results from the card risk management tests over a separate communication channel 254 to the application system. This separate communication channel may be internet communication over a mobile network. This data from the mobile device was acquired from the point-of-sale and kept by the mobile device as shown in figure 24, elements 240 and 242, but may not have been used in the calculation of the cryptogram passed in figure 24 element 241. This data, which is sent to the application system by the mobile device 254 may be used to compare and corroboratively verify unpredictable number and transaction data that was separately sent by the point-of-sale 252. The unpredictable number and transaction data reported from the point-of-sale should match the reported unpredictable number and transaction data from the

mobile device. Using the term "corroboratively" herein refers to verifying unpredictable data delivered by two separate communication channels.

[00157] An added security measure may be implemented that pertains to the data sent from the mobile device to the application system over the communication channel 254. Prior to sending the data, if the data contains transactional amount data for example: "$16.24 USD", that data may be presented to the mobile device display screen 371 from for card holder validation like this:

a. "Do you authorize this $16.24 USD purchase?"

The card holder may be asked to review and validate the transaction amount by touching the screen 371 or pressing a button 372 for approval. After this card holder approval process, the mobile device may make a decision to send or not send the transactional data, or simply send an "authorization failure" message to the application system, if the transaction amount is not validated on the mobile device by the card holder.

[00158] Fig. 26 illustrates the transaction table 262 that is also shown in figure 25, element 253 and figure 22, element 210. The state of the transaction table in figure 26 represents that of after a transaction interrogation has been preformed and after the application system has received data from the mobile device as in figure 25, element 254. The example of the data received is shown for the unpredictable number from the terminal 260 and the transaction data 261. Both of these numbers may be used to verify an authorization request shown in figure 25, element 252, as they could be compared and match that of the authorization request. These numbers also may be used as placeholders to identify that a system authorization is complete.

[00159] Fig. 27 illustrates how the application system 270 may make an authorization decision regarding a particular transaction such as that listed in figure 26. In one embodiment shown in figure 27, a method of verifying a predetermined cryptogram 278 is shown. The data from a row in the transaction list table 262 in figure 26, which matches element 272 in figure 27, in addition to the cryptogram and PAN passed to the application system 271 by the point-of-sale over a communication channel, may be used to create the

input to the "verify cryptogram" request 273. The HSM 275 may then use a particular key that is kept securely inside it to calculate a cryptogram based on the algorithm supplied by the applicable card specification and see if it matches the one passed in 273. Depending on the status of this match, a response is issued back to the application system that indicates "approved" or "denied". Notice that the UN and transaction data from the point-of-sale 276 is NOT used in cryptogram verification, and instead is substituted with the UN 213 and transaction data 215 that was previously created and stored in the application system. In a typical scenario, this is unexpected as the card specification for creating the cryptogram expects the cryptogram to be calculated, at least in part, from the UN and transaction data selected by the point-of-sale 276. Because our application system, prior to the interrogation with the point-of-sale, predetermined these values for unpredictable number and transaction data in order to calculate a predetermined cryptogram, the values in 276 can be ignored for the cryptogram verification process and substituted with the application system values. The emphasis about this figure and how it relates to the verification of a cryptogram is that the input data, at least in part, to the cryptogram verification is NOT the unpredictable number and transaction data passed from the point-of-sale 276 over a communication channel, but instead the randomly generated values that were previously selected and stored in a transaction table are used 272. The unpredictable number and transaction data that was generated by the point-of-sale terminal 276 is never actively used to create or verify the cryptogram, but may be used to match with a reported response from the mobile device 277 after the interrogation as an additional verification method.

[00160] In a further embodiment that is not shown but relates to figure 27, if a predetermined cryptogram is used that is comprised of random data and not calculated using a cryptographic key, the application system may verify a cryptogram by simply comparing the cryptogram received from the point-of-sale with a reference to a predetermined cryptogram that is kept in the application system.

[00161] In a further embodiment shown in figure 27, a method of verifying an unpredictable cryptogram 279 is shown. For the verification process 279, the application system would verify the cryptogram from the point-of-sale using the temporary

cryptographic key that was assigned to the transaction as seen in table 210, element 380. The temporary key was used by the mobile device to create the unpredictable cryptogram that was sent from the point-of-sale. The inputs for the calculation 391 comprise data from the application system 390 and inputs from the point-of-sale 393. The inputs from the application system may comprise a temporary cryptographic key, and an application transaction counter. The inputs from the point-of-sale may comprise a cryptogram, a PAN, a UN, a transaction data. The application system may then follow the expected algorithm supplied in the card specification for verifying an expected cryptogram with the exception of substituting the expected permanent cryptographic key with the temporary cryptographic key. Notice in this embodiment a permanent cryptographic key is never used for cryptogram verification. Notice the UN and transactional data from the mobile device 392 may not be used for cryptogram verification.

[00162] Fig. 28 illustrates an overview of the authorization of a transaction process comprising a method for substituting an expected cryptogram with a predetermined cryptogram or unpredictable cryptogram. Fig. 28 also illustrates an overview of the authorization of a transaction process comprising a method of authorization using an expected cryptogram. Fig. 28, for all embodiments, employs the concept of the mobile device without having local access to a permanent cryptographic key that is expected to be used to create an expected cryptogram. Fig. 21, 22, 23, 24, 25, 26, 27, 29, and 30 all have a part of this process. Fig. 21 illustrates a repository of a plurality of secure element software representations. Fig. 22, 23 and 29 illustrate how the mobile device shares data with an application system over a communication channel. Fig. 24 illustrates interrogation between a point-of-sale and mobile device. Fig. 25, 26 and 27 illustrate the authorization process after an interrogation is completed. Fig. 30 illustrates a mobile device that comprises one embodiment of corroborative authorization that displays the transaction amount data for manual verification by a card holder.

[00163] In Fig. 28, a mobile device first requests transaction cache information from an application system 280 over a communication channel. The application system may have created or creates at that time random data such as unpredictable number and transaction data

that is required to calculate a predetermined cryptogram 281. This random data is similar in format to that of which the point-of-sale would generate at the time of interrogation with the mobile device. The application system keeps this data for later, and shares a predetermined cryptogram with the mobile device 282.

[00164] As an alternative to the method of 280, 281, 282, and 283, one embodiment may comprise the application system and the mobile device simply sharing a random sequence of data that represents a predetermined cryptogram. This is possible because the application system is the only entity that both creates and verifies the predetermined cryptogram.

[00165] As a further alternative to the method of 280, 281, 282, and 283, a further embodiment may comprise the application system and mobile device sharing a temporary cryptographic key that the mobile devices will use to create an unpredictable cryptogram.

[00166] As a further alternative to the method of 280, 281, 282, and 283, a further embodiment, although less secure, comprises the application system sending the permanent cryptographic key needed to create an expected cryptogram to the mobile device to be stored transiently; the mobile device would then have the capability to calculate the expected cryptogram locally when receiving a request for an expected cryptogram from the point-of-sale.

[00167] Data may be delivered to the mobile device 283 that comprises, for example, card risk management logic, information needed to respond to "select AID", "get processing options", "read record", and "compute cryptographic checksum" APDU requests during interrogation 282.

[00168] The mobile device receives the transaction caching data information over a communication channel and keeps it for use in the next point-of-sale interrogation 283.

[00169] As used herein "sending data" from one entity to another such as a mobile device to a remote application system or vise versa should be taken to mean sending the data from one location to another wherein the receiving entity may receive the data as a duplicate

from the sending entity or receive the data in parts in addition to receiving information about the data that would enable the receiving entity to reconstruct the original data that was sent from the sending entity.

[00170] A point-of-sale performs an interrogation 284 with the mobile device, the mobile device has a cache prepared to answer the point-of-sale APDU requests over its NFC interface. As part of the interrogation, the mobile device receives a request to calculate an expected cryptogram using, at least in part, the unpredictable data sent by the point-of-sale such as an unpredictable number and transaction data.

[00171] In one embodiment of the interrogation 284, the mobile device saves, but does not use this unpredictable data from the point-of-sale 290, and instead delivers a response APDU that contains the predetermined cryptogram that is in the mobile device cache 291. The interrogation is completed. In this embodiment, element 399 is not used.

[00172] In a further embodiment of the interrogation 284, the mobile device creates an unpredictable cryptogram calculated from a temporary cryptographic key and, at least in part, the unpredictable data from the point-of-sale 399. In this embodiment, elements 290 and 291 are not used.

[00173] In a further embodiment of the interrogation 284, the mobile device creates an expected cryptogram calculation from a permanent cryptographic key transiently stored on the mobile device; and, at least in part, the unpredictable data from the point-of-sale. In this embodiment, elements 290, 291, and 399 are not used.

[00174] Then, in parallel, the point-of-sale sends data it had acquired from the mobile device during the interrogation, such as the expected cryptogram, predetermined cryptogram or unpredictable cryptogram, and ATC, in addition to details about the transaction to the application system over a communication channel 285; and the mobile device sends, over a separate communication channel, information it had acquired from the interrogation with the point-of-sale such as unpredictable number and transaction data to the application system 286.

[00175] It is possible, at this point, for an added "card holder verification" step if transactional data such as transactional dollar amount is delivered to the mobile device from the point-of-sale during the interrogation. The card holder that is using the mobile device may be asked to verify a purchase amount displayed on the mobile device display screen 371 prior to the mobile device sending the data to the application system over the seperate communication channel.

[00176] The application system then uses the data from the point-of-sale, and optionally from the mobile device, to verify and authorize the transaction 287.

[00177] The application system may identify a particular transaction from a transaction table 210 as a transaction using a predetermined cryptogram, unpredictable cryptogram, or an expected cryptogram and proceed with the appropriate verification technique.

[00178] The application system may have to compare the unpredictable data sent from the point-of-sale and the unpredictable data sent from the mobile device to corroborate the transaction as an added corroborative verification method 289.

[00179] In one embodiment, the application system may verify the predetermined cryptogram with an HSM by using the previously randomly selected unpredictable number 213 and transaction data 215 as part of the input data as a substitute for the unpredictable number and transaction data sent to the application system by the point-of-sale.

[00180] In a further embodiment, the verification process could be a simple comparison between the predetermined cryptogram delivered to the mobile device (figure 23, elements 226, 227) and the predetermined cryptogram received from the point-of-sale (figure 25, element 252).

[00181] In a further embodiment, the verification process could be verification of an unpredictable cryptogram using a temporary cryptographic key assigned to the transaction in the transaction table to calculate and verify the unpredictable crytptogram.

[00182] In a further embodiment, the verification process is the verification of an expected cryptogram using an HSM that contains a permanent cryptographic key.

[00183] If the cryptogram is verified 289, authorization is considered successful, otherwise, it has failed.

[00184] Fig. 30 illustrates a mobile device. The mobile device screen 371 is contained within the body of the mobile device 370 and can be configured to display text or graphics. An input button 372 to the mobile device can be used to manually submit input to the mobile device.

[00185] Figures 21, 22, 23, 24, 25, 26, 27, 28, 29, 30 comprise the method of cryptogram substitution where an expected cryptogram is substituted by either a predetermined cryptogram or an unpredictable cryptogram. The method using an application system that may contain an HSM as a repository for software secure element representations. It is important to note that a cryptogram in these figures may be calculated by using a HSM that securely houses keys used to create a cryptogram. Because the application system, however, is the only entity trusted to both create and verify the cryptogram, the cryptogram that is substituted could effectively be made up of completely random data without the use of an HSM, or created from a temporary cryptographic key assigned to each transaction.

[00186] Used herein the term "interrogation" or "interrogation sequence" refers to all the APDU command requests and APDU responses between a mobile device and a point-of-sale using RFID (NFC) required to deliver a complete credential for authorizing a financial transaction to a point-of-sale as defined by a card specification. Typically, an NFC interrogation does not span multiple NFC field entrances and exits. Typically the beginning of an interrogation starts when a mobile device enters the NFC field of a point-of-sale and ends at least prior to when the mobile device exits the NFC field.

[00187] An interrogation sequence is can be entirely defined by a card specification and an interrogation is expected to gather all the digital credential data required from the mobile device in order to authorize a financial transaction. The timing of an interrogation or interrogation sequence may also be defined by a card specification. As used herein an

interrogation ad heirs to the timing requirement that indicates a maximum interrogation time as specified in the card specification. Maximum interrogation time the time required to complete the entire interrogation. If the card specification does not contain timing requirements that define a maximum interrogation time, the maximum interrogation time is one second as used herein. A "fast interrogation" as used herein refers to an interrogation wherein the maximum interrogation time is to be less than 250 milliseconds. A "super fast interrogation" as used herein refers to an interrogation wherein the maximum interrogation time is to be less than 150ms. An "ultra fast interrogation" as used herein refers to an interrogation wherein the maximum interrogation time is to be less than 100ms. An "efficient interrogation" as used herein refers to an interrogation wherein the total interrogation time does not comprise system latency time, wherein system latency time is incurred by sending or receiving data to or from a remote source from a mobile device during the interrogation.

[00188] The term transaction as in "100% transaction caching" and other uses, based on context, may be used as a synonym for interrogation or interrogation sequence. Examples of an interrogation and interrogation data are shown in figures 1, 2, and 3.

[00189] An interrogation can be considered time sensitive as the likely hood of a successful interrogation sequence greatly increases the shorter it is. This is a property of proximate nature of NFC. It is simply hard to "hover" a mobile device in an NFC field for any long length of time.

[00190] Another important aspect of the overall system described herein is the time sensitive nature of the authorization step depicted in figure 28 elements 285, 286, 287, 288, and 289. This is the process following the interrogation of authorizing the transaction. In a retail environment, this is expected to take less than 15 seconds and require little or no manual input from the time just after interrogation step to a receipt of an authorization response from the application system. As used herein the term "completed authorization" refers to the part of the method for authorization following that starts when the interrogation step is complete and stopping when the point-of-sale receives an authorization response from the application system. As used herein the term "fast completed authorization step" refers to a completed authorization with a maximum duration time of 15 seconds. As used herein the

term "super fast completed authorization" refers to a completed authorization with a maximum duration time of 5 seconds. As used herein the term "authorization step requiring no manual input" refers to a completed authorization that contains no requirement for manual input to the mobile device by a card holder.

[00191] The method of Cryptogram Substitution is only possible in the event there is a channel to share a predetermined cryptogram or unpredictable cryptogram between the application system and the mobile device. Because of this channel for delivery, there is never a need for a permanent cryptographic key to be persistently stored local to the mobile device. Persistent storage of a permanent cryptographic key in a second location remote from the application system, as in the typical scenario of distributed secure elements inside plastic cards, is no longer a requirement in the event there is an active communication channel between a mobile device and the remote application system.

[00192] In the typical scenario, the SE on the plastic card must create an expected cryptogram independent of the remote application system, because it has no channel to receive the digital credential data. After the interrogation between the plastic card and the point-of-sale, the remote application system is then used to verify the expected cryptogram by the SE after each interrogation. This means the SE and the remote authentication server must both possess a copy of the permanent cryptographic key that generates the expected cryptogram.

[00193] In this method of Cryptogram Substitution, because there is a communication channel from the mobile device to the application system, there is no need to distribute a second copy of a permanent cryptographic key, to be stored persistently, and used for expected cryptogram calculation, to the mobile device when it is used as a payment instrument.

[00194] As discussed herein, various embodiments describe methods for performing a timely authorization of digital credential data delivered from a mobile device that is without access to a local persistently stored permanent cryptographic key; through an interrogation with a point-of-sale that behaves according to the direction of a card specification. Typically,

the card specification expects the mobile device to create a cryptogram that is calculated, at least in part, using a permanent cryptographic key and, at least in part, from unpredictable data delivered from the point-of-sale to the mobile device during the interrogation. A further consideration is that a mobile device may be without power in which case the local permanent cryptographic key would need to be stored persistently in order to function properly in the system when power is restored. A further consideration is that a mobile device, or an application running in the operating system of that mobile device, may have no means to persistently store the permanent cryptographic key locally based on the requirements set forth by the card specification and based on the resources available to the mobile device or application on the mobile device. A further consideration is that the card specification requirements may dictate that the mobile device, or application running in the operating system of that mobile device, is too hostile and vulnerable, based on various criteria, to be qualified to persistently store the permanent cryptographic key in the operating system. A further consideration is that the mobile device or the application running in the operating system of the mobile device, may not have local access to the persistently stored cryptographic key in an embedded SE or embedded secure storage, or any other secure local storage container.

[00195] As used herein the terms "point-of-sale", "POS", and "point-of-sale terminal" are synonyms and include, for example, terminals that are installed at merchant checkout counters, automated teller machines (ATMs), self-serve facilities (such as gasoline pumps), and similar service stations where financial transactions are authorized, and the terms also include computers that accept payment card data for authorizing financial transactions. POS terminals may accept payment card data in a plurality of ways including magnetic stripe reading, NFC reading, ISO78161-3 contact card reading, manual typing of card data, etc. As used herein the terms "point-of-sale (POS)" and "point-of-sale terminal" are limited to a point-of-sale that behaves according to the direction of a card specifications during an interrogation with a mobile device such that the point-of-sale controls the interrogation through sending commands to the mobile device and receiving responses from a mobile device.

[00196] As used herein the term "mobile device" refers to an electronic communication device having a weight of less than 2 pounds (0.907 kg). Examples of mobile devices are cell phones, smart phones, personal digital assistants (PDAs), electronic book readers and tablet computers, provided that the device weighs less than 2 pounds (0.907 kg).

[00197] ~~As used herein where~~ When it is said herein that a mobile device does not access a local persistently stored permanent cryptographic key, ~~it refers~~ such a reference may include ~~to~~ a mobile device that comprises an operating system, with an application that runs in that operating system, ~~wherein~~ such that the application does not have access to a local persistently stored permanent cryptographic key; ~~wherein~~ and/or such that that local persistently stored permanent cryptographic key is expected to be used to calculate an expected cryptogram, ~~wherein~~ and/or such that the expected cryptogram is expected to be contained within at least a portion of the digital credential data sent to the point-of-sale during an interrogation; ~~wherein~~ and/or such that the process is under the direction of the application.

[00198] As used herein the term "NFC emulating mobile device" is a mobile device that comprises an operating system, with an application that runs in that operating system, wherein the application has the capability of being interrogated by a point-of-sale in the role of a card, SE, or mobile device as that capability is defined in a card specification.

[00199] As used herein the term "secure mobile device" is a mobile device that has access to a local persistently stored permanent cryptographic key; wherein that local persistently stored permanent cryptographic key is expected to be used to calculate the expected cryptogram, wherein the expected cryptogram is expected to be contained within at least a portion of the digital credential data.

[00200] A cryptogram may be computed with unpredictable input data such as an unpredictable number (UN) and transaction data such as a transaction amount that is created un-predictably by a point-of-sale terminal. Even though a transaction amount may seem deterministic, it is unpredictable to the authorization system and considered unpredictable

Mastercard, Ex1002, p. 100

data. As used herein, this "unpredictable input data" that is used as input to a cryptogram calculation may for example be an unpredictable number, terminal input data, unpredictable terminal input data, transaction data, a transaction amount, or some other unpredictable data such as a random number, or combinations thereof.

[00201] The point-of-sale typically has no means to verify the expected cryptogram it received was actually calculated, at least in part or if at all, by the unpredictable data that it had delivered, or that the expected cryptogram it receives was actually calculated, at least in part or if at all, by the expected permanent cryptographic key. Thus, the mobile device may typically substitute the "expected" cryptogram with an "unexpected cryptogram" without detection of the substitution by the point-of-sale.

[00202] Later, the point-of-sale may request an authorization based on data, including the unexpected cryptogram that was received during the interrogation. This data is sent to an authorization authority (application system) for verification and authorization. The authorization authority is assumed to have access to the credential data, including cryptogram calculation keys, automated transaction counter, etc. that are linked to the credential data delivered by the card, SE or mobile device during the interrogation. If the authorizing authority is aware of the substitution and also has access to the unexpected cryptogram itself, or the unpredictable data that may have been used, at least in part, to create it, or the temporary cryptographic key that may have been used, at least in part, to create it, then the authorization authority may successfully verify the correctness of the cryptogram. This may happen either through a simple comparison of the cryptogram delivered by the point-of-sale with the unexpected cryptogram reference in the application system, or by performing correctness verification of the cryptogram delivered by the point-of-sale by re-calculating it.

[00203] Figure 23 discusses the idea of a mobile device requesting cache data to be used in a future interrogation with a point-of-sale. Element 227 indicates the passing of this data from the remote source of the application system to the local source of the mobile device for caching. The data contained in element 227 are data required to respond to a point-of-sale during an interrogation. This could include a predetermined cryptogram. Alternatively, but less secure, this cache data may also include the permanent cryptographic key, in addition

Mastercard, Ex1002, p. 101

with other required data, to calculate an expected cryptogram locally on the mobile device when an expected cryptogram is requested. Alternatively, the cache data may also include a temporary cryptographic key, in addition with other required data, to calculate an unpredictable cryptogram locally on the mobile device. The application system has access to the cryptogram key, and additional data used to calculate a cryptogram, so it has the ability to calculate a cryptogram or simply pass the encryption key to the mobile device with supporting calculation data, and allow the mobile device to calculate the cryptogram during an interrogation.

[00204] It is important to note that during many embodiments disclosed herein the application server and mobile device can be said to share information if the data at any point in time is sent from one entity to another. In one example, unpredictable data that are used to create a predetermined cryptogram may be created by the application system and share that data with the mobile device. It is entirely possible that the mobile device creates the unpredictable data and sends it to the application system. Similarly, in another example it is possible that the mobile device creates a predetermined cryptogram made exclusively from random data and sends the predetermined cryptogram to the application system instead of the application system sending the predetermined cryptogram to the mobile device. Similarly, in another example it is possible that the mobile device creates a temporary cryptographic key that is used to create an unpredictable cryptogram and sends it to the application system instead of the inverse.

[00205] As previously noted, an application running on an operating system in a mobile device may not have access to a local persistently stored cryptographic key. Consequently it may be said that the mobile device does not have a permanent cryptographic key for use to create an expected cryptogram to be sent to the application system because the permanent cryptographic key is expected to be persistent for the life of the card, and this implies that the mobile device has the means to access the permanent cryptographic key for use during the life of the card which needs to persist through mobile device power cycles.; Inversely, however, it is possible for an application system to create the permanent

Mastercard, Ex1002, p. 102

cryptographic key, store it persistently, and send it to the mobile device to be stored transiently.

[00206] NFC payment transactions, in particular, may be made secure by using disclosed data connection methods because the security of the transaction is based largely on the data content itself. Each transactional request that is passed through the interrogation phase of the reader and card yields Track1/Track2 equivalent data that change with every subsequent transaction, offering a single credential for each and every transaction. Further, the data content itself is shared-key-based data that may be, with virtually 100% certainty, verified that it was received from a specific card holder secure element. Because of this, the security of the data pipeline that actively transports the data are less important and may actually be considered a non-factor for the security of the financial transaction.

[00207] In some embodiments disclosed herein, a specific payment standard issued from MASTERCARD International. This standard is based on reference documentation published by PayPass - Mag Stripe (V3.3).pdf and other derivations. In this card specification, PayPass contactless payment card reader and card interrogation is documented. This document discusses specifically how an RFID reader interrogator would interact with a card containing a SE to extract and build Track1/Track2 equivalent data that is compatible for existing processing infrastructure, but contains the more secure and dynamic aspects of SE driven credential data.

[00208] In some embodiments disclosed herein, provisions are made for managing a remote system containing of a plurality of SE readers, each one being addressable and matched to a particular mobile device.

[00209] In some embodiments disclosed herein provisions are made for authenticating and validating a mobile device with a remote system to obtain access to a particular SE within a plurality of SEs in that remote system.

[00210] In some embodiments disclosed herein provisions are made for connecting a mobile device to a remote service via activating a data-pass-through mode for ISO7816-4

data commands from an POS RFID reader through a mobile device NFC interface through the mobile device OS, to a data connection to a remote system containing a plurality SEs.

[00211] In some embodiments disclosed herein provisions are made for using TCP/UDP/IP sockets to enable a communication channel between a RFID POS reader and a single SE within remote system containing a plurality of SEs.

[00212] In some embodiments disclosed herein provisions are made for authenticating over SSL to enable a TCP/UDP/IP socket communication channel between a RFID POS reader and a single SE within a remote system containing a plurality of SEs.

[00213] In some embodiments disclosed herein, similar to transaction caching above, provisions are made for one hundred percent transaction caching. These are methods and configurations that allow a mobile device to request a cache from the remote authentication system, where the cache request response encompasses data that can be used to create APDU responses to an entire point-of-sale interrogation sequence that may happen in the future. This cache may be stored securely in non-persistent memory (RAM) in the mobile device and used at the time of interrogation with the RFID (NFC) point-of-sale reader.

[00214] Building on systems for local caching as described above, some embodiments may allow a mobile device and an RFID (NFC) point-of-sale reader to interact exclusively with each other at the time of transaction (interrogation) without performing a remote request, which would result in a network delay, using data stored in the mobile device cache.

[00215] In some embodiments disclosed herein, provisions are made for substituting a properly formatted predetermined cryptogram that was created without using unpredictable data, at all, from the point-of-sale in place of actively creating and using an expected cryptogram that was created using data, at least in part, from a point-of-sale during an NFC interrogation sequence between a point-of-sale and a mobile device.

[00216] In some embodiments disclosed herein, provisions are made for substituting a properly formatted unpredictable cryptogram that was created using a temporary key in place of an expected cryptogram that was created with a permanent cryptographic key.

Mastercard, Ex1002, p. 104

[00217] Cryptogram substitution builds on the advantages by transaction caching because a predetermined cryptogram or unpredictable cryptogram allows for the caching of data on a mobile device that may be used to create a response to a cryptogram request; where the cryptogram request from the point-of-sale expects the cryptogram response to use, at least in part, unpredictable data from the point-of-sale, and a permanent cryptographic key, at least in part, to create an expected cryptogram. Substituting a predetermined cryptogram or unpredictable cryptogram as the data to be used in the expected cryptogram response removes the requirement to use network resources that incur the effect of network latency time while contacting the remote secure element representation to perform the cryptogram calculation. The predetermined cryptogram or unpredictable cryptogram may be delivered to the point-of-sale instead, in this manner, as a "cache hit." When the secure element is said to be remote, it indicates that there is no access to a locally stored permanent cryptographic key to be used in an expected cryptogram calculation.

[00218] In some embodiments disclosed herein, provisions are made for a remote source to deliver a permanent cryptographic key, along with any other required data, that are used to create an expected cryptogram in a mobile device. Although, this is a less secure embodiment, as the permanent cryptographic key is exposed to the mobile device, the concept of 100% transaction caching can also be achieved with this embodiment as all of the elements to create an expected cryptogram are now located in the local cache and the mobile device need not access the remote source during the cryptogram calculation phase of the interrogation.

[00219] In some embodiments disclosed herein, the mobile device has access to transactional data information such as transactional amount that it acquired during an interrogation with a point-of-sale. This transactional amount may be used as a second verification method to the mobile device user, or card holder. The mobile device may display this amount with a verification request to the mobile device screen. Prior to successful authorization of the request, the application system may use this input in the authorization decision. Advantages to this added verification method is related to added security and confirmation of transaction amount to be authorized. This method further

confirms that the user knows the dollar amount that is to be authorized during a financial transaction.

[00220] Various embodiments provide a software representation of a SE. The advantages of such embodiments include replacing a concept that may commonly perceived as a hardware solution with a software solution that saves in cost as well as space requirements.

[00221] Some embodiments disclosed herein use a base-band processor on the NFC mobile device to do one or all of the following tasks:

a. Begin a connection to a POS RFID reader through the mobile device's NFC radio interface.

b. Receive commands through the mobile device's NFC radio interface from the interrogation sequence offered by the POS RFID reader and pass those same commands to a remote system that is configured to receive those commands.

c. Receive responses from a remote system and pass those responses to a POS RFID reader through the mobile device's NFC radio interface.

[00222] Alternatively, some embodiments use the base-band processor in the mobile device to do one or all of the following tasks:

a. Begin a connection to a remote terminal configured to interrogate using 7816-4 data over TCP/UDP/IP.

b. Receive commands through this remote terminal interface over TCP/UDP/IP interface from the remote terminal and pass those same commands to a remote system that is configured to receive those commands.

c. Receive responses from a remote system and pass those responses to a remote terminal that is configured to receive the 7816-4 data over TCP/UDP/IP.

Mastercard, Ex1002, p. 106

[00223] Some embodiments disclosed herein use a remote server network and remote array of secure elements or representations of secure elements (remote system) to do one or all of the following tasks:

a. Authenticate a particular remote mobile device or owner of a mobile device that wishes to send commands from an interrogator to a SE that is contained in this system.

b. Properly address a single SE within an array of SEs to respond appropriately to a validated remote device.

c. Properly route commands that were passed to this system to a particular SE or SE software representation within the system and properly route responses from the SE out of the system to the correct validated remote device.

d. Properly bypass a remote SE or remote SE representation and respond with static or persistent data that may represent transaction data that may be used in a contactless transaction.

[00224] Some embodiments disclosed herein combine both the tasks performed by the NFC mobile device and the remote system to allow for a complete and un-interrupted interrogation between a RFID POS reader or remote terminal and an NFC mobile device. The interrogation may be performed as set forth by payment card standards such as MASTERCARD PayPass, VISA Contactless, AMEX Express Pay, DISCOVER Zip, and contactless EMV.

[00225] The data link or data connection and communication between the mobile device and the remote system or remote terminal stated above may be carried out over standard TCP/UDP/IP services that are currently available on mobile devices.

[00226] Some advantages of various embodiments include:

a. In the event a mobile device that is used to conduct an NFC payment transaction with an RFID terminal is lost or stolen, the remote system may be

notified and communication with the SE may be blocked until the stolen or lost device is recovered or replaced. In the event the device is replaced, new card credentials do not have to be issued again, but a communication channel with the SE may be opened back up and continued upon proper authorization. Prior to this invention, all new SE credentials or cards would have to be re-issued as the hardware that contained the SE itself would have been lost or stolen also.

b. The SE that is associated with a remote mobile device may be switched to another mobile device fast and easily and is not hardware form factor dependant. The same SE may be used with multiple mobile devices, laptop or desktop computers that have the ability to connect to this remote system that contains the SE over a data connection and authenticate properly.

c. Compared to changing hardware interfaces, and array of different hardware interfaces, and supported hardware interfaces on a mobile device, a data connection is ubiquitous and standard. SE's currently have various hardware form factors such as:

    i. Embedded microchip (soldered to a circuit board)

    ii. SD, mini-SD, micro-SD interface

    iii. USB interface

    iv. SIM card interface

    Many mobile devices support different sets of the above hardware form factors and many support none of them at all, however, most all mobile devices support a data connection. This ubiquity aids to the portability of SE applications from device to device.

d. Because some embodiments contain an array of SEs or SE representations, and because the remote system is designed to host and connect SE

applications to multiple remote devices, it is possible for multiple remote devices from separate remote device owners to share a single SE from the array of SEs in the remote system. This sort of sharing of space on the SE enables consolidation and ultimately savings by more efficient utilization of memory on an array of SEs.

e. Because some embodiments do not rely on a hardware specific interface for the SE, but a data connection only. It is a more ubiquitous interface and may be used with more devices without being modified or changed from a hardware perspective.

f. Because some embodiments use an array or plurality of SEs, the ability to purchase SE chips in quantity for use in this array brings a possibility of a lower over-all cost per SE chip.

[00227] Some additional advantages of various embodiments also include:

a. Using "2 factor" authentication to protect connection to a remote SE from a mobile device. Upon authentication, a connection channel may be opened to a SE that relates to a particular mobile device. 2 factor authentication comprises of "something you have or do" AND "something you know".

b. An example of using "something you do" and "something you know" is using gestures (moving the phone through 3d space in reasonably reproducible manner) and an accelerometer to measure these gestures on a mobile device to create a "gesture signature" in combination with a typed in pin or password to authenticate to a remote system with an array of SEs as defined in this invention.

[00228] The foregoing descriptions of embodiments have been presented for purposes of illustration and exposition. They are not intended to be exhaustive or to limit the embodiments to the precise forms disclosed. Obvious modifications or variations are possible in light of the above teachings. The embodiments are chosen and described in an

effort to provide the best illustrations of principles and practical applications, and to thereby enable one of ordinary skill in the art to utilize the various embodiments as described and with various modifications as are suited to the particular use contemplated. All such modifications and variations are within the scope of the appended claims when interpreted in accordance with the breadth to which they are fairly, legally, and equitably entitled.

Mastercard, Ex1002, p. 110

CLAIMS

1. A method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction comprising:

using a remote permanent cryptographic key to calculate an expected cryptogram that is expected to comprise at least a portion of the digital credential data, wherein the remote permanent cryptographic key is persistently stored at a remote source that is remote from the mobile device and wherein the mobile device does not access a duplicate local permanent cryptographic key persistently stored locally to the mobile device;

performing an interrogation between the point-of-sale terminal and the mobile device comprising:

sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device requesting the digital credential data; and

sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal comprising the expected cryptogram as the at least a portion of the digital credential data;

wherein the financial transaction is authorized.

2. The method of Claim 1 further comprising a further step that precedes the performing the interrogation step, the further step comprising:

sending the remote permanent cryptographic key to the mobile device from the remote source; and

transiently caching the remote permanent cryptographic key in the mobile device as a cached transient permanent cryptographic key;

and wherein:

the step of sending through the communication channel the at least one POS command communication comprises sending unpredictable data;

the step of sending through the communication channel the at least one POS command communication comprises sending a request for an expected cryptogram that is expected to be calculated by the mobile device, at least in part, from the unpredictable data; and

the step of sending through the communication channel the at least one device response communication from the mobile device to the point-of-sale terminal comprises sending the expected cryptogram calculated, at least in part, from the unpredictable data and, at least in part, from the cached transient cryptographic key.

3. A method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction comprising:

performing an interrogation between the point-of-sale terminal and the mobile device comprising:

sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device, the at least one POS command communication comprising (a) a request for the digital credential data that is expected to comprise an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data, and, at least in part, from a permanent cryptographic key and (b) the unpredictable data; and

sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal, the at least one device response communication comprising at least a portion of the

digital credential data that comprises an unexpected cryptogram, substituted in place of the expected cryptogram;

wherein the financial transaction is authorized.

4. The method of Claim 3, wherein the unpredictable data comprises an unpredictable number.

5. The method of Claim 3, wherein the unpredictable data comprises a transaction amount.

6. The method of Claim 3 further comprising a mobile device preparation step that precedes the performing an interrogation step, the mobile device preparation step comprising sending critical data from a remote source to a mobile device, wherein the critical data comprises data used to formulate at least a portion of the digital credential data as a local portion of the digital credential data.

7. The method of Claim 6 wherein the local portion of the digital credential data comprises a predetermined cryptogram, which is calculated without the use of the unpredictable data, as the unexpected cryptogram.

8. The method of Claim 6 wherein the mobile device preparation step further comprises:

creating remote unpredictable data in a remote application system wherein the remote application system is the remote source;

sending the remote unpredictable data from application system to an HSM;

calculating a predetermined cryptogram in the HSM;

sending the predetermined cryptogram from the HSM to the remote application system;

sending at least a portion of the predetermined cryptogram from the remote application system to the mobile device as a portion of the critical data; and wherein

the local portion of the digital credential data comprises the predetermined cryptogram as the unexpected cryptogram.

9. The method of Claim 6 wherein the mobile device preparation step further comprises:

creating a predetermined cryptogram, which is calculated without the use of the unpredictable data, in a remote application system wherein the remote application system as the remote source;

sending at least a portion the predetermined cryptogram from the remote application system to the mobile device as a portion of the critical data; and wherein

the local portion of the digital credential data comprises the predetermined cryptogram as the unexpected cryptogram.

10. The method of Claim 6 wherein the critical data comprises a set of possible predetermined cryptograms; and the method further comprises a logical step of logically determining, in the mobile device, which of the possible predetermined cryptograms within the set of predetermined cryptograms to designate as the unexpected cryptogram; wherein the logical step is based, at least in part, on the unpredictable data; and wherein the local portion of the digital credential data comprises the designated predetermined cryptogram as the unexpected cryptogram.

11. The method of Claim 6 wherein the critical data comprises a set of possible predetermined cryptograms and card risk management data; and the method further comprises a logical step of logically determining, in the mobile device, which of the possible predetermined cryptograms within the set of possible predetermined cryptograms to designate as the unexpected cryptogram; wherein the logical step of is

based, at least in part, on the unpredictable data or based, at least in part, on the card risk management data; and wherein the local portion of the digital credential data comprises the designated predetermined cryptogram as the unexpected cryptogram.

12. The method of Claim 6 wherein the mobile device preparation step further comprises transiently storing at least a portion of the critical data on the mobile device, wherein the mobile device does not persistently store the at least a portion of critical data.

13. The method of Claim 6 wherein the local portion of the digital credential data comprises an unpredictable cryptogram as the unexpected cryptogram, wherein the unpredictable cryptogram is calculated, at least in part, using a temporary cryptographic key.

14. The method of Claim 6 wherein the mobile device preparation step further comprises:

creating a temporary cryptographic key in a remote application system wherein the remote application system is the remote source;

sending at least a portion of the temporary cryptographic key from the remote application system to the mobile device as a portion of the critical data; and wherein

the local portion of the digital credential data comprises an unpredictable cryptogram as the unexpected cryptogram, wherein the unpredictable cryptogram is calculated, at least in part, using the temporary cryptographic key.

15. The method of Claim 6 wherein the critical data comprises a temporary cryptographic key; and the method further comprises a step of calculating at least one local unpredictable cryptogram that is calculated, in at least part, using the temporary cryptographic key, and, in at least part, using a calculation formula determined from a set of calculation formulas; and the method further comprises a logical step of logically determining, in the mobile device, which local unpredictable cryptogram to designate as the unpredictable cryptogram; wherein the step of logically determining a decision is

made based, at least in part, on the unpredictable data; and wherein the local portion of the digital credential data comprises the designated local unpredictable cryptogram as the unexpected cryptogram.

16. The method of Claim 6 wherein the critical data comprises a temporary cryptographic key and card risk management data; and the method further comprises a step of calculating at least one local unpredictable cryptogram that is calculated, in at least part, using the temporary cryptographic key, and, in at least part, using a calculation formula determined from a set of calculation formulas; and the method further comprises a logical step of logically determining, in the mobile device, which local unpredictable cryptogram to designate as the unpredictable cryptogram; wherein the logical step is made based, at least in part, on the unpredictable data or based, at least in part, on the card risk management data; and wherein the local portion of the digital credential data comprises the designated local unpredictable cryptogram as the unexpected cryptogram.

17. The method of Claim 3 further comprising:

creating a predetermined cryptogram on the mobile device as the unexpected cryptogram; wherein the predetermined cryptogram is calculated without the use of the unpredictable data; and

sending at least a portion of the predetermined cryptogram from the mobile device to a remote application system.

18. The method of Claim 3 further comprising:

creating a temporary cryptographic key on the mobile device; wherein the temporary cryptographic key is used to calculate, at least in part, an unpredictable cryptogram as the unexpected cryptogram;

sending at least a portion of the unpredictable cryptogram from the mobile device to a remote application system.

19. The method of Claim 3 further comprising an authorizing step that follows the step of performing the interrogation, the authorizing step comprising:

sending an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system, wherein the unexpected cryptogram comprises a predetermined cryptogram;

verifying a correctness of the predetermined cryptogram by the application system (a) by comparing the predetermined cryptogram with a previously stored reference predetermined cryptogram and (b) without reference to the unpredictable data from the point-of-sale terminal; and

sending an authorization response from the remote application system to the point-of-sale wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the predetermined cryptogram.

20. The method of Claim 3 further comprising an authorizing step that follows the step of performing the interrogation, the authorizing step comprising:

sending an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system, wherein the unexpected cryptogram comprises an unpredictable cryptogram;

verifying a correctness of the unpredictable cryptogram by the application system wherein the unpredictable cryptogram is compared with a result of an unpredictable cryptogram calculation; wherein the unpredictable cryptogram calculation is calculated using, at least in part, a temporary cryptographic key; and

sending an authorization response from the remote application system to the point-of-sale wherein data contained in the authorization response is determined,

at least in part, by the verifying of the correctness of the unpredictable cryptogram.

21. The method of Claim 3 further comprising a corroborative authorizing step that follows the step of performing the interrogation, the corroborative authorizing step comprising:

sending through a second communication channel an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system;

sending through a third communication channel the unpredictable data from the mobile device to the remote application system;

verifying a correctness of the unexpected cryptogram in the remote application system;

verifying a correctness of the unpredictable data in the remote application system by comparing the unpredictable data sent through the second communication channel with the unpredictable data sent through the third communication channel;

sending through the second communication channel an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable data and, at least in part, by the verifying of the correctness of the unexpected cryptogram.

22. The method of Claim 21 further comprising a verifying a transaction amount step that follows the step of performing an interrogation and precedes the corroborative authorizing step, the verifying a transaction amount step comprising:

displaying transaction amount data to a display on the mobile device wherein the transaction amount data is at least a portion of the unpredictable data;

requesting verification of the transaction amount data from a card holder by the mobile device display screen;

sending the result of the requesting verification of the transaction amount data to a remote application system as input transaction amount data; and

wherein the corroborative authorizing step comprises determining, at least in part, an accuracy of the result of the verification step by using the input of the transaction amount data.

23. The method of Claim 3, further comprising an authorizing step that follows the step of performing an interrogation, the authorizing step comprising:

sending an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system, wherein the unexpected cryptogram comprises a predetermined cryptogram;

verifying a correctness of the predetermined cryptogram wherein the unpredictable data from the point-of sale (a) is substituted by the application system with a previously created unpredictable data that was previously used to calculate the predetermined cryptogram; and subsequently (b) is sent with the predetermined cryptogram to the HSM for cryptogram correctness verification; and

sending an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the predetermined cryptogram.

24. The method of Claim 3, further comprising an authorizing step that follows the step of performing an interrogation, the authorizing step comprising sending the unpredictable data from the mobile device to a remote application system.

25. The method of Claim 3 wherein the POS command communication conforms to ISO7816-4 data protocol and the device response communication conforms to ISO7816-4 data protocol.

26. The method of Claim 3 wherein the communication channel comprises a near-field communication channel.

27. The method of Claim 3 wherein the mobile device does not access a local persistently stored permanent cryptographic key that is expected to be used to calculate the expected cryptogram wherein the expected cryptogram is expected to be contained within the at least a portion of the digital credential.

28. A method for acquiring digital credential data by a point-of-sale terminal from a secure mobile device for authorization of a financial transaction comprising:

performing an interrogation between the point-of-sale terminal and the secure mobile device comprising:

sending through a communication channel at least one POS command communication from the point-of-sale terminal to the secure mobile device, the at least one POS command communication comprising (a) a request for the digital credential data that is expected to comprise an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data, and, at least in part, from a permanent cryptographic key and (b) the unpredictable data; and

sending through the communication channel at least one device response communication from the secure mobile device to the point-of-sale terminal, the at least one device response communication comprising at least a portion of the digital credential data that comprises the expected cryptogram;

in a step that follows the step of performing an interrogation, a secure mobile device transmitting step comprising sending over a second communication

channel the unpredictable data from the secure mobile device to a remote application system;

in a step that follows the step of performing an interrogation, a point-of-sale terminal transmitting step comprising sending over a third communication channel an authorization request from the point of sale terminal to the remote application system, the authorization request comprising the expected cryptogram and the unpredictable data;

in a step that follows the secure mobile device transmitting step and the point-of-sale terminal transmitting step, a corroborative authorizing step comprising:

verifying a correctness of the expected cryptogram by the application system;

verifying a correctness of the unpredictable data by the application system by comparing the unpredictable data sent over the second communication channel with the unpredictable data sent over the third communication channel; and

sending through the third communication channel an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable data and at least in part by the verifying of the correctness of the expected cryptogram;

wherein the financial transaction is authorized.

29. The method of Claim 28 further comprising a verifying step that follows the step of performing an interrogation and precedes the corroborative authorizing step, the verifying step comprising:

displaying transaction amount data to the secure mobile device display screen wherein the transaction amount data is comprised within the unpredictable data;

requesting verification of the transaction amount data from a card holder by the secure mobile device display screen;

sending the result of the requesting verification of the transaction amount data to a remote application system as input of the transaction amount data; and

wherein the corroborative authorizing step comprises determining, at least in part, the correctness of the result of the verification step by using the input of the transaction amount data.

ABSTRACT

Methods are described for performing a timely authorization of digital credential data delivered from a mobile device that is without access to a local persistently stored permanent cryptographic key; through an interrogation with a point-of-sale that behaves according to the direction of a card specification; wherein the card specification expects the mobile device to create a cryptogram that is calculated, at least in part, using the permanent cryptographic key and, at least in part, from unpredictable data delivered from the point-of-sale to the mobile device during the interrogation.

Mastercard, Ex1002, p. 123

DECLARATION FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM

the specification of which is attached hereto unless the following box is checked:

	was filed on	as U.S. Application No.
or	PCT International Application No.	and was amended on (if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56.
I hereby claim foreign priority benefits under 35 U.S.C. § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Applications	Application No.	Country	Day/month/year filed	Priority Not Claimed:

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application listed below.

Application No. 61/575,846	Filing Date: 2011-08-30
Application No. 61/573,476	Filing Date: 2011-09-06
Application No. 61/685,863	Filing Date: 2012-03-26

I hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

Application No.	Filing Date:	Status:
Application No.	Filing Date:	Status: (patented, pending, abandoned)

I hereby appoint the attorneys associated with **Customer No. 000408** (Luedeka Neely Group, P.C.) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Address all telephone calls to **James R. Palmer** at telephone number (865) 546-4305, and all correspondence to the address of **Customer No. 000408.**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or **first** inventor (give) name, family name)	**C. Douglas YEAGER**	
Inventor's Signature		**Date:** 6/30/2007
Citizenship	US	
Residence	7502 West Rim Dr., Austin, TX 78731	
Post Office Address	7502 West Rim Dr., Austin, TX 78731	

PTO/SB/14 (11-08)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	67979.U2
	Application Number	
Title of Invention	SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Douglas	C.	Yeager	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Austin	State/Province	TX	Country of Residence i	US

Citizenship under 37 CFR 1.41(b) i: US

Mailing Address of Applicant:

Address 1	7502 West Rim Dr.		
Address 2			
City	Austin	State/Province	TX
Postal Code	78731	Country i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	00408		
Email Address	JPalmer@LNG-Patent.com	Add Email	Remove Email

Application Information:

Title of the Invention	SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM		
Attorney Docket Number	67979.U2	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)		Suggested Figure for Publication (if any)	

PTO/SB/14 (11-08)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	67979.U2
	Application Number	
Title of Invention	SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM	

Publication Information:

☐	Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐	**Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S. C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	00408		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61685863	2012-03-26
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61573476	2011-09-06
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61575846	2011-08-30

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

Application Number	Country [i]	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			◉ Yes ○ No

PTO/SB/14 (11-08)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	67979.U2
	Application Number	
Title of Invention	SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM	

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.

Assignee 1 Remove

If the Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information:

Address 1			
Address 2			
City		**State/Province**	
Country [i]		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee Data may be generated within this form by selecting the **Add** button. Add

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/James R. Palmer/			Date (YYYY-MM-DD)	2012-08-30
First Name	James	Last Name	Palmer	Registration Number	48633

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM
First Named Inventor/Applicant Name:	C. Douglas Yeager
Filer:	James Roy Palmer/Jennifer McDonald
Attorney Docket Number:	67979.U2

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	95	95
Utility Search Fee	2111	1	310	310
Utility Examination Fee	2311	1	125	125
Pages:				
Claims:				
Claims in excess of 20	2202	9	30	270
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	800

Electronic Acknowledgement Receipt	
EFS ID:	13630179
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM
First Named Inventor/Applicant Name:	C. Douglas Yeager
Customer Number:	408
Filer:	James Roy Palmer/Jennifer McDonald
Filer Authorized By:	James Roy Palmer
Attorney Docket Number:	67979.U2
Receipt Date:	30-AUG-2012
Filing Date:	
Time Stamp:	16:43:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$800
RAM confirmation Number	3564
Deposit Account	122355
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)	
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)	
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Drawings-only black and white line drawings	67979u2-topto-20120830_Drawings.pdf	2375926 9cd8d16702a65a2c9f58f1f75a8bdbaa2e517b1bd	no	24
Warnings:					
Information:					
2		67979u2-topto-20120830-PatentApplication.pdf	501663 4913ca8b0c5886fa307bd375a243bcbb1df61e2208	yes	98

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	85
Claims	86	97
Abstract	98	98

Warnings:					
Information:					
3	Oath or Declaration filed	67979u2-topto-20120830-Declaration.pdf	1796650 5e1c559cbe9d6f6143697fbdf83f15f8e89106a0	no	2
Warnings:					
Information:					
4	Application Data Sheet	67979u2-topto-20120830-ADS.pdf	1421053 /9dc7f9443422fdfc948891ca7fbb6ea94ac2b26b	no	4
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	36727 0f0133f7ca73864df15dbe85e4b9aa6247f7a783	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	6132019		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Acknowledgement Receipt	
EFS ID:	13630179
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM
First Named Inventor/Applicant Name:	C. Douglas Yeager
Customer Number:	408
Filer:	James Roy Palmer/Jennifer McDonald
Filer Authorized By:	James Roy Palmer
Attorney Docket Number:	67979.U2
Receipt Date:	30-AUG-2012
Filing Date:	
Time Stamp:	16:43:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$800
RAM confirmation Number	3564
Deposit Account	122355
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)	
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)	
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Drawings-only black and white line drawings	67979u2-topto-20120830_Drawings.pdf	2375926 9cd8d16702a65a2c9f58f1f75a8bdbaa2e517b1bd	no	24
Warnings:					
Information:					
2		67979u2-topto-20120830-PatentApplication.pdf	501663 4913ca8b0c5886fa307bd375a243bcbb1df61e2208	yes	98

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	85
Claims	86	97
Abstract	98	98

Warnings:					
Information:					
3	Oath or Declaration filed	67979u2-topto-20120830-Declaration.pdf	1796650 5e1c559cbe9d6f43497fbdf83f15f8e89f0c4d0	no	2
Warnings:					
Information:					
4	Application Data Sheet	67979u2-topto-20120830-ADS.pdf	1421053 /9dc7f9443422fdfc948891ca7fbb6ea94ac2b26b	no	4
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	36727 0f0133f7ca73864df15dbe85e4b9aa6247f7d783	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	6132019		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/599,647	08/30/2012	2617	800	67979.U2	29	3

CONFIRMATION NO. 1919

408
LUEDEKA NEELY GROUP, P.C.
P O BOX 1871
KNOXVILLE, TN 37901

FILING RECEIPT

OC000000056523343

Date Mailed: 09/18/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

C. Douglas YEAGER, Austin, TX;

Applicant(s)

C. Douglas YEAGER, Austin, TX;

Power of Attorney: The patent practitioners associated with Customer Number 000408

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/685,863 03/26/2012
and claims benefit of 61/573,476 09/06/2011
and claims benefit of 61/575,846 08/30/2011

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

Projected Publication Date: 02/28/2013

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****

Title

SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM

Preliminary Class

455

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where

the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/599,647

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	95		N/A	
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	310		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	125		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	29 minus 20 =	* 9	x 30 =	270	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 125 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2			TOTAL	800		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

To: PTO-EMAIL@LNG-patent.com,LNG.PATENT@gmail.com,
From: PAIR_eOfficeAction@uspto.gov
Cc: PAIR_eOfficeAction@uspto.gov
Subject: Private PAIR Correspondence Notification for Customer Number 408

Sep 18, 2012 05:25:41 AM

Dear PAIR Customer:

LUEDEKA NEELY GROUP, P.C.
P O BOX 1871
KNOXVILLE, TN 37901
UNITED STATES

The following USPTO patent application(s) associated with your Customer Number, 408 , have new outgoing correspondence. This correspondence is now available for viewing in Private PAIR.

The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

Disclaimer:
The list of documents shown below is provided as a courtesy and is not part of the official file wrapper. The content of the images shown in PAIR is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
13599647	APP.FILE.REC	09/18/2012	67979.U2

To view your correspondence online or update your email addresses, please visit us anytime at https://sportal.uspto.gov/secure/myportal/privatepair.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov with 'e-Office Action' on the subject line or call 1-866-217-9197 during the following hours:

Monday - Friday 6:00 a.m. to 12:00 a.m.

Thank you for prompt attention to this notice,

UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT APPLICATION INFORMATION RETRIEVAL SYSTEM

9/13

DEPARTMENT OF DEFENSE
ACCESS ACKNOWLEDGEMENT / SECRECY ORDER RECOMMENDATION
FOR PATENT APPLICATION

Application Serial No: DP13599647

Date Referred: 09/06/2012

I hereby acknowledge that the Department of Defense reviewers have inspected this application in administration of 35 USC 181 on behalf of the Agencies/Commands specified below. DoD reviewers will not divulge any information from this application for any purpose other than administration of 35 USC 181.

Defense Agency	Recommendation	Reviewer Name	Date Reviewed
NSA	Secrecy Not Recommended	Robert Morelli	13 Sep 2012

Defense Agency	Reviewer Name	Date Viewed PDF
DTSA	Tim Hamilton	06 Sep 2012 15:38

Instructions to Reviewers:

1. All DoD personnel reviewing this application will be listed on this form regardless of whether they are making a secrecy order recommendation.
2. This form will be forwarded to USPTO once all assigned DoD entities have provided their secrecy order recommendation.

DoD Completion of Review: Final

Forwarded to USPTO: 09/13/2012

Mastercard, Ex1002, p. 143

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	13599647
Filing Date	2012-08-30
First Named Inventor	YEAGER, C. Douglas
Art Unit	2617
Examiner Name	
Attorney Docket Number	67979.U2

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6199762	B1	2001-03-13	Hohle	
	2	7774231	B2	2010-08-10	Pond et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030163708	A1	2003-08-28	Tang	
	2	20040118914	A1	2004-06-24	Smith et al.	
	3	20060224470	A1	2006-10-05	Garcia Ruano et al.	
	4	20070075133	A1	2007-04-05	Yeager	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13599647
	Filing Date	2012-08-30
	First Named Inventor	YEAGER, C. Douglas
	Art Unit	2617
	Examiner Name	
	Attorney Docket Number	67979.U2

	5	20080046367	A1	2008-02-21	Billmaier et al.	
	6	20080238610	A1	2008-10-02	Rosenberg	
	7	20090044012	A1	2009-02-12	Bishop et al.	
	8	20100274726	A1	2010-10-28	Florek et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13599647
	Filing Date	2012-08-30
	First Named Inventor	YEAGER, C. Douglas
	Art Unit	2617
	Examiner Name	
	Attorney Docket Number	67979.U2

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13599647
	Filing Date	2012-08-30
	First Named Inventor	YEAGER, C. Douglas
	Art Unit	2617
	Examiner Name	
	Attorney Docket Number	67979.U2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James R Palmer/	Date (YYYY-MM-DD)	2012-11-27
Name/Print	James R. Palmer	Registration Number	48633

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt	
EFS ID:	14314673
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Customer Number:	408
Filer:	James Roy Palmer/Jennifer McDonald
Filer Authorized By:	James Roy Palmer
Attorney Docket Number:	67979.U2
Receipt Date:	27-NOV-2012
Filing Date:	30-AUG-2012
Time Stamp:	13:26:31
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	67979u2-topto-20121127-IDS_CitingREfsFrmW2ISR.pdf	612693 f5b07515656281493863c367f4d0439c4244d1d1	no	5

Warnings:
Information:

2	Information Disclosure Statement (IDS) Form (SB08)	67979u2-topto-20121127-IDS_CitingRefsFrmW1ISR.pdf	612709 [illegible]	no	5

Warnings:	
Information:	
Total Files Size (in bytes):	1225402

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	13599647
Filing Date	2012-08-30
First Named Inventor	YEAGER, C. Douglas
Art Unit	2617
Examiner Name	
Attorney Docket Number	67979.U2

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060022033	A1	2006-02-02	Smets et al.	
	2	20070075133	A1	2007-04-05	Yeager	
	3	20070266131	A1	2007-11-15	Mazur et al.	
	4	20070278291	A1	2007-12-06	Rans et al.	
	5	20080219444	A1	2008-09-11	Benteo et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13599647
	Filing Date	2012-08-30
	First Named Inventor	YEAGER, C. Douglas
	Art Unit	2617
	Examiner Name	
	Attorney Docket Number	67979.U2

	6	20090006262	A1	2009-01-01	Brown et al.	
	7	20090124234	A1	2009-05-14	Fisher et al.	
	8	20100185545	A1	2010-07-22	Royyuru et al.	
	9	20100207742	A1	2010-08-19	Buhot et al.	
	10	20110112918	A1	2011-05-12	Mestre et al.	
	11	20110140841	A1	2011-06-16	Bona et al	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13599647
	Filing Date	2012-08-30
	First Named Inventor	YEAGER, C. Douglas
	Art Unit	2617
	Examiner Name	
	Attorney Docket Number	67979.U2

	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13599647
	Filing Date	2012-08-30
	First Named Inventor	YEAGER, C. Douglas
	Art Unit	2617
	Examiner Name	
	Attorney Docket Number	67979.U2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James R Palmer/	Date (YYYY-MM-DD)	2012-11-27
Name/Print	James R. Palmer	Registration Number	48,633

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/599,647	08/30/2012	C. Douglas YEAGER	67979.U2

CONFIRMATION NO. 1919

408
LUEDEKA NEELY GROUP, P.C.
P O BOX 1871
KNOXVILLE, TN 37901

PUBLICATION NOTICE

OC000000059582754

Title:SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM

Publication No.US-2013-0054474-A1
Publication Date:02/28/2013

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

To: PTO-EMAIL@LNG-patent.com,LNG.PATENT@gmail.com,
From: PAIR_eOfficeAction@uspto.gov
Cc: PAIR_eOfficeAction@uspto.gov
Subject: Private PAIR Correspondence Notification for Customer Number 408

Mar 01, 2013 05:36:32 AM

Dear PAIR Customer:

LUEDEKA NEELY GROUP, P.C.
P O BOX 1871
KNOXVILLE, TN 37901
UNITED STATES

The following USPTO patent application(s) associated with your Customer Number, 408 , have new outgoing correspondence. This correspondence is now available for viewing in Private PAIR.

The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

Disclaimer:
The list of documents shown below is provided as a courtesy and is not part of the official file wrapper. The content of the images shown in PAIR is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
13599647	NTC.PUB	02/28/2013	67979.U2

To view your correspondence online or update your email addresses, please visit us anytime at https://sportal.uspto.gov/secure/myportal/privatepair.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov with 'e-Office Action' on the subject line or call 1-866-217-9197 during the following hours:

Monday - Friday 6:00 a.m. to 12:00 a.m.

Thank you for prompt attention to this notice,

UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT APPLICATION INFORMATION RETRIEVAL SYSTEM

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	13/599,647
Applicant:	YEAGER, C. Douglas
Filing Date:	30 August 2012
Confirmation No.:	1919
Title:	SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM

PRELIMINARY AMENDMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Prior to examination on merits please amend the above-referenced application as follows and consider the included Remarks.

Amendments to the Specification begin on page 2 of this submittal.

Amendments to the Claims are reflected in the listing of claims which begins on page 4 of this submittal.

Remarks begin on page 16 of this submittal.

In the Specification:

Please replace paragraph [00118] with the following amended paragraph:

[**00118**] Cryptograms used herein are many times may be "expected" to be calculated, at least in part, from a permanent cryptographic key that during an interrogation between a mobile device and a point-of-sale. ~~Used~~ As used herein the term "unpredictable cryptogram" refers to a cryptogram calculated, at least in part, from a temporary cryptographic key for use in an interrogation between a mobile device and a point-of-sale; wherein the interrogation is defined by a card specification; and the card specification indicates a cryptogram to be calculated, at least in part, by a permanent cryptographic key. As used herein "unpredictable cryptogram" also refers to a type of unexpected cryptogram.

Please replace paragraph [00197] with the following amended paragraph:

[**00197**] ~~As used herein where~~ ~~When~~ When it is said ~~herein~~ herein that a mobile device does not access a local persistently stored permanent cryptographic key, ~~it refers such a reference may include to~~ such a reference may include a mobile device that comprises an operating system, with an application that runs in that operating system, ~~wherein such that~~ such that the application does not have access to a local persistently stored permanent cryptographic key; ~~wherein and/or such that~~ and/or such that that local persistently stored permanent cryptographic key is expected to be used to calculate an expected cryptogram, ~~wherein and/or such that~~ and/or such that the expected cryptogram is expected to be contained within at least a portion of the digital credential data sent to the point-of-sale during an interrogation; ~~wherein and/or such that~~ and/or such that the process is under the direction of the application.

As a consequence of the above changes, Paragraph [00197] now reads as follows.

[**00197**] When it is said herein that a mobile device does not access a local persistently stored permanent cryptographic key, such a reference may include a mobile device that comprises an operating system, with an application that runs in that operating system, such that the application does not have access to a local persistently stored permanent cryptographic key; and/or such that that local persistently stored permanent cryptographic key is expected to be used to calculate a

Mastercard, Ex1002, p. 159

first cryptogram, and/or such that the first cryptogram is expected to be contained within at least a portion of the digital credential data sent to the point-of-sale during an interrogation; and/or such that the process is under the direction of the application.

Mastercard, Ex1002, p. 160

In the Claims:

This listing of claims will replace all prior versions, and listing, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction comprising:

using a remote permanent cryptographic key to calculate an expected cryptogram, wherein the expected cryptogram ~~that~~ is expected to comprise at least a portion of the digital credential data, wherein the remote permanent cryptographic key is persistently stored at a remote source that is remote from the mobile device and wherein ~~the mobile device does not access a~~ there is no duplicate local permanent cryptographic key persistently stored locally to the mobile device;

performing an interrogation between the point-of-sale terminal and the mobile device comprising:

sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device requesting the digital credential data wherein the at least one POS command communication conforms to a card specification; and

sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal comprising the expected cryptogram as the at least a portion of the digital credential data;

wherein the financial transaction is authorized.

Mastercard, Ex1002, p. 161

2. (Currently Amended) The method of Claim 1 further comprising a further step that precedes the performing the interrogation step, the further step comprising:

sending the remote permanent cryptographic key to the mobile device from the remote source; and

transiently caching the remote permanent cryptographic key in the mobile device as a cached transient permanent cryptographic key;

and wherein:

the step of sending through the communication channel the at least one POS command communication comprises sending unpredictable data;

the step of sending through the communication channel the at least one POS command communication comprises sending a request for an expected cryptogram, wherein the expected cryptogram ~~that~~ is expected to be calculated by the mobile device, at least in part, from the unpredictable data; and

the step of sending through the communication channel the at least one device response communication from the mobile device to the point-of-sale terminal comprises sending the expected cryptogram calculated, at least in part, from the unpredictable data and, at least in part, from the cached transient cryptographic key.

3. (Currently Amended) A method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction comprising:

performing an interrogation between the point-of-sale terminal and the mobile device comprising:

sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device wherein the at least one POS command communication conforms to a card specification, and the at least one POS command communication comprising (a) a request for the

Mastercard, Ex1002, p. 162

digital credential data, wherein the digital credential data ~~that~~ is expected to comprise an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data, and, at least in part, from a permanent cryptographic key and (b) the unpredictable data; and

sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal, the at least one device response communication comprising at least a portion of the digital credential data that comprises an unexpected cryptogram that is different from the expected cryptogram, substituted in place of the expected cryptogram;

wherein the financial transaction is authorized.

4. (Original) The method of Claim 3, wherein the unpredictable data comprises an unpredictable number.

5. (Original) The method of Claim 3, wherein the unpredictable data comprises a transaction amount.

6. (Currently Amended) The method of Claim 3 further comprising a mobile device preparation step that precedes the performing an interrogation step, the mobile device preparation step comprising ~~sending~~ exchanging critical data ~~from~~ between a remote source ~~to a~~ and the mobile device, wherein the critical data comprises data used to formulate at least a portion of the digital credential data as a local portion of the digital credential data and the critical data are dynamic over a life of the digital credential.

7. (Currently Amended) The method of Claim 6 wherein the local portion of the digital credential data comprises a predetermined cryptogram, wherein the predetermined cryptogram ~~which~~ is ~~calculated~~ formulated without the use of the unpredictable data, as the unexpected cryptogram.

8. (Currently Amended) The method of Claim 6 wherein the mobile device preparation step further comprises:

creating remote unpredictable data in a remote application system wherein the remote

Mastercard, Ex1002, p. 163

application system is the remote source;

sending the remote unpredictable data from application system to an HSM;

calculating a predetermined cryptogram in the HSM without the use of the unpredictable data;

sending the predetermined cryptogram from the HSM to the remote application system;

sending at least a portion of the predetermined cryptogram from the remote application system to the mobile device as a portion of the critical data; and wherein

the local portion of the digital credential data comprises the predetermined cryptogram ~~as~~ and the unexpected cryptogram comprises the predetermined cryptogram.

9. (Currently Amended) The method of Claim 6 wherein the mobile device preparation step further comprises:

creating a predetermined cryptogram in a remote application system, wherein the predetermined cryptogram ~~which~~ is ~~calculated~~ formulated without the use of the unpredictable data~~, in a remote application system~~ and wherein the remote application system [[as]] is the remote source;

sending at least a portion the predetermined cryptogram from the remote application system to the mobile device as a portion of the critical data; and wherein

the local portion of the digital credential data comprises the predetermined cryptogram as the unexpected cryptogram.

10. (Currently Amended) The method of Claim 6 wherein the critical data comprises a set of possible predetermined cryptograms, which are formulated without the use of the unpredictable data; and the method further comprises a logical step of logically determining, in the mobile device, which of the possible predetermined cryptograms within the set of

Mastercard, Ex1002, p. 164

predetermined cryptograms to designate as the unexpected cryptogram; wherein the logical step is based, at least in part, on the unpredictable data; and wherein the local portion of the digital credential data comprises the predetermined cryptogram as the unexpected cryptogram..

11. (Currently Amended) The method of Claim 6 wherein the critical data comprises a set of possible predetermined cryptograms, which are formulated without the use of the unpredictable data, and card risk management data; and the method further comprises a logical step of logically determining, in the mobile device, which of the possible predetermined cryptograms within the set of possible predetermined cryptograms to designate as the unexpected cryptogram; wherein the logical step of is based, at least in part, on the unpredictable data or based, at least in part, on the card risk management data; and wherein the local portion of the digital credential data comprises the predetermined cryptogram as the unexpected cryptogram.

12. (Original) The method of Claim 6 wherein the mobile device preparation step further comprises transiently storing at least a portion of the critical data on the mobile device, wherein the mobile device does not persistently store the at least a portion of critical data.

13. (Original) The method of Claim 6 wherein the local portion of the digital credential data comprises an unpredictable cryptogram as the unexpected cryptogram, wherein the unpredictable cryptogram is calculated, at least in part, using a temporary cryptographic key.

14. (Currently Amended) The method of Claim 6 wherein the mobile device preparation step further comprises:

creating a temporary cryptographic key in a remote application system wherein the remote application system is the remote source;

sending at least a portion of the temporary cryptographic key from the remote application system to the mobile device as a portion of the critical data; and wherein

the local portion of the digital credential data comprises an unpredictable cryptogram as the unexpected cryptogram, wherein the unpredictable calculated cryptogram is calculated, at

Mastercard, Ex1002, p. 165

least in part, using the temporary cryptographic key and the unexpected cryptogram comprises the unpredictable cryptogram.

15. (Currently Amended) The method of Claim 6 wherein the critical data comprises a temporary cryptographic key; and the method further comprises a step of calculating ~~at least one local~~ a plurality of unpredictable cryptograms that ~~is~~ are calculated, in at least part, using the temporary cryptographic key, and, in at least part, using a calculation formula determined from a set of calculation formulas; and the method further comprises a logical step of logically determining, in the mobile device, which ~~local~~ of the plurality unpredictable cryptograms to designate as the unpredictable cryptogram; wherein the step of logically determining a decision is made based, at least in part, on the unpredictable data; and wherein the local portion of the digital credential data comprises the designated ~~local~~ unpredictable cryptogram ~~as~~ and the unexpected cryptogram comprises the designated unpredictable cryptogram.

16. (Currently Amended) The method of Claim 6 wherein the critical data comprises a temporary cryptographic key and card risk management data; and the method further comprises a step of calculating ~~at least one~~ a plurality of ~~local~~ unpredictable cryptograms that ~~is~~ are calculated, in at least part, using the temporary cryptographic key, and, in at least part, using a calculation formula determined from a set of calculation formulas; and the method further comprises a logical step of logically determining, in the mobile device, which ~~local~~ of the plurality of unpredictable cryptograms to designate as the unpredictable cryptogram; wherein the logical step is made based, at least in part, on the unpredictable data or based, at least in part, on the card risk management data; and wherein the local portion of the digital credential data comprises the designated local unpredictable cryptogram ~~as~~ and the unexpected cryptogram comprises the designated unpredictable cryptogram.

17. (Currently Amended) The method of Claim [[3]] 6 ~~further comprising~~ wherein the mobile device preparation step further comprises:

creating a predetermined cryptogram [[on]]in the mobile device, ~~as the unexpected cryptogram;~~ wherein the predetermined cryptogram is ~~calculated~~ formulated without the use of the unpredictable data; and

Mastercard, Ex1002, p. 166

sending at least a portion of the predetermined cryptogram from the mobile device to a remote application system as a portion of the critical data; wherein the remote application system is the remote source; and wherein

the local portion of the digital credential data comprises the predetermined cryptogram as the unexpected cryptogram.

18. (Currently Amended) The method of Claim [[3]] 6 ~~further comprising~~ wherein the mobile device preparation step further comprises:

creating a temporary cryptographic key [[on]]in the mobile device; ~~wherein the temporary cryptographic key is used to calculate, at least in part, an unpredictable cryptogram as the unexpected cryptogram~~;

sending at least a portion of the ~~unpredictable cryptogram~~ temporary cryptographic key from the mobile device to a remote application system as a portion of the critical data; wherein the remote application system is the remote source; and wherein

the local portion of the digital credential data comprises an unpredictable cryptogram as the unexpected cryptogram, wherein the unpredictable cryptogram is calculated, at least in part, using the temporary cryptographic key and the unexpected cryptogram comprises the unpredictable cryptogram.

19. (Currently Amended) The method of Claim 3 further comprising an authorizing step that follows the step of performing the interrogation, the authorizing step comprising:

sending an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system, wherein the unexpected cryptogram comprises a predetermined cryptogram that is formulated without the use of the unpredictable data;

verifying a correctness of the predetermined cryptogram by the application system (a) by comparing the predetermined cryptogram with a previously stored reference predetermined cryptogram and (b) without reference to the unpredictable data from the point-of-sale terminal; and

Mastercard, Ex1002, p. 167

sending an authorization response from the remote application system to the point-of-sale wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the predetermined cryptogram.

20. (Currently Amended) The method of Claim 3 further comprising an authorizing step that follows the step of performing the interrogation, the authorizing step comprising:

sending an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system, wherein the unexpected cryptogram comprises an unpredictable cryptogram that is calculated using, at least in part, a temporary cryptographic key;

verifying a correctness of the unpredictable cryptogram by the remote application system wherein the unpredictable cryptogram is compared with a result of an unpredictable cryptogram calculation~~; wherein the unpredictable cryptogram calculation is calculated using, at least in part, a temporary cryptographic key~~; and

sending an authorization response from the remote application system to the point-of-sale wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable cryptogram.

21. (Original) The method of Claim 3 further comprising a corroborative authorizing step that follows the step of performing the interrogation, the corroborative authorizing step comprising:

sending through a second communication channel an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system;

sending through a third communication channel the unpredictable data from the mobile device to the remote application system;

verifying a correctness of the unexpected cryptogram in the remote application system;

Mastercard, Ex1002, p. 168

verifying a correctness of the unpredictable data in the remote application system by comparing the unpredictable data sent through the second communication channel with the unpredictable data sent through the third communication channel;

sending through the second communication channel an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable data and, at least in part, by the verifying of the correctness of the unexpected cryptogram.

22. (Original) The method of Claim 21 further comprising a verifying a transaction amount step that follows the step of performing an interrogation and precedes the corroborative authorizing step, the verifying a transaction amount step comprising:

displaying transaction amount data to a display on the mobile device wherein the transaction amount data is at least a portion of the unpredictable data;

requesting verification of the transaction amount data from a card holder by the mobile device display screen;

sending the result of the requesting verification of the transaction amount data to a remote application system as input transaction amount data; and

wherein the corroborative authorizing step comprises determining, at least in part, an accuracy of the result of the verification step by using the input of the transaction amount data.

23. (Original) The method of Claim 3, further comprising an authorizing step that follows the step of performing an interrogation, the authorizing step comprising:

sending an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system, wherein the unexpected cryptogram comprises a predetermined cryptogram;

verifying a correctness of the predetermined cryptogram wherein the unpredictable

Mastercard, Ex1002, p. 169

data from the point-of sale (a) is substituted by the application system with a previously created unpredictable data that was previously used to calculate the predetermined cryptogram; and subsequently (b) is sent with the predetermined cryptogram to the HSM for cryptogram correctness verification; and

sending an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the predetermined cryptogram.

24. (Original) The method of Claim 3, further comprising an authorizing step that follows the step of performing an interrogation, the authorizing step comprising sending the unpredictable data from the mobile device to a remote application system.

25. (Original) The method of Claim 3 wherein the POS command communication conforms to ISO7816-4 data protocol and the device response communication conforms to ISO7816-4 data protocol.

26. (Original) The method of Claim 3 wherein the communication channel comprises a near-field communication channel.

27. (Original) The method of Claim 3 wherein the mobile device does not access a local persistently stored permanent cryptographic key that is expected to be used to calculate the expected cryptogram wherein the expected cryptogram is expected to be contained within the at least a portion of the digital credential.

28. (Currently Amended) A method for acquiring digital credential data by a point-of-sale terminal from a secure mobile device for authorization of a financial transaction comprising:

performing an interrogation between the point-of-sale terminal and the secure mobile device comprising:

sending through a communication channel at least one POS command communication from the point-of-sale terminal to the secure mobile device wherein the at least one POS command communication conforms to a card specification, and the at least one POS command communication comprising (a) a

Mastercard, Ex1002, p. 170

request for the digital credential data, wherein the digital credential data ~~that~~ is expected to comprise an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data, and, at least in part, from a permanent cryptographic key and (b) the unpredictable data; and

sending through the communication channel at least one device response communication from the secure mobile device to the point-of-sale terminal, the at least one device response communication comprising at least a portion of the digital credential data that comprises the expected cryptogram;

in a step that follows the step of performing an interrogation, a secure mobile device transmitting step comprising sending over a second communication channel the unpredictable data from the secure mobile device to a remote application system;

in a step that follows the step of performing an interrogation, a point-of-sale terminal transmitting step comprising sending over a third communication channel an authorization request from the point of sale terminal to the remote application system, the authorization request comprising the expected cryptogram and the unpredictable data;

in a step that follows the secure mobile device transmitting step and the point-of-sale terminal transmitting step, a corroborative authorizing step comprising:

verifying a correctness of the expected cryptogram by the application system;

verifying a correctness of the unpredictable data by the application system by comparing the unpredictable data sent over the second communication channel with the unpredictable data sent over the third communication channel; and

sending through the third communication channel an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable data and at least in part by the verifying of the correctness of the expected cryptogram;

Mastercard, Ex1002, p. 171

wherein the financial transaction is authorized.

29. (Original) The method of Claim 28 further comprising a verifying step that follows the step of performing an interrogation and precedes the corroborative authorizing step, the verifying step comprising:

displaying transaction amount data to the secure mobile device display screen wherein the transaction amount data is comprised within the unpredictable data;

requesting verification of the transaction amount data from a card holder by the secure mobile device display screen;

sending the result of the requesting verification of the transaction amount data to a remote application system as input of the transaction amount data; and

wherein the corroborative authorizing step comprises determining, at least in part, the correctness of the result of the verification step by using the input of the transaction amount data.

Mastercard, Ex1002, p. 172

Remarks

Paragraph [00117] is currently amended to delete the extraneous word "Used." No new matter is entered with this amendment of paragraph [00117].

Paragraph [00197] was inadvertently filed with strike-through text and underlined text that were used in a prior draft to indicate text deletions and text additions made in that draft. This preliminary amendment deletes the strike-through text and deletes the underlines from the underlined text. Converting these annotated changes to final format adds no new matter to the specification.

Claim 1 is currently amended to specify "wherein ~~the mobile device does not access a~~ there is no duplicate local permanent cryptographic key persistently stored locally to the mobile device." Support for this change may be found at least, for example, in paragraphs [0005], [00190], [00192], [00193], [00196], and [00204], of the specification. Consequently no new matter is entered with this amendment of Claim 1.

Claims 1, 2, 3 and 28 are amended to replace "that" with a "wherein" clause. This change is made to more clearly define the element being modified by the subsequently-stated limitation. No new matter is entered with these clarifications.

Claims 1, 3 and 28 are currently amended to specify that the at least one POS command communication conforms to a card specification. Support for this limitation may be found at least, for example, in paragraphs [00117] - [00122] and [00133] of the specification. Consequently no new matter is entered with these amendments.

Claim 3 is currently amended to specify "an unexpected cryptogram that is different from the expected cryptogram, substituted in place of the expected cryptogram." Support for this limitation may be found at least, for example, in paragraph [00119] of the specification. Consequently, no new matter is entered with this amendment of Claim 3.

Claim 6 is currently amended to specify that the mobile device preparation step comprises exchanging critical data between a remote source and the mobile device. Support for this limitation may be found at least, for example, in paragraphs [00187] and [00203] which

Mastercard, Ex1002, p. 173

describe exchanging data such as a predetermined cryptogram or a permanent cryptographic key "in addition with other required data" between a remote source and a mobile device during an interrogation. Claim 6 is further currently amended to specify that the critical data (where the critical data comprises data used to formulate at least a portion of the digital credential data) are dynamic over the life of the digital credential. Support for these limitations may be found at least, for example, in paragraph [00110] of the specification. Consequently no new matter is entered with the current amendment of Claim 6.

Claims 7 and 9 are currently amended to replace "which" with a "wherein" clause. This change is made to more clearly define the element being modified by the subsequently-stated limitation. No new matter is entered with these clarifications.

Claims 7, 9, 10, 11 and 17 are currently amended to specify that the predetermined cryptogram is formulated without the use of unpredictable data. Support for this limitation may be found at least, for example, in paragraph [00117] of the specification, so now new matter is entered with this amendment of Claims 7, 9, 10, 11 and 17.

Claims 8 – 11 are currently amended to specify that the unexpected cryptogram comprises the predetermined cryptogram. Support for this limitation may be found at least, for example, in paragraphs [00117] and [00119] of the specification. Consequently no new matter is entered with this these amendments of Claims 8 – 11.

Claim 9 is currently amended to correct a typographical error, replacing "as" with "is." No new matter is entered with this correction.

Claim 17 is currently amended to correct a typographical error, replacing "on" with "in." No new matter is entered with this correction.

Claims 14 – 16 are currently amended to specify that the unexpected cryptogram comprises the unpredictable cryptogram. Support for this limitation may be found at least, for example, in paragraphs [00117] and [00119] of the specification, so no new matter is entered with this amendment of Claims 14 – 16.

Mastercard, Ex1002, p. 174

Claims 15 and 16 are currently amended to specify calculating a plurality of unpredictable cryptograms instead of at least one cryptogram. Claims 15 and 16 (as originally and currently drafted) specify a step of logically determining which unpredictable cryptogram to use. This step would have no meaning if only one unpredictable cryptogram is calculated, so the current amendment corrects that inconsistency in the original claims without adding any new matter.

Claims 17 and 18 are currently amended to specify dependency from Claim 6 instead of Claim 3. Claim 6 depends from Claim 3, so no new matter is entered by incorporating the further limitations of Claim 6 into Claims 17 and 18.

Claims 18 is currently amended to specify that the unpredictable cryptogram is calculated at least in part from a temporary cryptographic key. Support for this limitation may be found at least, for example, in paragraph [00151] of the specification. Consequently no new matter is entered with this amendment of Claim 18.

Claim 18 is currently amended to specify "sending at least a portion of the temporary cryptographic key to a remote application system." Support for this limitation may be found at least, for example, in paragraph [00114] of the specification. Consequently no new matter is entered with this amendment of Claim 18.

Claim 18 is currently amended to specify certain characteristics of the local portion of the digital credential data. These limitations are adapted from Claim 14 as originally filed. Consequently no new matter is entered with this amendment of Claim 18.

Claim 19 is currently amended to specify that the predetermined cryptogram is formulated without the use of the unpredictable data. Support for this limitation may be found at least, for example, in original Claims 7, 9, and 17. Consequently no new matter is entered with this amendment of Claim 19.

Consideration and allowance of the amended and new Claims is respectfully requested.

Conclusion

The Applicant respectfully requests that this amendment be considered in conjunction

Mastercard, Ex1002, p. 175

with the first review of this application. In the event that an Office Action on this application predates this Preliminary Amendment, the Applicant respectfully requests that consideration of this Amendment be withheld pending Applicant's review of the Office Action and incorporation of the elements of this Amendment into a response to the Office Action.

In the event that payment submitted with this filing is inadequate to cover applicable fees with respect to this submittal please charge any shortfall to our Deposit Account No. 12-2355.

Respectfully submitted,
LUEDEKA NEELY GROUP, P.C.
By: James R Palmer
James R. Palmer
Registration No. 48,633

Date: April 15, 2013
P.O. Box 1871
Knoxville, Tennessee 37901
(865) 546-4305

Mastercard, Ex1002, p. 176

Electronic Acknowledgement Receipt	
EFS ID:	15520242
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Customer Number:	408
Filer:	James Roy Palmer/Jennifer McDonald
Filer Authorized By:	James Roy Palmer
Attorney Docket Number:	67979.U2
Receipt Date:	15-APR-2013
Filing Date:	30-AUG-2012
Time Stamp:	16:31:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		67979u2-topto-20130415-PreliminaryAmendment.pdf	146471 9a8adb6c04e27e9617dad27d03bd27e5d1921e	yes	19

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Preliminary Amendment	1	1
	Specification	2	3
	Claims	4	15
	Applicant Arguments/Remarks Made in an Amendment	16	19
Warnings:			
Information:			
	Total Files Size (in bytes):	146471	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/599,647	Filing Date 08/30/2012	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 = *		X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 = *		X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 04/15/2013	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	(Column 3) ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 29	Minus	** 29	= 0	X $40 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	(Column 3) ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LDRC
/ADRIANE WINSTON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/80 (07-12)
Approved for use through 11/30/2014 OMB 0651-0035
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:

■ Practitioners associated with Customer Number: 122870

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignments documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:

■ The address associated with Customer Number: 122870

OR

☐ Firm or individual Name	
Address	
City	State / Zip
Country	
Telephone	Email

Assignee Name and Address: SimplyTapp, Inc.
7200 Spurlock Dr.
Austin, TX 78731

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be Filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of The practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature	C. Douglas Yeager	Date	5/8/2015
Name		Telephone	512 629 0546
Title	CEO, SimplyTapp, Inc.		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: C. Douglas Yeager

Application No./Patent No.: 13/599,647 Filed/Issue Date: 8/30/2012

Titled: System and Method For Authorizing A Transaction With An unexpected Cryptogram

Simplytapp, Inc., a Corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☑ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 031642, Frame 0304, or for which a copy thereof is attached.

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

   1. From: _____ To: _____

      The document was recorded in the United States Patent and Trademark Office at

      Reel _____, Frame _____, or for which a copy thereof is attached.

   2. From: _____ To: _____

      The document was recorded in the United States Patent and Trademark Office at

      Reel _____, Frame _____, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel , Frame , or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☐ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Walter G. Hanchuk 35,179/	May 11, 2015
Signature	Date
Walter G. Hanchuk	35179
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	22303439
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Customer Number:	408
Filer:	Walter G. Hanchuk
Filer Authorized By:	
Attorney Docket Number:	67979.U2
Receipt Date:	12-MAY-2015
Filing Date:	30-AUG-2012
Time Stamp:	00:31:34
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	POA_signed.pdf	859357 ddf271fb360375f0a7d89bcd8cc4ce6da7d9 88e3d	no	1

Warnings:	
Information:	

2	Assignee showing of ownership per 37 CFR 3.73	373_statement.pdf	96151 a2616cefc1dd5390a4db328b1762418b525e90611	no	3
Warnings:					
Information:					
		Total Files Size (in bytes):	955508		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/599,647	08/30/2012	C. Douglas YEAGER	67979.U2

CONFIRMATION NO. 1919

408
LUEDEKA NEELY GROUP, P.C.
P O BOX 1871
KNOXVILLE, TN 37901

POWER OF ATTORNEY NOTICE

OC000000075172475

Date Mailed: 05/15/2015

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 05/12/2015.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/mbeyene/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/599,647	08/30/2012	C. Douglas YEAGER	67979.U2

CONFIRMATION NO. 1919

122870
Hanchuk Kheit LLP
258 Saint Nicholas Avenue, No. 8A
New York, NY 10027-5353

POA ACCEPTANCE LETTER

OC000000075172483

Date Mailed: 05/15/2015

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 05/12/2015.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/mbeyene/

To: docketing@hanchukkheit.com,,
From: PAIR_eOfficeAction@uspto.gov
Cc: PAIR_eOfficeAction@uspto.gov
Subject: Private PAIR Correspondence Notification for Customer Number 122870

May 15, 2015 05:38:58 AM

Dear PAIR Customer:

Hanchuk Kheit LLP
258 Saint Nicholas Avenue, No. 8A
New York, NY 10027-5353
UNITED STATES

The following USPTO patent application(s) associated with your Customer Number, 122870 , have new outgoing correspondence. This correspondence is now available for viewing in Private PAIR.

The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

Disclaimer:
The list of documents shown below is provided as a courtesy and is not part of the official file wrapper. The content of the images shown in PAIR is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
13599647	N570	05/15/2015	67979.U2
	N570	05/15/2015	67979.U2

To view your correspondence online or update your email addresses, please visit us anytime at https://sportal.uspto.gov/secure/myportal/privatepair.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov with 'e-Office Action' on the subject line or call 1-866-217-9197 during the following hours:

Monday - Friday 6:00 a.m. to 12:00 a.m.

Thank you for prompt attention to this notice,

UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT APPLICATION INFORMATION RETRIEVAL SYSTEM

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/599,617	08/30/2012	C. Douglas YEAGER	Simplytapp0002US1	1919

122870 7590 10/06/2015

Hanchuk Kheit LLP
258 Saint Nicholas Avenue, No. 8A
New York, NY 10027-5353

EXAMINER	
PUTTAIAH, ASHA	

ART UNIT	PAPER NUMBER
3695	

NOTIFICATION DATE	DELIVERY MODE
10/06/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@hanchukkheit.com

Office Action Summary	Application No. 13/599,647	Applicant(s) YEAGER, C. DOUGLAS	
	Examiner ASHA PUTTAIAH	Art Unit 3695	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 August 2012 and 15 April 2013*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-29* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-29* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *30 August 2012* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *11/27/2012, 11/27/2012*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

1. The present application is being examined under the pre-AIA first to invent provisions.

2. The following is a non-final, first office action in response to the application filed 30 August 2012 and the preliminary amendment of 15 April 2013.

The applicant's claim for benefit of provisional application US 61685863 filed 26 March 2012, US 61573476 filed 6 September 2011, and US 61575846 filed 30 August 2011 has been received and acknowledged.

Claims 1-29 have been examined and are pending.

Specification

3. The use of the trademark VISA® and MASTERCARD® has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology.

4. Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Claim Rejections - 35 USC § 112

5. The following is a quotation of 35 U.S.C. 112(b):

> (B) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1-29 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

7. Claims 1, 2, 3, 8, 23 and 28 recite acronyms such as POS and HSM which have not been defined upon first use in the claim. As such the metes and bounds of the claim are not clear. Examiner will interpret as a label. Claims 2, 4-27 and 29 are rejected by virtue of their dependency on a rejected independent claim.

8. Claims 25 recite an ISO standard. The limitation specifying an ISO standard (ISO7816-4) render the claim indefinite as the ISO standard is an industry standard which can change upon updates and is therefore, transitory-in-nature. Consequently, the ISO standard limitation without a set-in-stone definition renders the metes and bounds of the claim confusing.

Claim Rejections - 35 USC § 101

9. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

10. **Claims 1-27** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

11. When considering subject matter eligibility under 35 U.S.C. 101, (1) it must be determined whether the claim is directed to one of the four statutory categories of invention, i.e., process, machine, manufacture, or composition of matter. If the claim does fall within one of the statutory categories, (2a) it must then be determined whether the claim is directed to a judicial exception (i.e., law of nature, natural phenomenon, and abstract idea), and if so (2b), it must additionally be determined whether the claim is a patent-eligible application of the exception. If an abstract idea is present in the claim, any element or combination of elements in the claim must be sufficient to ensure that the claim amounts to significantly more than the abstract idea itself. Examples of abstract ideas include fundamental economic practices; certain methods of organizing human activities; an idea itself; and mathematical relationships/formulas. *Alice Corporation Pty. Ltd. v. CLS Bank International, et al.*, 573 U.S. ____ (2014).

12. The claimed invention is directed to a judicial exception (i.e. a law of nature, a natural phenomenon, or an abstract idea) without significantly more. In the

instant case, the claim(s) as a whole, considering all claim elements both individually and in combination, do not amount to significantly more than an abstract idea.

13. (1) In the instant case, the claims are directed towards payment and authorization methods using cryptography.

14. (2a) Payment systems and authorization of payments is akin to comparing new and store information and using rules to identify options and an algorithm for calculating parameters indicating an abnormal condition. As such, the claims include an abstract idea.

15. (2b) In the instant case, Claims 1-2, 3-27 and 28-29 are directed to processes. The invention is directed to *methods for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction comprising: using a remote permanent cryptographic key to calculate an expected cryptogram, wherein the expected cryptogram is expected to comprise at least a portion of the digital credential data, wherein the remote permanent cryptographic key is persistently stored at a remote source that is remote from the mobile device and wherein there is no duplicate local permanent cryptographic key persistently stored locally to the mobile device; performing an interrogation between the point-of-sale terminal and the mobile device comprising: sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device*

requesting the digital credential data wherein the at least one POS command communication conforms to a card specification; and

sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal comprising the expected cryptogram as the at least a portion of the digital credential data; wherein the financial transaction is authorized.

16. Additionally, the claims do not include additional elements that are sufficient to amount to significantly more than the judicial exception of abstract idea because the claims do not include an improvement to another technology or technical field, an improvement to the functioning of the computer itself, or meaningful limitations beyond generally linking the use of an abstract idea to a particular technological environment.

17. Further, note that the limitations, in the instant claims, are done by the generically recited computing devices. The limitations are merely instructions to implement the abstract idea on a computer and require no more than a generic computer to perform generic computer functions that are well-understood, routine and conventional activities previously known to the industry. Therefore, claims 1-27 are rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter.

Claim Rejections - 35 USC § 102

18. The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

19. **Claims 1, 2, and 28** are rejected under pre-AIA 35 U.S.C. 102b as being anticipated by US 20080040285 A1, Wankmueller hereinafter referred to as Wankmueller.

20. **Claim 1**

Wankmueller discloses a *method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction comprising:*

- *using a remote permanent cryptographic key to calculate an expected cryptogram, wherein the expected cryptogram is expected to comprise at least a portion of the digital credential data, wherein the remote permanent cryptographic key is persistently stored at a remote source that is remote from the mobile device and wherein there is no duplicate local permanent cryptographic key persistently stored locally to the mobile device;* (See at least

Wankmueller, Fig. 1, PIN, application cryptogram, [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)

- *performing an interrogation between the point-of-sale terminal and the mobile device comprising:*
    - *sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device requesting the digital credential data wherein the at least one POS command communication conforms to a card specification; and* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)
    - *sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal comprising the expected cryptogram as the at least a portion of the digital credential data;* (See at least Wankmueller, Fig. 1, [0017-0019] application cryptogram)
- *wherein the financial transaction is authorized.* (*See* at least Wankmueller, Fig. 1, authorize transaction)

21. Claim 2

Wankmueller discloses the invention as claimed above in Claim 1.

Wankmueller further discloses:

- *……a further step that precedes the performing the interrogation step, the further step comprising:*
  - *sending the remote permanent cryptographic key to the mobile device from the remote source; and* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)
  - *transiently caching the remote permanent cryptographic key in the mobile device as a cached transient permanent cryptographic key;* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram) *and*
- *wherein:*
  - *the step of sending through the communication channel the at least one POS command communication comprises sending unpredictable data;* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, [0014-0016] pin input,

unpredictable data, generate encryption key [0017-0019] application cryptogram)

- *the step of sending through the communication channel the at least one POS command communication comprises sending a request for an expected cryptogram, wherein the expected cryptogram is expected to be calculated by the mobile device, at least in part, from the unpredictable data; and* (See at least Wankmueller, Fig. 1, application cryptogram, convert application cryptogram to an authentication code, positive response)
- *the step of sending through the communication channel the at least one device response communication from the mobile device to the point-of-sale terminal comprises sending the expected cryptogram calculated, at least in part, from the unpredictable data and, at least in part, from the cached transient cryptographic key. ;* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)

22. Claim 28

Wankmueller discloses a *method for acquiring digital credential data by a point-of-sale terminal from a secure mobile device for authorization of a financial transaction comprising:*

performing an interrogation between the point-of-sale terminal and the secure mobile device comprising:

- *sending through a communication channel at least one POS command communication from the point-of-sale terminal to the secure mobile device wherein the at least one POS command communication conforms to a card specification, and the at least one POS command communication comprising (a) a request for the digital credential data, wherein the digital credential data that is expected to comprise an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data, and, at least in part, from a permanent cryptographic key and (b) the unpredictable data; and* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)
- *sending through the communication channel at least one device response communication from the secure mobile device to the point-of-sale terminal, the at least one device response communication comprising at least a portion of the digital credential*

data that comprises the expected cryptogram; (See at least Wankmueller, Fig. 1, [0017-0019] application cryptogram)

- *in a step that follows the step of performing an interrogation, a secure mobile device transmitting step comprising sending over a second communication channel the unpredictable data from the secure mobile device to a remote application system;* (See at least Wankmueller, Fig. 1, PIN, validate pin [0014-0016] pin input, unpredictable data, generate encryption key)
- *in a step that follows the step of performing an interrogation, a point-of-sale terminal transmitting step comprising sending over a third communication channel an authorization request from the point of sale terminal to the remote application system, the authorization request comprising the expected cryptogram and the unpredictable data;* (See at least Wankmueller, Fig. 1, application cryptogram, convert application cryptogram to an authentication code, positive response)

- *in a step that follows the secure mobile device transmitting step and the point-of-sale terminal transmitting step, a corroborative authorizing step comprising:*
    - *verifying a correctness of the expected cryptogram by the application system;* (See at least Wankmueller, Fig. 1,

application cryptogram, convert application cryptogram to an authentication code, positive response)

- *verifying a correctness of the unpredictable data by the application system by comparing the unpredictable data sent over the second communication channel with the unpredictable data sent over the third communication channel; and* (See at least Wankmueller, Fig. 1, PIN, validate pin [0014-0016] pin input, unpredictable data, generate encryption key)
- *sending through the third communication channel an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable data and at least in part by the verifying of the correctness of the expected cryptogram;* (See at least Wankmueller, Fig. 1, application cryptogram, convert application cryptogram to an authentication code, positive response)

- *wherein the financial transaction is authorized.* (See at least Wankmueller, Fig. 1, authorize transaction)

Claim Rejections - 35 USC § 103

23. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

24. **Claims 3-24, 27 and 29** are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Wankmueller further in view of US 20040143550 A1, Creamer et al. hereinafter referred to as Creamer.

25. **Claim 3**

Wankmueller discloses a *method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction comprising:*

- *performing an interrogation between the point-of-sale terminal and the mobile device comprising:*
  - *sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device wherein the at least one POS command communication conforms to a card specification, and the at least one POS command communication comprising (a) a*

request for the digital credential data, wherein the digital credential data is expected to comprise an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data, and, at least in part, from a permanent cryptographic key and (b) the unpredictable data; and (See at least Wankmueller, Fig. 1, PIN, application cryptogram, [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)

- *wherein the financial transaction is authorized*(See at least Wankmueller, Fig. 1, authorize transaction)

Wankmueller does not directly disclose the following; however, Creamer teaches:

- *sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal, the at least one device response communication comprising at least a portion of the digital credential data that comprises an unexpected cryptogram that is different from the expected cryptogram, substituted in place of the expected cryptogram;.* (See at least Creamer, [0043] bar code … PIN and transaction amount)

The Supreme Court has supported in *KSR International Co. Teleflex Inc. (KSR), 550US___, 82 USPQ2d 1385 (2007),* that merely applying a known technique to a known method, yield predictable results, render the claimed invention obvious over such combination. In the instant case, Wankmueller discloses a method and apparatus of conducting a secure transaction. *Creamer* is merely an another method and device of conducting a secure transaction with a barcode cryptogram feature. One of ordinary skill in the art would clearly recognize that this combination would lead to a predictable result (i.e. method and device of conducting a secure transaction with a barcode cryptogram feature). As such the claimed invention is obvious over Wankmueller */ Creamer.*

26. Claim 4

Wankmueller and Creamer disclose the invention as claimed above in Claim 3. Wankmueller does not directly disclose the following; however, Creamer teaches:

- *wherein the unpredictable data comprises an unpredictable number.* (See at least Creamer, [0043] bar code … PIN and transaction amount)

27. Claim 5

Wankmueller and Creamer disclose the invention as claimed above in Claim 3. Wankmueller does not directly disclose the following; however, Creamer teaches:

- *wherein the unpredictable data comprises a transaction amount.* (See at least Creamer, [0043] bar code … PIN and transaction amount)

28. Claim 6

Wankmueller and Creamer disclose the invention as claimed above in Claim 3. Wankmueller does not directly disclose the following; however, Creamer teaches:

- *further comprising a mobile device preparation step that precedes the performing an interrogation step, the mobile device preparation step comprising exchanging critical data between a remote source and the mobile device, wherein the critical data comprises data used to formulate at least a portion of the digital credential data as a local portion of the digital credential data and the critical data are dynamic over a life of the digital credential.* (See at least Creamer, [0043] bar code … PIN and transaction amount[0049] merchant …from bar code… authenticate user…)

29. Claim 7

Wankmueller and Creamer disclose the invention as claimed above in Claim 6.

Wankmueller does not directly disclose the following; however, Creamer teaches:

- *wherein the local portion of the digital credential data comprises a predetermined cryptogram, wherein the predetermined cryptogram is formulated without the use of the unpredictable data, as the unexpected cryptogram.* (See at least Creamer, [0043] bar code … PIN and transaction amount[0049] merchant …from bar code… authenticate user…)

30. Claim 8

Wankmueller and Creamer disclose the invention as claimed above in Claim 6.

Wankmueller further discloses:

- *wherein the mobile device preparation step further comprises:*
  - *creating remote unpredictable data in a remote application system wherein the remote application system is the remote source;* (See at least Wankmueller, Fig. 1, PIN, application cryptogram,

[0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)

- *sending the remote unpredictable data from application system to an HSM;* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)
- *calculating a predetermined cryptogram in the HSM without the use of the unpredictable data;* (See at least Wankmueller, Fig. 3, [0032-0033] mobile device identifier, personalization data)
- *sending the predetermined cryptogram from the HSM to the remote application system;* (See at least Wankmueller, Fig. 3, [0032-0033] mobile device identifier, personalization data…communication)

Wankmueller does not directly disclose the following; however, Creamer teaches:

- *sending at least a portion of the predetermined cryptogram from the remote application system to the mobile device as a portion of the critical data; and*(See at least Creamer, [0043] bar code … PIN and transaction amount[0049] merchant …from bar code… authenticate user…)

- *wherein the local portion of the digital credential data comprises the predetermined cryptogram and the unexpected cryptogram comprises the predetermined cryptogram.* (See at least Creamer, [0043] bar code … PIN and transaction amount[0049] merchant …from bar code… authenticate user…)

31. Claim 9

Wankmueller and Creamer disclose the invention as claimed above in Claim 6.

Wankmueller further discloses:

- *creating a predetermined cryptogram in a remote application system, wherein the predetermined cryptogram is formulated without the use of the unpredictable data,* (See at least Wankmueller, Fig. 3, [0032-0033] mobile device identifier, personalization data)

Wankmueller does not directly disclose the following; however, Creamer teaches:

- *wherein the remote application system is the remote source;* (See at least Creamer, [0043] bar code … PIN and transaction amount[0049] merchant …from bar code… authenticate user…)

- *sending at least a portion the predetermined cryptogram from the remote application system to the mobile device as a portion of the critical data; and* (See at least Creamer, [0043] bar code … PIN and transaction amount[0049] merchant …from bar code… authenticate user…)
- *wherein the local portion of the digital credential data comprises the predetermined cryptogram as the unexpected cryptogram.* (See at least Creamer, [0043] bar code … PIN and transaction amount[0049] merchant …from bar code… authenticate user…)

32. Claim 10

Wankmueller and Creamer disclose the invention as claimed above in Claim 6. Wankmueller further discloses:

- *wherein the critical data comprises a set of possible predetermined cryptograms, which are formulated without the use of the unpredictable data;* (See at least Wankmueller, Fig. 3, [0032-0033] mobile device identifier, personalization data)
- *the method further comprises a logical step of logically determining, in the mobile device, which of the possible predetermined cryptograms within the set of predetermined*

cryptograms to designate as the unexpected cryptogram; (See at least Wankmueller, Fig. 1, PIN, application cryptogram, authorize transaction [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)

- *wherein the logical step is based, at least in part, on the unpredictable data; and* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, authorize transaction [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)

Wankmueller does not directly disclose the following; however, Creamer teaches:

- *wherein the local portion of the digital credential data comprises the predetermined cryptogram as the unexpected cryptogram..* (See at least Creamer, [0043] bar code … PIN and transaction amount[0049] merchant …from bar code… authenticate user…)

33. Claim 11

Wankmueller and Creamer disclose the invention as claimed above in Claim 6.

Wankmueller further discloses:

- *wherein the critical data comprises a set of possible predetermined cryptograms, which are formulated without the use of the unpredictable data, and card risk management data; and* (See at least Wankmueller, Fig. 3, [0032-0033] mobile device identifier, personalization data)
- *the method further comprises a logical step of logically determining, in the mobile device, which of the possible predetermined cryptograms within the set of possible predetermined cryptograms to designate as the unexpected cryptogram;* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, authorize transaction [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)

Wankmueller does not directly disclose the following; however, Creamer teaches:

- *wherein the logical step of is based, at least in part, on the unpredictable data or based, at least in part, on the card risk management data; and* . (See at least Creamer, [0043] bar code … [0049] merchant …from bar code… authenticate user…)
- *wherein the local portion of the digital credential data comprises the predetermined cryptogram as the unexpected*

cryptogram. (See at least Creamer, [0043] bar code … PIN and transaction amount[0049] merchant …from bar code… authenticate user…)

34. Claim 12

Wankmueller and Creamer disclose the invention as claimed above in Claim 6.

Wankmueller further discloses:

- *wherein the mobile device preparation step further comprises transiently storing at least a portion of the critical data on the mobile device, wherein the mobile device does not persistently store the at least a portion of critical data.* (See at least Wankmueller, [0028] secret data)

35. Claim 13

Wankmueller and Creamer disclose the invention as claimed above in Claim 6.

Wankmueller further discloses:

- *wherein the local portion of the digital credential data comprises an unpredictable cryptogram as the unexpected cryptogram, wherein the unpredictable cryptogram is calculated, at least in part, using a temporary cryptographic key.* (See at least Wankmueller, Fig. 1, PIN, validate pin

[0014-0016] pin input, unpredictable data, generate encryption key)

36. Claim 14

Wankmueller and Creamer disclose the invention as claimed above in Claim 6.

Wankmueller further discloses:

- *wherein the mobile device preparation step further comprises:*
  - *creating a temporary cryptographic key in a remote application system wherein the remote application system is the remote source;* (See at least Wankmueller, Fig. 1, PIN, validate pin [0014-0016] pin input, unpredictable data, generate encryption key)
  - *sending at least a portion of the temporary cryptographic key from the remote application system to the mobile device as a portion of the critical data; and*(See at least Wankmueller, Fig. 1, PIN, application cryptogram, authorize transaction [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)

Wankmueller does not directly disclose the following; however, Creamer teaches:

- *wherein the local portion of the digital credential data comprises an unpredictable cryptogram as the unexpected cryptogram, wherein the unpredictable calculated cryptogram is calculated, at least in part, using the temporary cryptographic key and the unexpected cryptogram comprises the unpredictable cryptogram.* (See at least Creamer, [0043] bar code … PIN and transaction amount[0049] merchant …from bar code… authenticate user…)

37. Claim 15

Wankmueller and Creamer disclose the invention as claimed above in Claim 6. Wankmueller further discloses:

- *wherein the critical data comprises a temporary cryptographic key;* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, authorize transaction [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)
- *the method further comprises a step of calculating a plurality of unpredictable cryptograms that are calculated, in at least*

part, using the temporary cryptographic key, and, in at least part, using a calculation formula determined from a set of calculation formulas; and(See at least Wankmueller, Fig. 1, PIN, application cryptogram, authorize transaction [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)

- *the method further comprises a logical step of logically determining, in the mobile device, which of the plurality unpredictable cryptograms to designate as the unpredictable cryptogram;* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, authorize transaction [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)
- *wherein the step of logically determining a decision is made based, at least in part, on the unpredictable data;* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, authorize transaction [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)*and*

Wankmueller does not directly disclose the following; however, Creamer teaches:

- *wherein the local portion of the digital credential data comprises the designated unpredictable cryptogram and the unexpected cryptogram comprises the designated unpredictable cryptogram.* (See at least Creamer, [0043] bar code … PIN and transaction amount[0049] merchant …from bar code… authenticate user…)

38. Claim 16

Wankmueller and Creamer disclose the invention as claimed above in Claim 6.

Wankmueller further discloses:

- *wherein the critical data comprises a temporary cryptographic key and card risk management data; and*(See at least Wankmueller, Fig. 3, [0032-0033] mobile device identifier, personalization data)
- *the method further comprises a step of calculating a plurality of unpredictable cryptograms that are calculated, in at least part, using the temporary cryptographic key, and, in at least part, using a calculation formula determined from a set of calculation formulas;* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, authorize transaction [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)

- *the method further comprises a logical step of logically determining, in the mobile device, which of the plurality of unpredictable cryptograms to designate as the unpredictable cryptogram;* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, authorize transaction [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)
- *wherein the logical step is made based, at least in part, on the unpredictable data or based, at least in part, on the card risk management data; and* See at least Wankmueller, Fig. 3, [0032-0033] mobile device identifier, personalization data..authorization)

Wankmueller does not directly disclose the following; however, Creamer teaches:

- *wherein the local portion of the digital credential data comprises the designated local unpredictable cryptogram and the unexpected cryptogram comprises the designated unpredictable cryptogram.* (See at least Creamer, [0043] bar code … PIN and transaction amount[0049] merchant …from bar code… authenticate user…)

39. Claim 17

Wankmueller and Creamer disclose the invention as claimed above in Claim 6.

Wankmueller further discloses:

- *creating a predetermined* cryptogram *in the mobile device,* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, authorize transaction [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram
- *wherein the predetermined cryptogram is formulated without the use of the unpredictable data; and* (See at least Wankmueller, Fig. 3, [0032-0033] mobile device identifier, personalization data)
- *sending at least a portion of the predetermined cryptogram from the mobile device to a remote application system as a portion of the critical data;* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, authorize transaction [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)
- *wherein the remote application system is the remote source; and*(See at least Wankmueller, Fig. 1/ Fig 3)

Wankmueller does not directly disclose the following; however, Creamer teaches:

- *wherein the local portion of the digital credential data comprises the predetermined cryptogram as the unexpected cryptogram.* (See at least Creamer, [0043] bar code … PIN and transaction amount)

40. Claim 18

Wankmueller and Creamer disclose the invention as claimed above in Claim 6. Wankmueller further discloses:

- *wherein the mobile device preparation step further comprises:*
  - *creating a temporary cryptographic key in the mobile device;* (See at least Wankmueller, Fig. 1, PIN, validate pin [0014-0016] pin input, unpredictable data, generate encryption key)
  - *sending at least a portion of the temporary cryptographic key from the mobile device to a remote application system as a portion of the critical data;* (See at least Wankmueller, Fig. 1, PIN, validate pin [0014-0016] pin input, unpredictable data, generate encryption key)
- *wherein the remote application system is the remote source;* (See at least Wankmueller, Fig. 1/ Fig 3)*and*

Wankmueller does not directly disclose the following; however, Creamer teaches:

- *wherein the local portion of the digital credential data comprises an unpredictable cryptogram as the unexpected cryptogram,* (See at least Creamer, [0043] bar code … PIN and transaction amount)
- *wherein the unpredictable cryptogram is calculated, at least in part, using the temporary cryptographic key and the unexpected cryptogram comprises the unpredictable cryptogram.* (See at least Creamer, [0043] bar code … PIN and transaction amount)

41. Claim 19

Wankmueller and Creamer disclose the invention as claimed above in Claim 3.

Wankmueller further discloses:

an authorizing step that follows the step of performing the interrogation, the authorizing step comprising:

- *sending an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system, wherein the unexpected cryptogram comprises a predetermined cryptogram that is formulated without the use*

of the unpredictable data; (See at least Wankmueller, Fig. 1, application cryptogram, convert application cryptogram to an authentication code, positive response)

- *verifying a correctness of the predetermined cryptogram by the application system (a) by comparing the predetermined cryptogram with a previously stored reference predetermined cryptogram and (b) without reference to the unpredictable data from the point-of-sale terminal; and* (See at least Wankmueller, Fig. 1, application cryptogram, convert application cryptogram to an authentication code, positive response)
- *sending an authorization response from the remote application system to the point-of- sale wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the predetermined cryptogram.* (See at least Wankmueller, Fig. 1, authorize transaction)

42. Claim 20

Wankmueller and Creamer disclose the invention as claimed above in Claim 3.

Wankmueller further discloses:

further comprising an authorizing step that follows the step of performing the interrogation, the authorizing step comprising:

- *sending an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system,* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, authorize transaction [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)
- *wherein the unexpected cryptogram comprises an unpredictable cryptogram that is calculated using, at least in part, a temporary cryptographic key;* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, authorize transaction [0014-0016] pin input, unpredictable data, generate encryption key [0017--0019] application cryptogram)
- *verifying a correctness of the unpredictable cryptogram by the remote application system wherein the unpredictable cryptogram is compared with a result of an unpredictable cryptogram calculation;* (See at least Wankmueller, Fig. 1, application cryptogram, convert application cryptogram to an authentication code, positive response)

- *sending an authorization response from the remote application system to the point-of- sale wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable cryptogram.* (See at least Wankmueller, Fig. 1, application cryptogram, convert application cryptogram to an authentication code, positive response)

43. Claim 21

Wankmueller and Creamer disclose the invention as claimed above in Claim 3.

Wankmueller further discloses:

further comprising a corroborative authorizing step that follows the step of performing the interrogation, the corroborative authorizing step comprising:

- *sending through a second communication channel an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of- sale terminal to a remote application system;* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, authorize transaction [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)

- *sending through a third communication channel the unpredictable data from the mobile device to the remote application system;* (See at least Wankmueller, Fig. 1, PIN, application cryptogram, authorize transaction [0014-0016] pin input, unpredictable data, generate encryption key [0017-0019] application cryptogram)
- *verifying a correctness of the unexpected cryptogram in the remote application system;* (See at least Wankmueller, Fig. 1, PIN, validate pin [0014-0016] pin input, unpredictable data, generate encryption key)
- *verifying a correctness of the unpredictable data in the remote application system by comparing the unpredictable data sent through the second communication channel with the unpredictable data sent through the third communication channel;* (See at least Wankmueller, Fig. 1, application cryptogram, convert application cryptogram to an authentication code, positive response)
- *sending through the second communication channel an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable data and, at*

least in part, by the verifying of the correctness of the unexpected cryptogram. (See at least Wankmueller, Fig. 1, application cryptogram, convert application cryptogram to an authentication code, positive response)

44. Claim 22

Wankmueller and Creamer disclose the invention as claimed above in Claim 21. Wankmueller does not directly disclose the following; however, Creamer teaches:

a verifying a transaction amount step that follows the step of performing an interrogation and precedes the corroborative authorizing step, the verifying transaction amount step comprising:

- *displaying transaction amount data to a display on the mobile device wherein the transaction amount data is at least a portion of the unpredictable data;* (See at least Creamer, [0043] bar code … PIN and transaction amount[0049] merchant …from bar code… authenticate user…)
- *requesting verification of the transaction amount data from a card holder by the mobile device display screen;* (See at least Creamer, [0043] bar code … PIN and transaction

amount[0049] merchant ...from bar code... authenticate user...)

- *sending the result of the requesting verification of the transaction amount data to a remote application system as input transaction amount data; and* (See at least Creamer, [0043] bar code ... PIN and transaction amount[0049] merchant ...from bar code... authenticate user...)
- *wherein the corroborative authorizing step comprises determining, at least in part, an accuracy of the result of the verification step by using the input of the transaction amount data.* (See at least Creamer, [0043] bar code ... PIN and transaction amount[0049] merchant ...from bar code... authenticate user...)

45. Claim 23

Wankmueller and Creamer disclose the invention as claimed above in Claim 3.

Wankmueller further discloses:

further comprising an authorizing step that follows the step of performing an interrogation, the authorizing step comprising:

- *sending an authorization request comprising the unpredictable data and the unexpected cryptogram from the*

point-of-sale terminal to a remote application system, wherein the unexpected cryptogram comprises a predetermined cryptogram; (See at least Wankmueller, Fig. 1, PIN, validate pin [0014-0016] pin input, unpredictable data, generate encryption key)

- *verifying a correctness of the predetermined cryptogram wherein the unpredictable data from the point-of sale (a) is substituted by the application system with a previously created unpredictable data that was previously used to calculate the predetermined cryptogram; and* (See at least Wankmueller, Fig. 1, application cryptogram, convert application cryptogram to an authentication code, positive response)
- *subsequently (b) is sent with the predetermined cryptogram to the HSM for cryptogram correctness verification; and*

  and (See at least Wankmueller, Fig. 1, PIN, validate pin [0014-0016] pin input, unpredictable data, generate encryption key)
- *sending an authorization response from the remote application system to the point-of- sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the*

predetermined cryptogram. (See at least Wankmueller, Fig. 1, application cryptogram, convert application cryptogram to an authentication code, positive response)

46. Claim 24

Wankmueller and Creamer disclose the invention as claimed above in Claim 3.

Wankmueller further discloses:

- *an authorizing step that follows the step of performing an interrogation, the authorizing step comprising sending the unpredictable data from the mobile device to a remote application system.* (See at least Wankmueller, Fig. 1, application cryptogram, convert application cryptogram to an authentication code, positive response)

47. Claim 27

Wankmueller and Creamer disclose the invention as claimed above in Claim 3.

Wankmueller does not directly disclose the following; however, Creamer teaches:

- *wherein the mobile device does not access a local persistently stored permanent cryptographic key that is expected to be used to calculate the expected cryptogram wherein the expected* cryptogram *is expected to be*

contained within the at least a portion of the digital credential. (See at least Creamer, [0043] bar code … PIN and transaction amount)

48. Claim 29

Wankmueller and Creamer disclose the invention as claimed above in Claim 28.

Wankmueller does not directly disclose the following; however, Creamer teaches:

further comprising a verifying step that follows the step of performing an interrogation and precedes the corroborative authorizing step, the verifying step comprising:

- *displaying transaction amount data to the secure mobile device display screen wherein the transaction amount data is comprised within the unpredictable data;* (See at least Creamer, [0043] bar code … PIN and transaction amount)
- *requesting verification of the transaction amount data from a card holder by the secure mobile device display screen;* (See at least Creamer, [0049] merchant …from bar code… authenticate user…)
- *sending the result of the requesting verification of the transaction amount data to a remote application system as input of the transaction amount data; and*(See at least

Creamer, [0049] merchant ...from bar code... authenticate user...)

- *wherein the corroborative authorizing step comprises determining, at least in part, the correctness of the result of the verification step by using the input of the transaction amount data.* (See at least Creamer, [0049] merchant ...from bar code... authenticate user...)

The Supreme Court has supported in *KSR International Co. Teleflex Inc. (KSR), 550US___, 82 USPQ2d 1385 (2007),* that merely applying a known technique to a known method, yield predictable results, render the claimed invention obvious over such combination. In the instant case, Wankmueller discloses a method and apparatus of conducting a secure transaction. *Creamer* is merely an another method and device of conducting a secure transaction with a barcode cryptogram feature. One of ordinary skill in the art would clearly recognize that this combination would lead to a predictable result (i.e. method and device of conducting a secure transaction with a barcode cryptogram feature). As such the claimed invention is obvious over Wankmueller / *Creamer.*

49. **Claims 25 and 26** are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Wankmueller further in view of Creamer further in view of US 20120109764, Martin et al. hereinafter referred to as Martin.

50. **Claim 25**

Wankmueller and Creamer disclose the invention as claimed above in Claim 3.

Wankmueller does not directly disclose the following; however, Martin teaches:

- *wherein the POS command communication conforms to ISO7816-4 data protocol and the device response communication conforms to ISO7816-4 data protocol. (See at least* Martin, [0008] NFC, ISO-7816)

The Supreme Court has supported in *KSR International Co. Teleflex Inc. (KSR), 550US___, 82 USPQ2d 1385 (2007),* that merely applying a known technique to a known method, yield predictable results, render the claimed invention obvious over such combination. In the instant case, Wankmueller discloses a method and apparatus of conducting a secure transaction. Martin is merely an another method and device of conducting a secure transaction which uses a known protocol standard/technology to establish communications. One of ordinary skill in the art would clearly recognize that this combination would lead to a predictable result (i.e. method and device of conducting a secure

transaction which uses a known protocol standard to establish communications). As such the claimed invention is obvious over Wankmueller / Martin.

51. Claim 26

Wankmueller and Creamer disclose the invention as claimed above in Claim 3.

Creamer discloses short range wireless communication. ([0055])

Wankmueller does not directly disclose the following; however, Martin teaches:

wherein the communication channel comprises a near- field communication channel. (See at least Martin, [0008] NFC, ISO-7816)

The Supreme Court has supported in *KSR International Co. Teleflex Inc. (KSR), 550US___, 82 USPQ2d 1385 (2007),* that merely applying a known technique to a known method, yield predictable results, render the claimed invention obvious over such combination. In the instant case, Wankmueller discloses a method and apparatus of conducting a secure transaction. Martin is merely an another method and device of conducting a secure transaction which uses a known protocol standard/technology to establish communications. One of ordinary skill in the art would clearly recognize that this combination would lead to a predictable result (i.e. method and device of conducting a secure transaction which uses a known protocol standard to establish

communications). As such the claimed invention is obvious over Wankmueller / Martin.

Conclusion

52. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US 5636280

53. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ASHA PUTTAIAH whose telephone number is (571)270-1352. The examiner can normally be reached on Monday- Friday 8:00am - 5:00 pm EST.

54. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ryan Donlon can be reached on (571) 270-3602. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

55. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ASHA PUTTAIAH/
Examiner, Art Unit 3695

Notice of References Cited	Application/Control No. 13/599,647	Applicant(s)/Patent Under Reexamination YEAGER, C. DOUGLAS	
	Examiner ASHA PUTTAIAH	Art Unit 3695	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-5,636,280 A	06-1997	Kelly; Tadhg	G06F21/31	380/281
*	B	US-2012/0109764 A1	05-2012	Martin; Philippe	G06Q20/204	705/17
*	C	US-2004/0143550 A1	07-2004	Creamer, Thomas E.	G06Q20/04	705/41
*	D	US-2008/0040285 A1	02-2008	Wankmueller; John	G06Q20/32	705/67
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author. Title Date, Publisher. Edition or Volume. Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13599647
	Filing Date	2012-08-30
	First Named Inventor	YEAGER, C. Douglas
	Art Unit	2617
	Examiner Name	A.Puttaiah
	Attorney Docket Number	67979.U2

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6199762	B1	2001-03-13	Hohle	
	2	7774231	B2	2010-08-10	Pond et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030163708	A1	2003-08-28	Tang	
	2	20040118914	A1	2004-06-24	Smith et al.	
	3	20060224470	A1	2006-10-05	Garcia Ruano et al.	
	4	20070075133	A1	2007-04-05	Yeager	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.P./

Receipt date: 11/27/2012	Application Number	13599647 13599647 - GAU: 3695
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2012-08-30
	First Named Inventor	YEAGER, C. Douglas
(Not for submission under 37 CFR 1.99)	Art Unit	2617
	Examiner Name	A.Puttaiah
	Attorney Docket Number	67979.U2

	5	20080046367	A1	2008-02-21	Billmaier et al.	
	6	20080238610	A1	2008-10-02	Rosenberg	
	7	20090044012	A1	2009-02-12	Bishop et al.	
	8	20100274726	A1	2010-10-28	Florek et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. **Add**

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button **Add**

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Asha Puttaiah/	Date Considered	09/29/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

All REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.P./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	20	("20040118914" | "20070266131" | "20070278291" | "20110140841" "20060022033" | "20090124234" "20100185545" | "20100274726" "6199762" | "7774231" | "20100207742" | "20080046367" | "20070075133" "20090006262" | "20110112918" "20060224470" | "20030163708" "20080238610" | "20090044012" "20080219444").PN.	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:04
S2	84	"pos command"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:05
S3	2	"expected cryptogram"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:06
S4	0	"pos command" with (expected adj value adj cryptogram)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:07
S5	0	"pos command" same (expected adj value adj cryptogram)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:07
S6	0	"pos command" same (expected with value with cryptogram)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:07
S7	1	"pos command" same (cryptogram)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:07
S8	1	"pos command" and cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:07
S9	1	"unexpected cryptogram"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:08
S11	20	cryptogram same value same expected	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:09
S12	5	cryptogram same value same expected and (mobile with point)	US-PGPUB; USPAT;	AND	OFF	2015/09/24 22:09

			USOCR			
S13	20	cryptogram same (mobile with point)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:10
S14	6	S1 and calculat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:19
S15	123874	(cryptogram or authenticat$5) calculatS3	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:23
S16	20011	(cryptogram or authenticat$5) same calculat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:24
S17	11595	(cryptogram or authenticat$5) with calculat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:24
S18	101	(cryptogram or authenticat$5) with calculat$3 and (permanent near4 key)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:25
S19	96	(cryptogram or authenticat$5) with calculat$3 and (permanent near3 key)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:25
S20	1	(cryptogram or authenticat$5) with calculat$3 and (remote with permanent near3 key)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:26
S21	1	(cryptogram or authenticat$5) with calculat$3 and (remote same (permanent near3 key))	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:27
S22	56	(remote same (permanent near3 key))	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:27
S23	56	(remote same (permanent near3 key))	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:28
S24	5	"pos command" and "unpredictable"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 13:26
S25	458	"unpredictable data"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 13:27
S26	0	"unpredictable data" and crytogra,	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 13:27
S27	0	"unpredictable data" and crytogram	US-	AND	OFF	2015/09/28

			PGPUB; USPAT; USOCR			13:27
S28	7	"unpredictable data" and cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 13:27
S29	29	$2expected with cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 13:29
S30	72	ISO7816-4	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 13:58
S31	4	ISO7816-4 and POS	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 14:01
S32	20	("2008/0040285").URPN.	USPAT	AND	OFF	2015/09/28 20:08
S33	143	transaction adj PIN	USPAT	AND	OFF	2015/09/28 20:12
S34	18	transaction adj PIN with amount	USPAT	AND	OFF	2015/09/28 20:12
S35	51	transaction adj PIN with amount	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:12
S36	84	"pos command"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:14
S37	0	S35 and S36	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:14
S38	0	S35 and S36	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:14
S39	18	S35 and S34	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:14
S40	0	transaction adj PIN with amount and "unpredictable data"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:15
S41	0	(transaction adj PIN with amount) and "unpredictable data"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:16
S42	0	(transaction adj PIN with amount) and "unpredictable"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:16
S43	20	("20040118914" | "20070266131" |	US-	AND	OFF	2015/09/28

		"20070278291" | "20110140841" "20060022033" | "20090124234" "20100185545" | "20100274726" "6199762" | "7774231" | "20100207742" | "20080046367" | "20070075133" "20090006262" | "20110112918" "20060224470" | "20030163708" "20080238610" | "20090044012" "20080219444").PN.	PGPUB; USPAT; USOCR			20:44
S44	0	S34 and S43	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:44
S45	4	S43 and cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:44
S46	20	("20040118914" | "20070266131" | "20070278291" | "20110140841" "20060022033" | "20090124234" "20100185545" | "20100274726" "6199762" | "7774231" | "20100207742" | "20080046367" | "20070075133" "20090006262" | "20110112918" "20060224470" | "20030163708" "20080238610" | "20090044012" "20080219444").PN.	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/29 11:08
S47	84	"pos command"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/29 11:08
S48	600	cryptogram same value	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/29 11:08

9/ 29/ 2015 4:51:15 PM
C:\ Users\ aputtaiah1\ Documents\ EAST\ Workspaces\ 13599647.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 1919

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/599,647	08/30/2012 RULE	705	3695	Simplytapp0002US1

APPLICANTS

INVENTORS

C. Douglas YEAGER, Austin, TX;

** **CONTINUING DATA** **********

This appln claims benefit of 61/685,863 03/26/2012
and claims benefit of 61/573,476 09/06/2011
and claims benefit of 61/575,846 08/30/2011

** **FOREIGN APPLICATIONS** **********

** **IF REQUIRED, FOREIGN FILING LICENSE GRANTED** ** ** SMALL ENTITY **

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ Yes ☑ No	☐ Yes ☑ No	/ASHA PUTTAIAH/ Examiner's Signature	☐ Initials	TX	24	29	3

ADDRESS

Hanchuk Kheit LLP
258 Saint Nicholas Avenue, No. 8A
New York, NY 10027-5353
UNITED STATES

TITLE

SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM

FILING FEE RECEIVED		
800	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed
PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	13599647
Filing Date	2012-08-30
First Named Inventor	YEAGER, C. Douglas
Art Unit	2617
Examiner Name	
Attorney Docket Number	67979.U2

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060022033	A1	2006-02-02	Smets et al.	
	2	20070075133	A1	2007-04-05	Yeager	
	3	20070266131	A1	2007-11-15	Mazur et al.	
	4	20070278291	A1	2007-12-06	Rans et al.	
	5	20080219444	A1	2008-09-11	Benteo et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.P./
Examiner Initials

Receipt date: 11/27/2012	Application Number	13599647	13599647 - GAU: 3695
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2012-08-30	
	First Named Inventor	YEAGER, C. Douglas	
(Not for submission under 37 CFR 1.99)	Art Unit	2617	
	Examiner Name		
	Attorney Docket Number	67979.U2	

	6	20090006262	A1	2009-01-01	Brown et al.	
	7	20090124234	A1	2009-05-14	Fisher et al.	
	8	20100185545	A1	2010-07-22	Royyuru et al.	
	9	20100207742	A1	2010-08-19	Buhot et al.	
	10	20110112918	A1	2011-05-12	Mestre et al.	
	11	20110140841	A1	2011-06-16	Bona et al	

If you wish to add additional U.S. Published Application citation information please click the Add button. **Add**

FOREIGN PATENT DOCUMENTS **Remove**

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button **Add**

NON-PATENT LITERATURE DOCUMENTS **Remove**

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.P./

Receipt date: 11/27/2012	Application Number	13599647	13599647 - GAU: 3695
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2012-08-30	
	First Named Inventor	YEAGER, C. Douglas	
(Not for submission under 37 CFR 1.99)	Art Unit	2617	
	Examiner Name		
	Attorney Docket Number	67979.U2	

	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Asha Puttaiah/	Date Considered	09/29/2015

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.P./

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13599647	YEAGER, C. DOUGLAS
	Examiner	Art Unit
	ASHA PUTTAIAH	3695

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	09/29/2015								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								
	28	✓								
	29	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13599647	YEAGER, C. DOUGLAS
	Examiner	Art Unit
	ASHA PUTTAIAH	3695

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor Search	9/27/2015	AP
East Search (please see attached)	9/29/2015	AP

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/ASHA PUTTAIAH/ Examiner.Art Unit 3695	

To: docketing@hanchukkheit.com,,
From: PAIR_eOfficeAction@uspto.gov
Cc: PAIR_eOfficeAction@uspto.gov
Subject: Private PAIR Correspondence Notification for Customer Number 122870

Oct 06, 2015 05:37:06 AM

Dear PAIR Customer:

Hanchuk Kheit LLP
258 Saint Nicholas Avenue, No. 8A
New York, NY 10027-5353
UNITED STATES

The following USPTO patent application(s) associated with your Customer Number, 122870 , have new outgoing correspondence. This correspondence is now available for viewing in Private PAIR.

The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

Disclaimer:
The list of documents shown below is provided as a courtesy and is not part of the official file wrapper. The content of the images shown in PAIR is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
13599647	CTNF	10/06/2015	Simplytapp0002US1
	892	10/06/2015	Simplytapp0002US1
	1449	10/06/2015	Simplytapp0002US1
	1449	10/06/2015	Simplytapp0002US1

To view your correspondence online or update your email addresses, please visit us anytime at https://sportal.uspto.gov/secure/myportal/privatepair.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov with 'e-Office Action' on the subject line or call 1-866-217-9197 during the following hours:

Monday - Friday 6:00 a.m. to 12:00 a.m.

Thank you for prompt attention to this notice,

UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT APPLICATION INFORMATION RETRIEVAL SYSTEM

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/599,617	08/30/2012	C. Douglas YEAGER	Simplytapp0002US1	1919

122870 7590 02/19/2016

Hanchuk Kheit LLP
258 Saint Nicholas Avenue, No. 8A
New York, NY 10027-5353

EXAMINER
PUTTAIAH, ASHA

ART UNIT	PAPER NUMBER
3695	

NOTIFICATION DATE	DELIVERY MODE
02/19/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@hanchukkheit.com

Applicant-Initiated Interview Summary	**Application No.**	**Applicant(s)**	
	13/599,647	YEAGER, C. DOUGLAS	
	Examiner	**Art Unit**	
	ASHA PUTTAIAH	3695	

All participants (applicant, applicant's representative, PTO personnel):

(1) *ASHA PUTTAIAH*. (3) *Doug Yeager*.

(2) *John Adair*. (4)_____.

Date of Interview: *11 February 2016*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☐ No.
If Yes, brief description: _____.

Issues Discussed ☒101 ☒112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *NA*.

Identification of prior art discussed: *NA*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applciants presented a brief history of the field and the problem which is attempting to be solved by the invention as well as the claims. Examiner provided suggestions for claim language and response. Applciant's will consider suggestion.

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☒ Attachment

/ASHA PUTTAIAH/ Primary Examiner, Art Unit 3695	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Power of Attorney to Transact Business with the United States Patent and Trademark Office

I hereby revoke all previous Powers of Attorney given in the application(s) identified in the attached Transmittal for Power of Attorney to One or More Registered Practitioners ("Transmittal Form").

I hereby appoint practitioners associated with the following Customer Number associated with Sprinkle IP Law Group, PC:

44654

as my/our attorney(s) or agent(s) and to transact all business before the United States Patent and Trademark Office (USPTO) in connection with any and all patents and patent applications that are assigned to **SimplyTapp, Inc.** (the "assignee's patents/patent applications") in which they shall appear, any and all assignee's patents/patent applications associated with the above-referenced customer number, and any and all patents and patent applications referenced in the attached Transmittal Form.

Please recognize or change the correspondence address for the patents and patent applications referenced in the attached Transmittal Form to the address associated with the above-referenced customer number.

The undersigned is:

- [x] Inventor or Joint Inventor
- [ ] Assignee or Person to Whom the Inventor is Under an Obligation to Assign
  *the undersigned has authority to act on behalf of the Assignee or Person to Whom the Inventor is Under an Obligation to Assign
- [ ] Legal Representative of a Deceased or Legally Incapacitated Inventor
- [ ] Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is currently being filed in this document)

The Transmittal Form may be completed and executed by one of the practitioners associated with the above-referenced customer number.

SIGNATURE OF APPLICANT		
Signature:		**Date:** 2/10/2016
Name:	**Charles Douglas Yeager**	
Title:	**Chief Executive Officer**	
Company:	**SimplyTapp, Inc.**	

PAGE 2/2 * RCVD AT 2/11/2016 11:50:50 AM [Eastern Standard Time] * SVR:W-PTOFAX-001/31 * DNIS:2702352 * CSID:15123719088 * DURATION (mm-ss):01-51

Mastercard, Ex1002, p. 254

PTOL-413A (09-08)
Approved for use through 12/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Applicant Initiated Interview Request Form

Application No.: 13/599,647 (STAPP1100-5) First Named Applicant: C. Douglas Yeager

Examiner: Asha Puttaiah Art Unit: 3695 Status of Application: Pending

Tentative Participants:

(1) Examiner Asha Puttaiah (2) Attorney John Adair, Reg. No. 48,828

(3) Doug Yeager (4)

Proposed Date of Interview: 02/11/2016 **Proposed Time:** 1:00 EST ~~AM~~/PM

Type of Interview Requested:

(1) [✓] **Telephonic** (2) [ ] **Personal** (3) [ ] **Video Conference**

Exhibit To Be Shown or Demonstrated: [ ] YES [✓] NO

If yes, provide brief description:

Issues To Be Discussed

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
(1) 101 Rejection			[ ]	[ ]	[ ]
(2) 103 Rejection	3-24, 27, 29	Wankmueller/Creamer	[ ]	[ ]	[ ]
(3)			[ ]	[ ]	[ ]
(4)			[ ]	[ ]	[ ]

[ ] Continuation Sheet Attached

Brief Description of Argument to be Presented:

Proposed Amendment to follow. Applicant would like to particularly point out specific elements not found in the prior art and would welcome any claim amendment suggestions from the examiner that would forward the prosecution.

An interview was conduction on the above-identified application on _____.

NOTE: This form should be completed by applicant and submitted to the examiner in advance of the interview (see MPEP § 713.01).

This application will not be delayed from issue because of applicant's failure to submit a written record of this interview. Therefore, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible.

/John L. Adair/	
Applicant/Applicant's Representative Signature	Examiner/SPE Signature
John L. Adair	
Typed/Printed Name of Applicant or Representative	
48,828	
Registration Number, if applicable	

This collection of information is required by 37 CFR 1.133. The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
PROPOSED AMENDMENT (NOT FOR ENTRY)	Atty. Docket No. **STAPP1100-5**

Applicants **C. Douglas Yeager**	
Application Number **13/599,647**	Date Filed **August 30, 2012**
Title **SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM**	
Group Art Unit **3695**	Examiner **Asha Puttaiah**
Confirmation Number: **1919**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

(PROPOSED AMENDMENT: NOT FOR ENTRY)

3. (Currently Amended) A method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction comprising:

receiving a first non-permanent cryptographic key at the mobile device from a remote source, wherein the first non-permanent cryptographic key is associated with an account;

storing the first non-permanent cryptographic key as a local cryptographic key;

~~performing~~ participating by the mobile device in an interrogation between the point-of-sale (POS) terminal and the mobile device comprising:

~~sending~~ receiving through a communication channel with a contactless reader at least one POS command communication from the point-of-sale terminal to the mobile device[[,]] wherein the at least one POS command communication ~~comprising~~ comprises (a) a request for the digital credential data, wherein the digital credential data comprises a first cryptogram ~~that is expected to comprise an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data, and, at least in part, from a permanent cryptographic key and (b) the unpredictable data~~; and

sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal, the at least one device response communication comprising at least a portion of the digital credential

data that comprises ~~an unexpected~~ a second cryptogram generated at the mobile device using the local cryptographic key, wherein mobile device generates the second cryptogram without using a permanent cryptographic key ~~cryptogram, substituted in place of the expected cryptogram~~;

~~wherein the financial transaction is authorized~~

receiving a second non-permanent cryptographic key at the mobile device, wherein the second non-permanent cryptographic key is associated with the account; and

changing the local cryptographic key at the mobile device prior to the mobile device participating in a subsequent interrogation.

14. (Currently Amended) The method of claim 6 wherein the mobile device preparation step further comprises:

creating the first non-permanent cryptographic key in a remote application system wherein the remote application system is the remote source;

sending ~~at least a portion of the temporary cryptographic key~~ the first cryptographic key from the remote application system to the mobile device as a portion of the critical data: and wherein the local portion of the digital credential data comprises ~~an unpredictable~~ a calculated cryptogram as the second ~~unexpected~~ cryptogram, wherein the ~~unpredictable~~ calculated cryptogram is calculated, at least in part, using the ~~temporary~~ first non-permanent cryptographic key and the second cryptogram comprises the calculated cryptogram.

20. (Currently Amended) The method of claim 3 further comprising an authorizing step that follows the step of performing the interrogation, the authorizing step comprising:

~~sending~~ receiving at a remote application system an authorization request comprising the unpredictable data and the ~~unexpected~~ second cryptogram from the point-of-sale terminal ~~to a remote application system~~, wherein the ~~unexpected cryptogram comprises an unpredictable cryptogram~~;

verifying a correctness of the ~~unpredictable~~ second cryptogram by the application system wherein the ~~unpredictable~~ second cryptogram is compared with a result of ~~an unpredictable~~ a cryptogram calculation; wherein the result of the ~~unpredictable~~ cryptogram calculation is calculated using, at least in part, ~~a temporary~~ the first non-permanent cryptographic key; and

sending an authorization response from the remote application system to the point-of-sale wherein data contained in the authorization response is determined, at least in part, by the

verifying of the correctness of the ~~unpredictable~~ second cryptogram.

30. (New) The method of Claim 3, further comprising:

at a remote computer system, maintaining a secure element for the mobile device;

running an application on the mobile device that emulates a card.

31. (New) A method for exchange of secure digital credential information from a mobile device to a point-of-sale (POS) terminal for authorization of a transactions at POS terminals:

at a mobile device configured to use a local cryptographic key to calculate cryptograms for authorizing POS transactions, receiving a plurality of non-permanent cryptographic keys over a network, wherein the non-permanent cryptographic keys are generated at a remote computer system and are associated with the account;

storing the plurality of non-permanent cryptographic keys in transitory memory at the mobile device as the local encryption key, such that local cryptographic key changes between at least two interrogations;

participating in an interrogation between a point-of-sale terminal and the mobile device comprising:

receiving through a communication channel with a contactless reader at least one POS command application data protocol unit (ADPU) communication from the point-of-sale terminal, the at least one POS command ADPU communication comprising (a) a request for digital credential data corresponding to the account according to a selected specification and (b) unpredictable data; and

sending through the communication channel at least one device response APDU communication from the mobile device to the point-of-sale terminal, the at least one device response APDU communication comprising a cryptogram generated at the mobile device using the local cryptographic key and formatted according to a proper format for the selected specification; and

after participating in the interrogation, changing the local cryptographic key at the mobile device prior to responding to a subsequent interrogation to authorize another transaction against the account,

wherein the mobile device does not store a permanent cryptographic key associated with the account.

41. (New) A system comprising:

a mobile device:

a controller configured route communications received over a communication channel from a contactless device reader;

a volatile memory;

a non-volatile memory;

a processor programmed to:

receive non-permanent cryptographic keys associated with an account over a network from a remote source;

store the received non-permanent cryptographic keys as a local non-permanent cryptographic key such that the local non-permanent cryptographic key changes;

participate in interrogations over the communication channel, wherein to participate in an interrogation further comprises to:

process one or more point-of-sale (POS) command application data program units (ADPU) received as part of the interrogation;

in response to a request contained in the one or more POS command ADPUs for digital credential data according to a specification, generate a cryptogram, at least in part, using the local non-permanent cryptographic key; and

send at least one device response APDU communication through the communication channel, the at least one device response APDU comprising the digital credential data in a proper format for the specification, wherein the digital credential data in the at least one device response APDU communication comprises the cryptogram generated using the local non-permanent cryptographic key, wherein processor is programmed to respond to the request without accessing a permanent cryptographic key associated with the account.

42. (New) The system of Claim 41, further comprising a remote application system wherein the application system comprises a computer system programmed to:

generate the non-permanent cryptographic keys;

send the non-permanent cryptographic keys to the mobile device.

To: docketing@hanchukkheit.com,,
From: PAIR_eOfficeAction@uspto.gov
Cc: PAIR_eOfficeAction@uspto.gov
Subject: Private PAIR Correspondence Notification for Customer Number 122870

Feb 19, 2016 07:10:27 AM

Dear PAIR Customer:

Hanchuk Kheit LLP
258 Saint Nicholas Avenue, No. 8A
New York, NY 10027-5353
UNITED STATES

The following USPTO patent application(s) associated with your Customer Number, 122870 , have new outgoing correspondence. This correspondence is now available for viewing in Private PAIR.

The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

Disclaimer:
The list of documents shown below is provided as a courtesy and is not part of the official file wrapper. The content of the images shown in PAIR is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
13599647	INTV.SUM.APP	02/19/2016	Simplytapp0002US1
	OA.APPENDIX	02/19/2016	Simplytapp0002US1
	OA.APPENDIX	02/19/2016	Simplytapp0002US1
	OA.APPENDIX	02/19/2016	Simplytapp0002US1

To view your correspondence online or update your email addresses, please visit us anytime at https://sportal.uspto.gov/secure/myportal/privatepair.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov with 'e-Office Action' on the subject line or call 1-866-217-9197 during the following hours:

Monday - Friday 6:00 a.m. to 12:00 a.m.

Thank you for prompt attention to this notice,

UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT APPLICATION INFORMATION RETRIEVAL SYSTEM

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
REPLY TO OFFICE ACTION DATED 10/06/2015	Atty. Docket No. **STAPP1100-5**

First Named Inventor **C. Douglas Yeager**	
Application Number **13/599,647**	Date Filed **August 30, 2012**
Title **Systems and Methods for Secure Application-Based Participation in an Interrogation by Mobile Device (as amended)**	
Group Art Unit **3695**	Examiner **Puttaiah, Asha**
Confirmation Number **1919**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission Under 37 C.F.R. § 1.8

I hereby certify that this correspondence is being deposited electronically with the U.S. Patent and Trademark Office using the United States Patent and Trademark Office's EFS-Web system on **March 22, 2016.**

Delia Narvaiz

Dear Sir:

This paper is submitted in response to the Official Action mailed on October 6, 2015 and the Examiner Interview held on February 11, 2016. Please reconsider the above-identified application in view of the following amendments and remarks.

Amendments to the Specification begin on page 2 of this paper.

Amendments to the Claims are reflected in the listing of claims which begins on page 18 of this paper.

Remarks/Arguments begin on page 25 of this paper.

AMENDMENTS TO THE SPECIFICATION:

Please amend the specification as set forth below. All paragraph numbers refer to the paragraph numbers as they appear in the Application as filed (the "*Application*").

Please replace the title of the Specification with the following amended title:

SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE ~~AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM~~

On page 37 of the Specification, please replace subparagraph a of paragraph [00100] with the following amended subparagraph a:

a. ~~Mastercard~~ MASTERCARD data: 54 13 12 34 56 78 48 00 D0 90 61 01 90 94 99 89 92 50 3F

On page 38 of the Specification, please replace subparagraph d of paragraph [00100] with the following amended subparagraph d:

d. Any propriety data format (~~McDonalds~~ MCDONALDS Arch Card): 64 13 12 34 56 78 48 00D0 90 61 01 90 94 99 89 92 50 3F

On page 40 of the Specification, please replace paragraph [00106] with the following amended paragraph:

[00106] Fig. 21 illustrates an arrangement of an application system 201 (a variant of remote system auth server) that contains a Hardware Security Module (HSM) 200. The application system also includes a system of one or more computers that all may have access to the transaction table 205 and the credential table 206 within the application system. The application system contains data that should be kept in a secure manner and as a result may have both network accessibility and physical accessibility limitations built in to it. The application system can be further detailed as a "software representation" of a plurality of secure element

representations as the application system has access to all the information used to create APDU responses for any particular SE representation in its repository data. An added feature of the application system that extend its capabilities beyond a "software representation" of a plurality of secure element representations is that because it has access to the HSM that stores keys used to create the data in each SE representation, it can be configured for authorizing or verifying the output data (digital credential data) for any of the SEs contained in its repository data as well. An HSM is a device commonly used in the banking and processing industry. The HSM is responsible for securely containing encryption keys 203 (cryptographic keys) that are used to authorize card payments, or create digital credential data for new cards. Encryption algorithms 204 that use these keys are also contained on the HSM. An example of an HSM used in the industry at the time of this filing is currently distributed by SafeNet Inc. and is named the Luna EFT Mark II Edition. An example, from the ~~MasterCard~~ MASTERCARD PayPass MSD v3.3 card specification document, of an encryption key that may be stored on the HSM is called an Issuer Master Key (IMK). The HSM can then, for example, use the embedded algorithms 204 to create a "diversified key for card verification code creation" (KDcvc3) from the IMK that is used for each individual card that is issued based on a certain algorithm that is also stored in the HSM. The HSM is designed to protect individual encryption keys, and to use embedded encryption algorithms to calculate encryption output based on an encryption input request from an application system. The encryption algorithm must be located within the HSM because the algorithm must have direct access to the protected encryption keys 203. The application system will provide additional input data to be used in the encryption algorithms to the HSM. The application system will also expect output data from the encryption algorithms from the HSM. The input data to the HSM may be stored in the transaction table 205 and the credential table 206. An HSM is commonly a separate device within the application system that is connected to other devices within the application system through a communication channel. The communication channel may be a network connection such as an RJ45 cable or in some cases is a hardware bus connection such as a PCI connector within a computer casing. An example of using this arrangement may be that the application system contains:

a. Encrypted data (cryptogram)
b. Unpredictable number (UN)
c. Application Transaction Counter (ATC)
d. Transaction data such as a dollar amount
e. A key identifier (but the not key itself)

in its transaction table and credential table. The application system would like to verify encrypted data (a) was created from a particular encryption key (e), unpredictable number (b), ATC (c), and transaction data (d). The application system knows which key was used to create the cryptogram (a), but opts, for security reasons, not to have access to the key itself. The application system then uses the cryptogram (a), unpredictable number (b), ATC (c), transaction data (d), and a key identifier (e) as input for the HSM and sends the input to the HSM. The HSM then uses the input data from the application system and locates the proper encryption algorithm and encryption key to use. The HSM then creates the output response from the algorithm using the encryption key and sends the output to the application system. The output in this example would be a simple "verified" or "not verified" message.

On page 43 of the Specification, please replace subparagraph d of paragraph [00109] with the following amended subparagraph d (there are no changes to Table 2):

d. Application Version Number

From this data, the application system can create the proper APDU response to the read record command that is formatted just like figure 3, element 13 and send it specifically for the card credential the mobile device has requested to the mobile device for caching over a communication channel. For a ~~MasterCard~~ MASTERCARD PayPass MSD v. 3.3 credential, table 2 shows a technical breakdown of how the data in the read record response is formulated from data in the application system in proper APDU response BER-TLV format.

TABLE 2

70		7F																	
		T	L	V															
	9F	6C	02	00	01	-Application Version Number													
	56	3E		42	35	34	31	33	31	32	33	34	35	36	37	38	34	38	30	Track 1
				30	5E	53	55	50	50	4C	49	45	44	2F	4E	4f	54	5E	30	Data
				39	30	36	31	30	31	33	33	30	30	30	33	33	33	30	30	
				30	32	32	32	32	32	30	30	30	31	31	31	31	30			
	9F	64	01	03											T1__NATC					
	9F	62	06	00	00	00	38	00	00						T1__PCVC3					
	9F	63	06	00	00	00	00	E0	E0						T1__PUNATC					
	9F	65	02	00	0E										T2__PCVC3					
	9F	66	02	0E	70										T2__PUNATC					
	9F	6B	13	54	13	12	34	56	78	48	00	D0	90	61	01	90	00	99	00	Track 2
				00	00	0F														Data
	9F	67	01	03			T2__NATC													
90		00																		

Application Version Number, Track 1 Data, T1_NATC, T1_PCVC3, T1_PUNATC, T2_PCVC3, T2_PUNATC, T2_NATC, and Track 2 Data are all accessible by the application system in the credential table.

On page 44 of the Specification, Please replace paragraph [00110] with the following amended paragraph:

[00110] As used herein the term "cryptogram" refers to encrypted data that may or may not be able to be un-encrypted. Encrypted data that cannot be un-encrypted is many times called a "hash." A cryptogram is typically calculated from a series of input data that comprises some data and a cryptographic key, where the cryptographic key is used to encrypt some data. As used herein the term "cryptographic key" refers to a key used, at least in part, to calculate a cryptogram. A cryptogram is calculated based on an algorithm or calculation formula. As use herein the term "calculation formula" refers to an algorithm or formula that is specified by a card specification as the method to calculate a cryptogram. A calculation formula typically may be known by any entity. The output result of the calculation formula that uses the input data and a cryptographic key is a cryptogram. Examples of cryptograms at the time of this filing are defined by the following card specifications in table 4.

Table 4

Card specification	Cryptogram Designator or Name
~~MasterCard~~ MASTERCARD PayPass MSD	CVC3
~~Visa~~ VISA Contactless MSD	dCVV
~~Discover~~ DISCOVER ZIP MSD	dCVV
EMV, ~~Visa~~ VISA QVSDC, VISA VSDC,	AC, TC, AAC, ARQC
~~MasterCard~~ MASTERCARD MCHIP	

A "cryptogram" as used herein may be classified as "dynamic" meaning that it is always changing from one interrogation (transaction) to the next over the life a digital credential (SE representation). As used herein the term "life of", as in, the life of a digital credential, the life of a card, the life of a SE, the life of a SE representation, refers to the life beginning when it is used its first interrogation and ending when it is used in its last interrogation. One indication of this dynamic aspect of a cryptogram is to perform two sequential independent interrogations between a mobile device and a point-of-sale

terminal where the same digital credential is used on the mobile device, and the point-of-sale terminal receives two sets of digital credential data with each including a single cryptogram, one with each interrogation. If the cryptogram received by the point-of-sale terminal is different from one interrogation to the next, it is dynamic. A "cryptogram" as used herein may be classified as "dynamic" meaning that it is always changing from one interrogation (transaction) to the next over the life a digital credential (SE representation). As used herein the term "life of", as in, the life of a digital credential, the life of a card, the life of a SE, the life of a SE representation, refers to the life beginning when it is used its first interrogation and ending when it is used in its last interrogation. One indication of this dynamic aspect of a cryptogram is to perform two sequential independent interrogations between a mobile device and a point-of-sale terminal where the same digital credential is used on the mobile device, and the point-of-sale terminal receives two sets of digital credential data with each including a single cryptogram, one with each interrogation. If the cryptogram received by the point-of-sale terminal is different from one interrogation to the next, it is dynamic.

On page 45 of the Specification, please replace paragraph [00111] with the following amended paragraph:

[00111] The details of an interrogation between a point-of-sale and a digital credential, card, SE representation, and mobile device are defined in "card specifications" and implemented in point-of-sale terminals. Examples of these card specifications at the time of this filing are ~~MasterCard~~ MASTERCARD PayPass—Mag Stripe v3.3, Contactless EMV, ~~Discover~~ DISCOVER Network RF Contactless Specification—Supplement Guide For Functional Support, AMEX ALIS v1.7, and ~~Visa~~ VISA Contactless Payment Specification v2.0.2. As used~~Used~~ herein the term "card specification" refers to a specification or reference within the specification to other specifications and so on that a point-of-sale terminal must adhere to in order to interrogate a card, SE, mobile device as expected by that card specification. A point-of-sale terminal, as the interrogator, controls the interrogation. The card specification that defines the details of an interrogation may also define the details of a cryptogram request, calculation, and delivery from the card, SE, or mobile device to the point-of-sale as part of the interrogation sequence. Card specifications may include references to other specifications and those other specifications to even more specification wherein the card specification may be defined by the card specification in

conjunction with other supporting documents sited within a card specification. Card specifications typically consist of an application layer that defines an interrogation sequence and calculations that are to be performed by both the card, SE, mobile device and also the interrogator or point-of-sale. Both a mobile device and a point-of-sale are expected to be operating under the direction of a card specification during an interrogation.

On page 46 of the Specification, please replace paragraph [00113] with the following amended paragraph:

[00113] Also, the card specification may define a cryptogram to be calculated by the card, SE, or mobile device based, at least in part, on a cryptographic key, where the cryptographic key is a "permanent cryptographic key". In this context, it is said that the cryptogram delivered by the mobile device is "expected" because the card specification indicates it will be calculated, at least in part, from a permanent cryptographic key and that is what the card specification expects. As usedUsed herein the term "permanent cryptographic key" refers to a cryptographic key that is unchanging (or static) throughout the life of a card, SE, mobile device, or digital credential.

On page 47 of the Specification, please replace paragraph [00116] with the following amended paragraph:

[00116] As usedUsed herein the terms "transient," "transiently stored," "non-persistent," and "non-persistently stored" refers to data that are stored in a storage container where the are erased or otherwise rendered not accessible after a power failure to the storage container. An example of a transient storage container is RAM (Random Access Memory).

On page 47 of the Specification, please replace paragraph [00117] with the following amended paragraph:

[00117] Cryptograms used herein may be "expected" to be calculated, at least in part, from unpredictable data passed from a point-of-sale to a mobile device during an interrogation that is dictated by a card specification. As usedUsed herein the term "predetermined cryptogram" refers to a cryptogram that is formulated without the use of unpredictable data passed from the point-of-

sale terminal to a mobile device during an interrogation; wherein the interrogation is defined by a card specification; and the card specification indicates the cryptogram to be calculated, at least in part, by the unpredictable data. This may include a predetermined cryptogram being entirely made up of a string of random data. This may also include a predetermined cryptogram being calculated based on other unpredictable data instead of the unpredictable data from the point-of-sale. As used herein "predetermined cryptogram" also refers to a type of unexpected cryptogram.

On page 47 of the Specification, please replace paragraph [00118] with the following amended paragraph:

[00118] Cryptograms used herein are many times may be "expected" to be calculated, at least in part, from a permanent cryptographic key ~~that~~ during an interrogation between a mobile device and a point-of-sale. As used herein the term "unpredictable cryptogram" refers to a cryptogram calculated, at least in part, from a temporary cryptographic key for use in an interrogation between a mobile device and a point-of-sale; wherein the interrogation is defined by a card specification; and the card specification indicates a cryptogram to be calculated, at least in part, by a permanent cryptographic key. As used herein "unpredictable cryptogram" also refers to a type of unexpected cryptogram.

On page 48 of the Specification, please replace paragraph [00119] with the following amended paragraph:

[00119] As used~~Used~~ herein the terms "unexpected cryptogram", "unexpected predetermined cryptogram", and "unexpected unpredictable cryptogram" refer to a cryptogram that is sent from a mobile device to a point-of-sale during an interrogation; wherein the interrogation is defined by a card specification implemented on the point-of-sale; and the cryptogram is calculated from a different calculation formula than is defined in the card specification. For example, the "different calculation formula" includes a predetermined cryptogram. As used herein the term "predetermined cryptogram" refers to a cryptogram that is calculated without the use of unpredictable data passed from the point-of-sale terminal to a mobile device during an interrogation; wherein the interrogation is defined by a card specification; and the card specification indicates the cryptogram to be calculated, at least in part, by the unpredictable data. A predetermined cryptogram may be entirely made up of a string of random

data. A predetermined cryptogram may also be calculated based on other unpredictable data instead of the unpredictable data from the point-of-sale. As used herein "predetermined cryptogram" is an example of an unexpected cryptogram.

On page 49 of the Specification, please replace paragraph [00122] with the following amended paragraph:

[00122] The response for the compute cryptographic checksum command (figure 3, element 14), is created by a method employed in figures 22, 23, 24, 25, 26, 27, 28, 29 and 30 called "Cryptogram Substitution" using a predetermined cryptogram or unpredictable cryptogram and in some embodiments sent for each transaction to the mobile device cache over a communication channel when requested by the mobile device. In other embodiments cryptogram substitution is used with unexpected cryptograms created on the mobile device and sent to a remote application system. For a ~~MasterCard~~ MASTERCARD PayPass MSD v. 3.3 credential, table 3 shows a technical breakdown of how the data in the read compute cryptographic checksum response is formulated from data in the application system in proper APDU response BER-TLV format.

Table 3

77 0F

T	L	V
9F 61	02	B8 92 T2_CVC3
9F 60	02	FB C7 T1_CVC3
9f 36	02	00 5E ATC

90 00

The ATC is the automated transaction counter that increments with every point-of-sale interrogation, and can be stored in the transaction table or credential table and updated with each interrogation by a mobile device. The CVC3 is cryptogram that is expected to be calculated with this algorithm from the ~~MasterCard~~ MASTERCARD PayPass MSD v3.3 card specification:
First KDcvc3 is created:

Z_L:=DES3(IMK$_{CVC3}$)[Y]

Z_R:=DES3(IMK$_{CVC3}$)[Y
⊕('FF'‖'FF'‖'FF'‖'FF'‖'FF'‖'FF'‖'FF'‖'FF')]

and define:

KD_{CVC3}:=(Z_L ‖ Z_R).

KDcvc3 calculation may be ~~preformed~~ performed inside the HSM because the HSM contains IMK. The application system will pass Y, which is defined as the PAN and PAN sequence number concatenated as an input to the HSM in conjunction with the IMK id to use. The HSM will respond back with the KDcvc3 as output. The KDcvc3 in this example would be considered a permanent cryptographic key because it will not change over the life of the digital credential, as none of the inputs to the calculation of KDcvc3 change over the life of the credential.

Next T2_IVCVC3 is created:

O:=PayPass-MagStripe(3.3) Annex B alg(KDcvc3)[Track 2 Data]

The least two significant bytes of the output data are defined to be T2_IVCVC3.

Finally, the CVC3 cryptogram for track 2 is calculated:
O:=DES3(KD_{CVC3})[T2_JVcvc3 ‖ UN ‖ ATC]

The least two significant bytes of the output data are defined to be CVC3

CVC3 calculation may be ~~preformed~~ performed inside the HSM because the HSM contains the IMK which is used to create KDcvc3, which is used to create IVCVC and CVC3. So the application system will pass UN and ATC as inputs in conjunction with the IMK id to use. The HSM will respond back with the CVC3 cryptogram as output. The CVC3 is a dynamic cryptogram as the input to the calculation of the cryptogram change with each interrogation. This is known because with each interrogation the digital credential is expected to increment the ATC (Automated Transaction Counter) and also have different UN value.

On page 52 of the Specification, please replace paragraph [00128] with the following amended paragraph:

[00128] The concept of transaction (command/response) caching is disclosed herein. A cache is a component that transparently stores data so that future requests for that data may be served faster. The data that are stored within a cache may be values that have been computed earlier or duplicates of original values that are stored elsewhere. If requested data are contained in the cache ("cache hit"), this request may be served by simply reading the local cache, which is comparatively faster that accessing the remote source. Otherwise ("cache miss"), the data have to be recomputed or fetched from its original storage location, which is comparatively slower. Hence, the more requests that may be served from the local cache, the faster will be the overall system performance. Caching implies that the cache values may be temporary and the original values from the remote source can be easily accessible time after time if needed in order to update, or replace the cached values. As used~~Used~~ herein the term "non-persistent cache" and "transient cache" refers to the cached data to be transient or non-persistent. Unless otherwise stated the term "cache" also refers to the cached data to be transient or non-persistent.

On page 53 of the Specification, please replace paragraph [00130] with the following amended paragraph:

[00130] As used~~Used~~ herein the term "card data" or "credential data" may refer to the data used to create a proper APDU response to credential specific APDU commands such "read record" 7, and data used in "compute cryptographic checksum" 8. It is common for an application system in a software representation of a plurality of remote secure element repository to have access to all the data to properly create a valid APDU response.

On page 53 of the Specification, please replace paragraph [00131] with the following amended paragraph:

[00131] Fig. 16 illustrates a caching system for each transaction or interrogation between a point-of-sale **778** and a mobile device **779** for a ~~MasterCard~~ MASTERCARD PayPass transaction. The advantage of caching secure element responses is to lessen the effect of network latency and speed up an interrogation. In the example contained Fig. 16, network latency

is reduced from a potential 800 ms to a potential 200 ms because of the caching technique applied. This is a significant effect in the application of NFC or RFID because the as the total interrogation timeframe shrinks, the likelihood of a successful interrogation sequence goes up because it is less likely the communication channel between the point-of-sale and the mobile device will be interrupted from the mobile device moving out of the field generated by the point-of-sale. Notice that not all interrogation command and responses **787** and **793** in Fig. 16 are handled from the mobile device cache **780.** The non-cached command and response, lead to the 200 ms network latency of the entire transaction in figure 16.

On page 53 of the Specification, please replace paragraph [00132] with the following amended paragraph:

[00132] Fig. 17 illustrates a caching system for each transaction or interrogation between a point-of-sale 794 and a mobile device 795 for a ~~Visa~~ VISA PayWave transaction. In this figure the concept of 100% transaction caching is employed. It illustrates how all of the responses for an interrogation from a point-of-sale may be cached at some point of time ahead 802 of the actual mobile device and point-of-sale interrogation. This causes network latency of the interrogation to be 0 ms (zero) because no data is queried during the interrogation over the network from the remote system auth server's remote repository. This is a tremendous advantage over the system in Fig. 16, which in-turn had a tremendous advantage to the system that does not employ transaction caching at all.

On page 53 of the Specification, please replace paragraph [00133] with the following amended paragraph:

[00133] Depending on the interrogation sequence selected by the point-of-sale, it may not always be possible to implement a system set forth in Fig. 17. Many point-of-sale interrogation sequences carried out at the time of this filing are based on card specifications such as:

a. ~~MasterCard~~ MASTERCARD, PayPass, MChip
b. ~~American Express~~ AMERICAN EXPRESS, Express Pay
c. ~~Discover~~ DISCOVER Zip
d. ~~Visa~~ VISA QVSDC, VSDC
e. Contactless EMV

Employ a method of creating an expected cryptogram by the mobile device that is calculated, at least in part, from unpredictable data generated on the point-of-sale and delivered to the mobile device during the interrogation sequence. Because creating an expected cryptogram requires a calculation to be ~~preformed~~ performed that includes a permanent cryptographic key, the secure element or system with access to this key must be used to carry out the expected cryptogram calculation. Because the secure element representation is stored in a remote repository and contains the permanent cryptographic key, this expected cryptogram calculation would incur network latency to perform the calculation during the interrogation, as shown in figure 16, element 793.

On page 55 of the Specification, please replace paragraph [00136] with the following amended paragraph:

[00136] If data created by the point-of-sale is not part of the input to the creation of the expected cryptogram, such as in ~~Visa~~ VISA Contactless MSD cryptogram (dCVV), then the cryptogram can be calculated by the remote repository, transferred to the mobile device, and cached for use at a later time during point-of-sale interrogation. This scenario creates no network latency and allows for one hundred percent transaction caching during the interrogation, because the secure element representation need not be accessed during the actual interrogation time. As used~~Used~~ herein the term "one hundred percent (100%) transaction caching" refers to the ability for the mobile device to complete the interrogation with a point-of-sale terminal without the requirement to contact the secure element during the interrogation, and instead have all the data on hand local to the mobile device to complete the interrogation.

On page 58 of the Specification, please replace paragraph [00143] with the following amended paragraph:

[00143] Fig. 29 illustrates a representation of a table of digital credentials 350 (digital credential data) that may be stored inside the application system. This table, in conjunction with the transaction table, and in some embodiments the HSM allows the application system to perform as a repository of a plurality of secure element software representations. The credential data used to create data inside an SE and also allow it to formulate its proper APDU responses is contained in this table for a plurality of credentials (SEs). For a ~~MasterCard~~ MASTERCARD

PayPass MSD v3.3 credential, the example shown in this table, the columns of data list personal account number (PAN) 351, expiration date 352, name of card holder 353, card code 354, track 1 data 355, track 2 data 356, track 1 cvc3 bitmap 357, track 2 cvc3 bitmap 358, track 1 UN and ATC bitmaps 359, track 2 UN and ATC bitmaps 360, track 1 number of ATC digits 361, track 2 number of ATC digits 362, CVM list 363, AC 364, application version number 365, and the master key identifier 366.

On page 58 of the Specification, please replace paragraph [00144] with the following amended paragraph:

[00144] FIG. 23 illustrates a method for a mobile device 220 to request a transaction cache 224 prior to being interrogated by a point-of-sale. As used~~Used~~ herein the term "transaction cache" refers to data required to formulate proper mobile device responses during an interrogation with a point-of-sale, which may comprise digital credential data. As discussed in figure 17 and figure 18, figure 23 is very similar and describes a method for a mobile device 220 to receive a cache of transaction data (transaction cache) 227 over a communication channel to be used during a point-of-sale interrogation at a later point in time. Before an interrogation with a point-of-sale, the mobile device will request a transaction cache to be used during the point-of-sale interrogation from the application system 222 over a communication channel. This transaction cache data may comprise the randomly generated unpredictable data such as UN and transaction data from the application system, the other credential based inputs 225 to cryptogram calculation and sends them to the HSM 223 over a communication channel. The HSM then may calculate the predetermined cryptogram 226 and return it to the application system. The predetermined cryptogram may then be used to formulate the cache response to a "request cryptogram" APDU command from a point-of-sale. In a further embodiment, the application system could avoid the step of contacting the HSM and simply make up a random sequence of bytes to be used as a predetermined cryptogram to be used in place of the expected cryptogram. This predetermined cryptogram is a sequence of random data and is shared with the mobile device, so the mobile device could have, just as well, created the random bytes as the predetermined cryptogram and shared them with the application system. In a further embodiment, the application system could avoid the step of contacting the HSM and simply make up a temporary cryptographic key from a random sequence of bytes to be shared with and used by the mobile device while creating an unpredictable cryptogram to be used in place of the

expected cryptogram. This temporary cryptographic key is a sequence of random data and is shared with the mobile device, so the mobile device could have, just as well, created the random bytes as the temporary cryptographic key and shared them with the application system.

On page 59 of the Specification, please replace paragraph [00145] with the following amended paragraph:

[00145] For an example, the ~~MasterCard~~ MASTERCARD PayPass interrogation from the point of sale incorporates an APDU command request called "compute cryptographic checksum" 14 as seen in figure 3. The command APDU follows a particular format and may look like this:

80 2A 8E 80 04 00 00 08 99 00

The digits 00 00 08 99 in the APDU command above from the point-of-sale indicate the unpredictable number to be used as an expected cryptogram calculation input. This unpredictable number is a random sequence of numbers that changes with each interrogation the point-of-sale initiates. The format of this APDU command request is discussed in more detail inside the ~~MasterCard~~ MASTERCARD PayPass MSD v3.3 card specification. The immediate APDU response from the mobile device is expected to follow a particular format and may look like this:

77 0F 9F 61 02 B8 92 9F 60 02 FB C7 9F 36 02 00 5E 90 00

The digits B8 92 represent the cryptogram. It is identified by the preceding BER-TLV formatted tag 9F 61 (track 2 CVC3), and length value of 02. It was expected to have been calculated from the unpredictable number issued by the preceding point-of-sale APDU command request in combination with other inputs such as the ATC. A correct expected cryptogram must be calculated using the permanent cryptographic key that is securely stored inside the SE. Because figure 23 implements 100% transaction caching, it is not impossible for the expected cryptogram to be calculated after receiving the unpredictable number from the point-of-sale, because in that event, the mobile device would need to access the network to contact the remote repository as in figure 16, elements 787 and 793 in order to perform the expected cryptogram calculation. The method of substituting a predetermining a cryptogram, or an unpredictable cryptogram in place of the expected cryptogram, in this case, needs to be applied in order to create this response. With this method applied, the "compute cryptographic checksum" response from the mobile device can

be successfully delivered interrogation with the point-of-sale without contacting the remote SE representation during the interrogation. In this case, the cached response may look like this instead:

77 0F 9F 61 02 A4 56 9F 60 02 FB C7 9F 36 02 00 5E 90 00

Where, in one embodiment, the digits A4 56 is the predetermined cryptogram, and NOT calculated using, at least in part, the expected unpredictable number from point-of-sale. Where, in another embodiment, the digits A4 56 is the unpredictable cryptogram, and NOT calculated, at least in part, using the expected permanent cryptographic key rather using a temporary cryptographic. This is an example of "Cryptogram Substitution" technique. The point-of-sale does not have the means or keys to check the received cryptogram for correctness, so it will accept the cryptogram answer because it is of the proper format. The point-of-sale will rely on the authorization request later to verify the correctness of the cryptogram.

On page 63 of the Specification, please replace paragraph [00154] with the following amended paragraph:

[00154] FIG. 25 illustrates an authorization request after an interrogation between a mobile device and a point-of-sale has been performed~~preformed~~, such as in fig. 24. Typically the point-of-sale 255 will formulate an authorization request which may be in the form of ISO8583 format. This format will contain data that pertains to the interrogation such as the cryptogram received from the mobile device, the unpredictable number and transaction data passed to the mobile device for cryptogram calculation, and other credential data. The authorization request will be passed to the application system 251 over a communication channel 252. This communication channel may not go directly to the application system, but may go first to an acquiring gateway, then to an issuing processor, and eventually to the application system 251. This communication channel may be referred to herein as "the interchange". The interchange is a private network that is used exclusively by the payment card industry for the purpose of authorization requests. After the authorization request is received by the application system, the authorization request may be matched to a particular transaction that is listed in the transaction table 210 based on the PAN 211 that is listed in the credential data of the authorization request. The application system will make the authorization decision for the authorization request.

On page 65 of the Specification, please replace paragraph [00158] with the following amended paragraph:

[00158] Fig. 26 illustrates the transaction table 262 that is also shown in figure 25, element 253 and figure 22, element 210. The state of the transaction table in figure 26 represents that of after a transaction interrogation has been performed~~preformed~~ and after the application system has received data from the mobile device as in figure 25, element 254. The example of the data received is shown for the unpredictable number from the terminal 260 and the transaction data 261. Both of these numbers may be used to verify an authorization request shown in figure 25, element 252, as they could be compared and match that of the authorization request. These numbers also may be used as placeholders to identify that a system authorization is complete.

On page 71 of the Specification, please replace paragraph [00186] with the following amended paragraph:

[00186] As used~~Used~~ herein the term "interrogation" or "interrogation sequence" refers to all the APDU command requests and APDU responses between a mobile device and a point-of-sale using RFID (NFC) required to deliver a complete credential for authorizing a financial transaction to a point-of-sale as defined by a card specification. Typically, an NFC interrogation does not span multiple NFC field entrances and exits. Typically the beginning of an interrogation starts when a mobile device enters the NFC field of a point-of-sale and ends at least prior to when the mobile device exits the NFC field.

AMENDMENTS TO THE CLAIMS:

Please amend the claims as set forth in the following listing. This listing of claims will replace all prior versions, and listings, of claims in the present application:

1-29. Cancelled.

30. (New) A method for secure application-based participation in a payment card transaction authorization process by a mobile device, the method comprising:

receiving over a wireless network at a mobile device a first non-permanent cryptographic key associated with an account having a corresponding digital credential, wherein the mobile device comprises an operating system and an application executable in the operating system, the application interrogable for digital credential data corresponding to the account, wherein the application does not access a permanent cryptographic key associated with the account during interrogations;

locally storing a first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;

participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device comprising:

receiving at least one POS command communication sent by the POS terminal over a communications channel, wherein the at least one POS command communication comprises a request for digital credential data to authorize a transaction against the account;

generating a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram; and

responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to an electronic reader through the communication channel, the at least one device response communication comprising at least a portion of the digital credential data, wherein the at least a portion of the digital credential data comprises the response cryptogram and an account identifier for the account;

receiving a second non-permanent cryptographic key at the mobile device, wherein the second non-permanent cryptographic key is associated with the account; and

replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key as the local cryptographic key associated with the account prior to the application participating in a subsequent interrogation.

31. (New) The method of Claim 30, wherein the mobile device is an NFC emulating device.

32. (New) The method of Claim 30, wherein the response cryptogram is a hash.

33. (New) The method of Claim 30, wherein the interrogation conforms to a card specification, the set of inputs is specified by the card specification and the at least one device response is formulated according to the card specification.

34. (New) The method of Claim 33, wherein the request for digital credential data comprises a request for a first cryptogram according to the card specification and the at least one device response communication comprises a second cryptogram, wherein the second cryptogram is the response cryptogram.

35. (New) The method of Claim 30, wherein generating the response cryptogram comprises encrypting the set of inputs using the local cryptographic key according to a digital encryption standard (DES) calculation to generate an output, wherein the reponse cryptogram includes a portion, but not all, of the output.

36. (New) The method of Claim 30, wherein the mobile device does not have connectivity to the wireless network during the interrogation.

37. (New) The method of Claim 30, further comprising, at a remote system:

prior to the interrogation, generating at a remote system the first non-permanent cryptographic key, associating the first non-permanent cryptographic key with the account, and sending the first non-permanent cryptographic key and the account identifier to the mobile device over the wireless network; and

after the interrogation generating at the remote system, the second non-permanent cryptographic key, associating the second non-permanent cryptographic key with the account and sending the second non-permanent cryptographic key and the account identifier to the mobile device over the wireless network.

38. (New) The method of Claim 37, wherein the digital credential comprises a secure element representation maintained at the remote system.

39. (New) The method of Claim 30, further comprising, at a remote system performing an authorization process comprising:

receiving an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the response cryptogram and the account identifier;

determining a current non-permanent cryptographic key associated with the account using the account identifier;

calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account;

verifying a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram; and

sending an authorization response to the POS terminal, wherein the data contained in the authorization response is determined, at least in part, by the verifying the correctness of the response cryptogram.

40. (New) The method of Claim 39, wherein:

the set of inputs comprises unpredictable data;

the authorization data comprises the unpredictable data; and

the calculated cryptogram is calculated using the unpredictable data.

41. (New) The method of Claim 40, wherein the POS command communications comprise the unpredictable data.

42. (New) The method of Claim 41, wherein the authorization data further comprises values from the transaction and wherein the POS terminal communicates the values from the

transaction, the response cryptogram and the account identifier to the remote system in track 2 format.

43. (New) The method of Claim 41, wherein the authorization data further comprises values from the transaction and wherein the POS terminal communicates values from the transaction, the response cryptogram and the account identifier in BER-TLV format.

44. (New) A system for secure application-based participation by a mobile device in point-of-sale interrogations, the system comprising:

a mobile device comprising:

a controller configured to route communications received over a communication channel from an electronic reader;

a wireless interface to connect to a wireless network;

a processor;

a computer readable storage medium accessible by the processor storing an application interrogable for digital credential data to authorize transactions against an account having a digital credential, the application executable in an operating system of the mobile device to participate in interrogations, wherein the application is executable to:

during an interrogation:

receive at least one point-of-sale (POS) command communication sent by a POS terminal to the mobile device over the communications channel, wherein the at least one POS command communication comprises a request for digital credential data;

access a locally stored cryptographic key associated with the account, wherein the mobile device does not have access to a permanent cryptographic key associated with the account and the locally stored cryptographic key associated with the account is a non-permanent cryptographic key that does not last a life of a digital credential for an account;

generate a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key

associated with the account used to generate the response cryptogram; and

respond to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response to the electronic reader through the communication channel, the at least one device response communication comprising at least a portion of the digital credential data, wherein the at least a portion of the digital credential data comprises the response cryptogram and an account identifier for the account;

receive non-permanent cryptographic keys associated with the account transmitted to the mobile device over the wireless network by a remote source; and

store the received non-permanent cryptographic keys as the locally stored cryptographic key associated with the account to change the locally stored cryptographic key associated with the account between at least two interrogations.

45. (New) The system of Claim 44, wherein the mobile device is an NFC emulating device.

46. (New) The system of Claim 44, wherein the response cryptogram is a hash.

47. (New) The system of Claim 44, wherein the interrogations conform to a card specification, the set of inputs is specified by the card specification and the at least one device response is formulated according to the card specification.

48. (New) The system of Claim 47, wherein the request for digital credential data requests digital credential data comprising a first cryptogram and the at least one device response communication comprises a second cryptogram, wherein the second cryptogram is the response cryptogram.

49. (New) The system of Claim 44, wherein generating the response cryptogram comprises encrypting the set of inputs using the local cryptographic key according to a digital encryption standard (DES) calculation to generate an output, wherein the response cryptogram includes a portion, but not all, of the output.

50. (New) The system of Claim 44, wherein the mobile device does not have connectivity to the wireless network during the interrogation.

51. (New) The system of Claim 44, wherein the mobile device is programmed to request a new non-permanent cryptographic key after the interrogation.

52. (New) The system of Claim 44, further comprising a remote computer system configured to generate the non-permanent cryptographic keys associated with the account and send each of the non-permanent cryptographic keys and the account identifier to the mobile device over the wireless network.

53. (New) The system of Claim 52, wherein the remote computer system is configured to maintain a secure element representation for the account, wherein the digital credential comprises the secure element representation.

54. (New) The system of Claim 44, further comprising, a remote computer system programmed to:

receive an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the response cryptogram and the account identifier;

determine a current non-permanent cryptographic key associated with the account using the account identifier;

calculate a calculated cryptogram using the current non-permanent cryptographic key associated with the account;

verify a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram; and

send an authorization response to the POS terminal, wherein the data contained in the authorization response is determined, at least in part, by the verifying the correctness of the response cryptogram.

55. (New) The system of Claim 54, wherein:
the set of inputs comprises unpredictable data;
the authorization data comprises the unpredictable data; and
the calculated cryptogram is calculated using the unpredictable data.

56. (New) The system of Claim 55, wherein the POS command communications comprise the unpredictable data.

57. (New) The system of Claim 55, wherein the authorization data further comprises values from the transaction and wherein the POS terminal communicates the values from the transaction, the response cryptogram and the account identifier to the remote system in track 2 format.

58. (New) The system of Claim 55, wherein the authorization data further comprises values from the transaction and wherein the POS terminal communicates the values from the transaction, the response cryptogram and the account identifier to the remote system in BER-TLV format.

REMARKS

Applicant appreciates the time taken by the Examiner to review Applicant's present application. This application has been carefully reviewed in light of the Official Action mailed October 6, 2015. Applicant respectfully requests reconsideration and favorable action in this case.

Interview Summary

A telephonic interview was conducted on Feb. 11, 2016 between Examiner Puttaiah, Inventor Doug Yeager and Attorney Adair. During the interview, proposed amendments to Claim 3 were discussed.

The Applicant and Examiner discussed the development of payment card technologies and the use of mobile devices as payment cards. Applicant pointed out that embodiments described in the present application address multiple problems specifically rooted in computer technology. Applicant discussed that security problems arise due to shared memory when attempting to use an application running in the operating system of a mobile device, rather than a hardware secure element, to participate in interrogations with smart payment card readers. Further, Applicant pointed out that several embodiments described in the application address not only security problems, but other problems, such as network delays and latency. Although no agreement was reached, the Examiner suggested amending the claims to more specifically recite the use of an application running in the operating system of the mobile device. Applicant appreciates the Examiner's suggestions.

New Claims

Applicant has added new Claims 30-58. As discussed in more detail below, the claims are supported by the *Application* as filed and do not add new matter. The support cited in the following discussion is not exhaustive. Moreover, the support cited for a particular claim or claim limitation(s) is not intended to be limiting of the claim or claim limitation(s) for which it is cited.

Claim 30 recites "[a] method for secure application-based participation in a payment card transaction authorization process by a mobile device . . . wherein the mobile device comprises an operating system and an application executable in the operating system, the application interrogable for digital credential data corresponding to the account, wherein the application does not access a permanent cryptographic key associated with the account during interrogations."

See, e.g., Application ¶ 197 ("a mobile device that comprises an operating system, with an application that runs in that operating system, such that the application does not have access to a local persistently stored permanent cryptographic key . . . and/or such that the process is under the direction of the application"); *id.* at ¶ 198 (describing "a mobile device that comprises an operating system, with an application that runs in that operating system, wherein the application has the capability of being interrogated by a point-of-sale"); *id.* at ¶ 205.

Claim 30 further recites "receiving over a wireless network at a mobile device a first non-permanent cryptographic key associated with an account having a corresponding digital credential," "locally storing a first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account," "receiving a second non-permanent cryptographic key at the mobile device, wherein the second non-permanent cryptographic key is associated with the account" and "replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key as the local cryptographic key associated with the account prior to the application participating in a subsequent interrogation." These recitations are supported throughout the *Application. See id. e.g.,* ¶¶ 107, 114, 128, 29, 144, 146, 151-153, 165, 167, and 168.

Claim 30 further recites "participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device" where participating in the interrogation comprises "receiving at least one POS command communication sent by the POS terminal over a communications channel, wherein the at least one POS command communication comprises a request for digital credential data to authorize a transaction against the account." These recitations are supported throughout the *Application. See, e.g., id.* at FIG. 24, FIG. 28 ¶¶ 153, 167, and 170.

Claim 30 further recites that participating in the interrogation by the application comprises "generating a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram." The *Application* supports generating a response cryptogram based on a set of inputs and the local cryptographic key (the non-permanent key associated with the account received from the remote system). *See, e.g., id.* at ¶¶ 146, 151-153, 165, and 172. Moreover, one of ordinary skill in the art would understand that cryptograms do not typically include the cryptographic key used to generate them. That is, the cryptogram cannot be decrypted to reveal the encryption key. For

example, the specification describes that, in one embodiment, a resultant cryptogram can be created in the same manner as a cryptogram created by the KDcvc3 key, but substituting a temporary key for the KDcvc3 key. *See, e.g., id.* at ¶ 123. A resulting cryptogram generated in this manner would not include the temporary encryption key used to generate it.

Claim 30 further recites that participating in the interrogation by the application comprises "responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to the electronic reader through the communication channel, the at least one device response communication comprising at least a portion of the digital credential data, wherein the at least a portion of the digital credential data comprises the response cryptogram and an account identifier for the account." As discussed above, the *Application* describes that the response to the at least one POS command communication can include the response cryptogram generated using a non-permanent cryptographic key. *See, e.g., id.* at ¶¶ 151-153, 165, and 172. The response may also include an account identifier (e.g., personal account number (PAN)). *See e.g., id.* at FIG. 24 and ¶ 153 (mobile device responding to READ RECORD APDU), ¶ 109 (describing that a response to a READ RECORD APDU may include "Track 1 and Track 2 data comprised of PAN, Exp. Date, card code, issuer discretionary data").

For at least the foregoing reasons, Applicant submits that Claim 30 does not add new matter. For similar reasons readily apparent from the foregoing, Applicant similarly submits that Claim 44 does not add new matter.

Claims 31 and 45 recite that "the mobile device is an NFC emulating mobile device." Support for Claims 31 and 45 can be found at least at *id.* at ¶¶ 153, 170, and 198.

Claims 32 and 46 recite "wherein the response cryptogram is a hash." Support for Claims 32 and 46 can be found at least at *id.* at ¶ 110.

Claims 33 and 47 recite "wherein the interrogation conforms to a card specification and the set of inputs [used in generating the response cryptogram] is specified by the card specification." Support for Claims 33 and 47 can be found at least at *id.* at ¶¶ 119, 123, 129, 153, 161, and 186.

Claims 34 and 48 recite "wherein the request for digital credential data requests digital credential data comprising a first cryptogram and the at least one device response

communication comprises a second cryptogram, wherein the second cryptogram is the response cryptogram." Support for claims 34 and 48 can be found at least at *id.* at FIG. 28, ¶¶ 170 and 172, which describe an embodiment in which the mobile device receives a request for an expected cryptogram, but generates an unpredictable cryptogram as the response cryptogram.

Claims 35 and 49 recite that "generating the response cryptogram comprises encrypting the set of inputs using the local cryptographic key according to a digital encryption standard (DES) calculation to generate an output, wherein the cryptogram includes a portion, but not all, of the output." Support for claims 35 and 49 can be found at least at *id.* at ¶¶ 122 and 123.

Claims 36 and 50 recite "wherein the mobile device does not have connectivity to the wireless network during the interrogation." Support for Claims 36 and 50 can be found at least at *id.* at ¶¶ 146 and 187.

Claim 37 recites "prior to the interrogation, at a remote system, generating the first non-permanent cryptographic key, associating the first non-permanent cryptographic key with the account, and sending the first non-permanent cryptographic key and the account identifier to the mobile device over the wireless network; and after the interrogation, at the remote system, generating the second non-permanent cryptographic key, associating the second non-permanent cryptographic key with the account and sending the second non-permanent cryptographic key and the account identifier to the mobile device over the wireless network." Claim 52 recites "a remote computer system configured to generate the non-permanent cryptographic keys associated with the account and send each of the non-permanent cryptographic keys and the account identifier to the mobile device over the wireless network." Support for Claims 37 and 52 can be found at least at *id.* at ¶¶ 107, 109, 114, 128-129, 144, 146, 151-153, 165, 167, and 168.

Claim 38 recites "wherein the digital credential comprises a secure element representation maintained at the remote system." Claim 53 recites that "the remote computer system is configured to maintain a secure element representation for the account, wherein the digital credential comprises the secure element representation." Support for Claims 38 and 54 can be found at least at *id.* at ¶¶ 107, 114, 136, 185, and 217.

Claim 39 recites performing an authorization process at a remote system, the authorization process comprising "receiving an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the response cryptogram and the account identifier;" "determining a

current non-permanent cryptographic key associated with the account using the account identifier;" "calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account;" "verifying a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram;" and "sending an authorization response to the POS terminal, wherein the data contained in the authorization response is determined, at least in part, by the verifying the correctness of the response cryptogram." Claim 54 recites a remote computer system programmed to perform a similar authorization process. Support for Claims 39 and 54 can be found at least at *id.* at ¶¶ 107, 109, 114, 161.

Claims 40 and 55 recite that "the set of inputs [used in generation of the response cryptogram] comprises unpredictable data," "the authorization data comprises the unpredictable data" and "the calculated cryptogram is calculated using the unpredictable data." Claims 41 and 56 recite that "the POS command communications comprise the unpredictable data and the set of inputs comprises the unpredictable data." Support for Claims 40, 41, 55 and 56 can be found at least at *id.* at ¶¶ 153 and 161.

Claims 42 and 57 recite that "the authorization data further comprises values from the transaction, and wherein the POS terminal communicates the values from the transaction, the response cryptogram and the account identifier to the remote system in track 2 format." Claims 43 and 58 recite that "the authorization data further comprises values from the transaction and wherein the POS terminal communicates the values from the transaction, the response cryptogram and the account identifier to the remote system in BER-TLV format." Support for Claims 42 and 57 can be found at least at *id.* at ¶¶ 51 and 161. Support for Claims 43 and 58 can be found at least at *id.* at ¶ 109 which describe that, for example, "data in the read record response is formulated from data in the application system in proper APDU response BER-TLV format." *See, id.* at ¶ 109. A person of ordinary skill in the art at the time of filing would have understood that POS terminals can further send the response data to an authorization system in BER-TLV format.

Claim 51 recites that "the mobile device is programmed to request a new non-permanent cryptographic key after the interrogation." Support for Claim 51 can be found at least at *id.* at ¶¶ 128-129, 146, 151-153,165, 167 and 168.

Rejections under 35 U.S.C. § 112

Claims 1-29 stand rejected under 35 U.S.C. § 112, second paragraph. Claims 1-29 have been cancelled. Therefore, Applicant respectfully requests withdrawal of the rejection.

Rejections under 35 U.S.C. § 101

Claims 1-27 stand rejected under 35 U.S.C. § 101. Claims 1-29 have been cancelled rendering the rejection of Claims 1-27 moot. Applicant submits that new Claims 30-58 encompass patentable subject matter and should not be rejected under 35 U.S.C. § 101.

The United States Patent and Trademark Office ("USPTO" or "Office") has prepared guidelines for use by USPTO personnel in determining subject matter eligibility under 35 U.S.C. § 101. *See "Interim Eligibility Guidance,"* 79 Fed. Reg. 74618, 74624 (Dec. 16, 2014). The analysis of patent subject matter eligibility is a two-step process. In Step 1, the Office must determine as a threshold matter if the claim is directed to one of the four statutory categories of invention (i.e., process, machine, manufacture or composition of matter). *Id.* at 74621. In Step 2, the Office must determine whether the claimed invention is wholly directed to subject matter encompassing a judicially recognized exception. *Id.* The Step 2 inquiry involves a two-part analysis: Part 1-determine whether the claim is directed to a law of nature, a natural phenomenon or an abstract idea; and Part 2-determine whether any element or combination of elements is sufficient to ensure the claim amounts to significantly more than the judicial exception. *Id.* at 74622-23.

As set forth below, Claims 30-58 are directed to a statutory category of invention and are not directed to an abstract idea or other judicial exception. Therefore, the claims cannot be rejected under 35 U.S.C. § 101.

Step 1: Determine if the claim is directed to a statutory category of invention.

In Step 1 of the subject matter eligibility analysis, the Office must determine if a claim is directed to one of the four statutory categories of invention (i.e., process, machine, manufacture or composition of matter). *Id.* at 74621.

Claims 30-43 recite "a method for secure application-based participation in a payment card transaction authorization process by a mobile device" and Claims 44-58 recite "a system for secure application-based participation by a mobile device in point-of-sale interrogations." Here, the claims are clearly directed to a statutory category of invention.

Step 2: Part 1 Determine if the claim is directed to an abstract idea.

In Step 2: Part 1 of the subject matter eligibility analysis, the Office is first to determine what the claim is "directed to." *Interim Eligibility Guidance* at 74622. The Office must identify the purpose of the claim—in other words, what the claimed invention is trying to achieve—and ask whether that purpose is abstract. *See, id.* ("it is important to understand what the applicant has invented and is seeking to patent"). With the purpose of the claim identified, the Office must identify the judicial exception recited in the claim. *Id.* Applicant notes the guidelines provided by the USPTO do not themselves define an abstract idea and on the matter include only examples of abstract ideas to use as guidelines. (*See, Abstract Idea Examples,* January 27, 2015) ("*Jan. 2015 Examples*"); *USPTO July 2015 Update: Subject Matter Eligibility* ("*July 2015 Update*")). The *July 2015 Update* cautions that a claimed concept should not be identified as an abstract idea "unless it is similar to at least one concept that the courts have identified as an abstract idea." *See, July 2015 Update* at 3.

The new independent claims, Claims 30 and 44, are not directed to an abstract idea or other judicial exception. Instead, the claims are directed to systems and methods for using an interrogable application that runs in a mobile device's operating system to securely participate in point-of-sale interrogations (e.g., interrogations with smart card readers). The claimed solution is rooted in computer technology in order to overcome problems specifically arising from *inter alia* memory accessibility by applications running in the operating system of a mobile device and network delays and latency. Under the Office's guidelines, such claims cannot be found to be patent ineligible under 35 U.S.C. § 101.

Background

To understand the claimed invention, some background in electronic payment systems and mobile devices will be helpful. While implementation details may vary, the following discussion is meant to provide a high level understanding of the background and some of the technical problems that the claimed solutions address.

Traditional magnetic stripe payment cards present significant security risks because the data on the magnetic stripe is typically static. Consequently, each time the card is swiped at a point-of-sale terminal, the magnetic card reader at the point-of-sale terminal extracts the same data. *See, Application* at ¶ 43. Security relies on the card holder's written signature, PIN and/or

visual inspection of the card by the point-of-sale terminal operator (e.g., cashier) to prevent a user from fraudulently presenting a card. In recent years, there have been well publicized cases in which magnetic stripe data has been captured by malicious code on a retailer's network, fake magnetic card readers or by other means. Because the magnetic stripe data does not change, it can be copied to another card or mobile device and used to make transactions continuously from the copy with no technical limitation. *Id.*

Smart payment cards were developed to enhance security. While they cannot prevent all forms of fraud, smart payment cards do limit card duplication so that a fraudulent card cannot be used at a point-of-sale (e.g., a retailer's checkout). A conventional smart payment card includes a tamper resistant microchip, referred to as a hardware "secure element," that uses cryptographic techniques to make duplicating the card difficult. *See, e.g., id.* at ¶ 3. The secure element chip has a burned-in or otherwise permanently stored cryptographic key associated with the card holder's personal account number (PAN) ("permanent" in that the cryptographic key does not change over the life of the secure element). When a conventional smart payment card is presented at a point-of-sale terminal for payment of a transaction, an electronic secure element reader at the point-of-sale (e.g., a contact or contactless smart payment card reader) interrogates the secure element microchip for digital credential data used to authorize the transaction against the card holder's account. *Id.* at ¶ 4. During the interrogation, a payment application embedded in the secure element microchip (the "embedded secure element payment application") generates a single use cryptogram using, in part, the permanent cryptographic key stored in the secure element microchip. The secure element chip returns the cryptogram along with other information to the secure element reader.

To authorize a transaction, the POS terminal typically sends the information to a backend authorization system. This information may include, for example, the cryptogram received from the secure element, an account identifier (e.g., PAN), transaction specific information and other information. As part of the authorization process, the backend authorization system generates a cryptogram using a copy of the permanent cryptographic key. The digital credential data provided by the secure element is verified in part by comparing the cryptogram received from the secure element microchip with the cryptogram generated by the authorization system.

The reader and secure element on the smart card typically follow industry standards and "card specifications" set forth by secure element payment application providers. *Id.* The card specifications are technical specifications that specify *inter alia* the interrogation (the command

requests and responses between a smart payment card and point-of-sale to deliver a complete credential for authorizing a transaction), the mechanisms by which cryptograms should be generated, etc. Card specifications typically specify that interrogations occur using industry standard protocols.

To provide an example, FIG. 2 of the *Application*, reproduced below, shows the flow of an interrogation between an electronic reader and secure element according to the MASTERCARD PayPass Ver. 3.3 card specification. The interrogation occurs using Application Data Protocol Unit (APDU) commands and responses (ISO/IEC 7816-4).

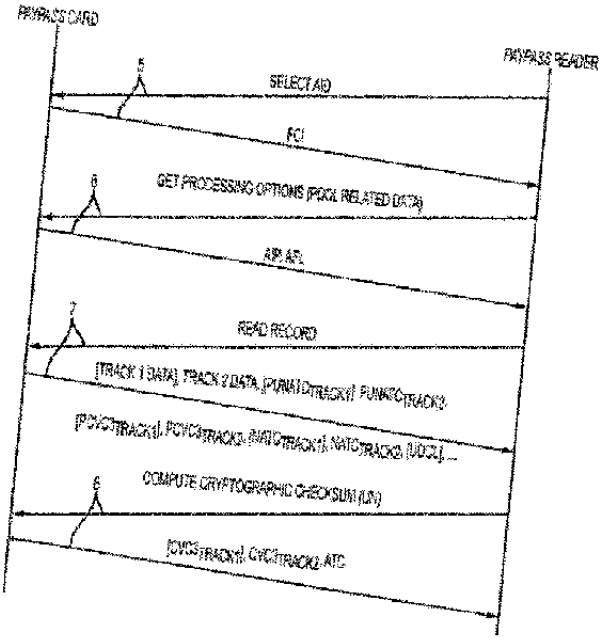


FIG. 2

Application, FIG. 2

During interrogation of a conventional smart payment card, the smart element reader typically requests that the secure element provide a cryptogram. This is shown by the COMPUTE CRYTOGRAPHIC CHECKSUM APDU in FIG. 2, above. According to various card specifications, the embedded secure element payment application in a conventional secure element microchip generates the response cryptogram based in part on the permanent

cryptographic key stored in the secure element. For example, a conventional secure element microchip operating according to the MASTERCARD PayPass Ver. 3.3 card specification will generate a CVC3 cryptogram using the permanent cryptographic key KD_{CVC3}. *See, e.g., id.* at ¶¶ 122; *see also id.* at ¶ 123 ("This card specification expects KD_{CVC3} to be a permanent cryptographic key"). As part of authorizing payment for a transaction, the cryptogram generated by the secure element microchip is verified by a backend authorization system that also generates a cryptogram (e.g., the CVC3 cryptogram) using a copy of the same permanent cryptographic key.

Conventional smart payment cards prevent duplication of cards in part because the permanent encryption key of a secure element is needed to duplicate the secure element. However, according to the various card specifications and as understood by those in the art, the cryptograms generated by the secure element do not contain the permanent cryptographic key. Therefore, capturing the data from a transaction—such as through malicious code on a retailer's network—does not provide sufficient information to duplicate a card. Moreover, conventional secure element microchips are tamper resistant such that it is extremely difficult, if not impossible, to extract the permanent cryptographic key from the secure element microchip.

Mobile devices may incorporate secure element microchips (e.g., in SIM cards, secure ICs etc.) so that the mobile device can serve essentially as an electronic smart payment card. A conventional mobile device of this type will run an operating system that controls, among other aspects of the mobile device, interfaces with the SIM, secure IC or other hardware containing the secure element microchip. While an application (e.g., wallet) on the mobile device may provide a user interface, the secure element microchip in the mobile device is still responsible for responding to interrogations. Typically, the secure element microchip is isolated from the operating system of the mobile device to provide a trusted execution environment such that the operating system and applications running in the operating system do not have access to the permanent cryptographic key of the secure element during interrogations. Thus, even if a malicious app is installed on the mobile device, the secure element cannot be duplicated.

Secure element payment systems require that the user have physical possession of a "card" (e.g., card or mobile device with a secure element microchip) that matches the authorization capabilities of a merchant's system where a purchase is made. *See, id.* at ¶ 5. Many mobile devices, however, do not have a secure element microchip for electronic payment or, if they do, the secure element microchip may be limited to a single or limited number of card

specifications and accounts. The *Application* recognizes that a more flexible system for mobile payment authorization is required. *Id.*

The inventor developed a system that allows mobile devices to be used with secure element payment authorization systems without requiring that the mobile device have a matching secure element chip installed on the mobile device. According to the *Application*, an application executing in the operating system of the mobile device may participate in interrogations with electronic secure element readers (e.g., contactless secure element readers). The use of an interrogable application running in the operating system of the mobile device obviates the need for a secure element microchip at the mobile device or expands the capabilities of the mobile device that has a limited capability secure element microchip. Thus, electronic payment systems and processes "may be extended to facilitate transactions at a point-of-sale terminal where it is not necessary for the user (e.g., the purchaser) to have physical possession of a secure element at the point-of-sale"). *See, id.* at ¶ 55. More specifically, the claims include features to address the problems of i) allowing an application running in the operating system of a mobile device to be interrogated for digital credential data by a POS terminal, that if adhering to conventional card specification functioning for generating a response cryptogram, would create a security risk ii) while retaining low latency during interrogations.

Applications running in an operating system often share or have access to the same memory. Consequently, malicious code (e.g., malware) executing in the operating system of the mobile device may be able copy data used by another application. The inventor appreciated that this aspect of computer technology would present a security problem for an interrogable application. More particularly, as discussed above, a secure element microchip conventionally responds to a COMPUTE CRYTOGRAPHIC CHECKSUM APDU command by generating a cryptogram using the permanent cryptographic key associated with the user's PAN. For an interrogable application running in the operating system of the mobile device to generate a cryptogram in this manner, the application would have to load the permanent cryptographic key into memory accessible to the application, potentially exposing the permanent cryptographic key to other software running in the operating system, including possible malware programmed to steal the key and other information that could be used to fraudulently to duplicate the mobile device for purposes of POS payment.

The *Application* describes several ways to address the problem of allowing an application running in the operating system of the mobile to securely participate in interrogations with a POS

terminal. Several of these solutions introduce delays in the interrogation process. According to one embodiment, a secure element for a mobile device is maintained at a remote system (a "Remote Hosted Secure Element"). *See, id.* at ¶ 55. During an interrogation, the mobile device contacts the remote hosted secure element to collect the data necessary to respond to interrogation. As described in conjunction with FIGS. 15 and 16, for example, when the mobile device receives a COMPUTE CRYTOGRAPHIC CHECKSUM APDU from a reader, the mobile device passes the APDU to a remote system. The Remote Hosted Secure Element for the mobile device generates the appropriate cryptogram (e.g., using a permanent cryptographic key associated with the account) and the remote system sends the cryptogram back to the mobile device. The mobile device then sends the cryptogram to the reader in response to the COMPUTE CRYTOGRAPHIC CHECKSUM APDU. These solutions provide the advantage that the mobile device does not need to access the permanent cryptographic key. However, solutions such as those described in FIG. 15 and, to a lesser extent, FIG. 16 can introduce delays in the interrogation process that may have deleterious effects, such as causing an interrogation to time out. These delays occur because "each round trip request to the remote SE is subject to network delay and latency". *See, id.* at ¶ 85.

Claim 30, on the other hand, recites "a method for secure application-based participation in a payment card transaction authorization process by a mobile device" that addresses the problem of allowing an application running in the operating system of a mobile device to securely participate in interrogations with a POS terminal for digital credential data while retaining low latency. According to Claim 30, "the [interrogable] application [executable in the operating system of the mobile device] does not access a permanent cryptographic key associated with the account during interrogations." Instead, as shown be the emphasized portions of Claim 30 below, the application generates response cryptograms during interrogations based on a non-permanent key that changes between at least two interrogations:

> 30. (New) A method for secure application-based participation in a payment card transaction authorization process by a mobile device, the method comprising:
> **receiving over a wireless network at a mobile device a first non-permanent cryptographic key associated with an account having a corresponding digital credential**, wherein the mobile device comprises an operating system and an application executable in the operating system, the application interrogable for digital credential data corresponding to the account, wherein the application does not access a permanent cryptographic key associated with the account during interrogations;

locally storing a first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;
participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device comprising:
receiving at least one POS command communication sent by the POS terminal over a communications channel, wherein the at least one POS command communication comprises a request for digital credential data to authorize a transaction against the account;
generating a response cryptogram based on a set of inputs and **the local cryptographic key associated with the account**, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram; and
responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to the electronic reader through the communication channel, the at least one device response communication comprising at least a portion of the digital credential data, wherein the at least a portion of the digital credential data comprises the response cryptogram and an account identifier for the account;
receiving a second non-permanent cryptographic key at the mobile device, wherein the second non-permanent cryptographic key is associated with the account; and
replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key as the local cryptographic key associated with the account prior to the application participating in a subsequent interrogation.

Claim 30 claims a solution that helps address security issues that arise from using an interrogable application executable in the operating system of the mobile device to respond to interrogations at least because the key used to generate response cryptograms changes, limiting the key's usefulness if stolen by other code running in the operating system of the mobile device. Moreover, the claimed invention helps address the issue of network delay and latency during an interrogation by retaining response cryptogram generation at the mobile device.

Analysis

Claims 30 and 44 do not recite a "fundamental economic practice," an "idea of itself," "certain methods of organizing human activity," "mathematical relationships/formulas," or "comparing new and stored information and using rules to identify options." Nor do the claims recite the performance of some business practice known from before mobile computing device technology along with the requirement to perform it on a mobile device. Instead, the claimed

solution is necessarily rooted in computer technology in order to overcome problems specifically arising from computer technology and computer networks.

The claims address using an interrogable application executing in the operating system of a mobile device to participate in interrogations with POS terminals. In particular, the claims address security problems that arise from shared memory accessibility by applications executing in the operating system and problems of delay and latency in computer networks. The *Interim Eligibility Guidance, Jan. 2015 Examples* and *July 2015 Update* identify no similar concept that has been found by a court to be abstract. To the contrary, the examples provided by the Office show that such claims—claims specifically rooted in computer technologies—should not be found to be abstract. *See, Jan. 2015 Examples* at 5-6 (finding a claim patent eligible where "the claimed solution is necessarily rooted in computer technology in order to overcome a problem specifically arising the realm of computer networks")(citing *DDR Holding LLC v. Hotels.com et al.,* 113 USPQ 2d 1097 (Fed. Cir. 2014)); *id.* at 3 ("the invention claimed here is directed towards performing isolation and eradication of computer viruses, worms and malicious code, a concept inextricably tied to computer technology and distinct from the types of concepts found by the courts to be abstract.").

Claims 30 and 44, are not directed to any concept that has been identified as abstract and are akin to claims that the Office has recognized as patent eligible. The claims therefore cannot be properly rejected under 35 U.S.C. § 101. *See, July 2015 Update* at 3 (it should be ensured "that a claimed concept is not identified as an abstract idea unless it is similar to at least one concept that the courts have identified as an abstract idea").

Step 2: Part 2 Determine if the claim is directed to significantly more than the judicial exception.

Under the *Interim Eligibility Guidance*, no analysis of the Claims under Step 2: Part 2 is necessary. From the foregoing discussion, however, it is apparent that the claims include limitations that amount to more than simply stating "apply an abstract idea at a mobile device." The claims include features for resolving problems that are rooted in computer technology, including security issues arising from shared access to memory by applications running in the operating system of a mobile device and delays and latency of computer networks. Therefore, when taken as a whole, the claimed invention has limitations that amount to significantly more

than an abstract idea. Under Step: Part 2 of the *Interim Eligibility Guidance* analysis framework, the claims recite patent eligible subject matter and should not be rejected under 35 U.S.C. § 101.

Rejections under 35 U.S.C. §§ 102 and 103

Claims 1, 2 and 28 were rejected as anticipated by U.S. Publication No. 2008/0040285 ("*Wankmueller*"). Claims 3-24, 27 and 29 were rejected as obvious over *Wankmueller* in view of U.S. Publication No. 2004/0143550 ("*Creamer*"). Claims 25 and 26 stand rejected as obvious over *Wankmueller* in view of *Creamer* and further in view of U.S. Publication No. 2012/0109764 ("*Martin*"). These rejections are rendered moot by the cancellation of Claims 1-29.

Wankmueller teaches a mobile device that "generates a dynamic authentication code 130 using a key 120, such as an encryption key." *Wankmueller* at ¶ 16. *Wankmueller,* does not teach "receiving over a wireless network at a mobile device a first non-permanent cryptographic key associated with an account having a corresponding digital credential," "locally storing a first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account," "generating a response cryptogram based on a set of inputs and the local [non-permanent] cryptographic key associated with the account," "receiving a second non-permanent cryptographic key at the mobile device, wherein the second non-permanent cryptographic key is associated with the account" and "replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key as the local cryptographic key associated with the account prior to the application participating in a subsequent interrogation" as recited in Claim 30. Therefore, *Wankmueller* does not anticipate Claim 30. For similar reasons *Wankmueller* does not anticipate Claim 44.

Moreover, *Wankmueller* teaches:

> The memory of the mobile device should contain no information that would identify the account with which the key 120 corresponds. Specifically, the key 120, and the mobile device memory, should not contain the payment account number (PAN), card expiry date, card track data typically stored on a transaction card magnetic stripe, the account holder name, nor any other data that could uniquely identify the financial account. In this way, if the mobile device is stolen or compromised, the device could not be used to perform a transaction as there would be no data identifying the financial account to which the key 120 corresponds.

Id. at ¶ 17; *see also id.* at ¶ 6 ("the mobile device will not contain data that could identify the particular account associated with it"). It thus appears that the mobile device of *Wankmueller* does not include the account identifier.

To the extent account identifying information is used in the authorization process of *Wankmueller*, it "should be collected using various techniques well known to personas skilled in the art. For example, the account identifier 140 may be stored on a magnetic stripe card 145, or a smart card, or collected through user input to a device such as a keypad, keyboard or input device." *See id.* at ¶ 29. *Wankmueller* does not teach that the mobile device responds to a POS terminal with a response "comprising at least a portion of the digital credential data, wherein the at least a portion of the digital credential data comprises the response cryptogram and an account identifier for the account." For at least this additional reason, *Wankmueller* does not anticipate Claim 30. For similar reasons readily apparent from the foregoing, *Wankmueller* does not anticipate Claim 44.

Applicant further submits that a person of ordinary skill in the art would not combine the teachings of *Creamer* and *Martin* cited by the Examiner with *Wankmueller* to achieve the claimed invention. Accordingly, Applicant respectfully requests allowance of the pending claims.

Conclusion

Applicant has now made an earnest attempt to place this case in condition for allowance. Other than as explicitly set forth above, this reply does not include an acquiescence to statements, assertions, assumptions, conclusions, or any combination thereof in the Office Action. For the foregoing reasons and for other reasons clearly apparent, Applicant respectfully requests full allowance of the pending claims. The Examiner is invited to telephone the undersigned at the number listed below for prompt action in the event any issues remain.

An extension of three (3) months is requested and a Notification of Extension of Time Under 37 C.F.R. § 1.136 with the appropriate fee is enclosed herewith.

The Director of the U.S. Patent and Trademark Office is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

Sprinkle IP Law Group
Attorneys for Applicant

John L. Adair
Reg No. 48,828

Date: March 22, 2016

1301 W. 25th Street, Suite 408
Austin, TX 78705
Tel. (512) 637-9220
Fax. (512) 371-9088

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
NOTIFICATION OF EXTENSION OF TIME UNDER 37 C.F.R § 1.136	Atty. Docket No. **STAPP1100-5**

First Named Inventor **C. Douglas Yeager**	
Application Number **13/599,647**	Date Filed **August 30, 2012**
Title **Systems and Methods for Secure Application-Based Participation in an Interrogation by Mobile Device (as amended)**	
Group Art Unit **3695**	Examiner **Puttaiah, Asha**
Confirmation Number **1919**	

Certificate of Transmission Under 37 C.F.R. § 1.8

I hereby certify that this correspondence is being deposited electronically with the U.S. Patent and Trademark Office using the United States Patent and Trademark Office's EFS-Web system on **March 22, 2016.**

Delia Narvaiz

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby takes an Extension of Time for responding to the **Office Action** mailed **October 6, 2015** for a period of **three** (3) months.

		Small Entity	*Large Entity*
	First Month	$ 100.00	$ 200.00
	Second Month	$ 300.00	$ 600.00
X	Third Month	$ 700.00	$ 1,400.00
	Fourth Month	$ 1,100.00	$ 2,200.00
	Fifth Month	$ 1,500.00	$ 3,000.00
	TOTAL	**$ 700.00**	**$**

The Commissioner is hereby authorized to deduct the above-noted fee from Deposit Account 50-3183 of Sprinkle IP Law Group. If any fees are inadvertently omitted, additional fees are required, or if any amounts have been overpaid, please appropriately charge or credit those fees to Deposit Account No. 50-3183 of SPRINKLE IP LAW GROUP.

Respectfully submitted,

SPRINKLE IP LAW GROUP

John L. Adair
Reg. No. 48,828

Date: March 22, 2016

1301 W. 25th Street, Suite 408
Austin, Texas 78705
(512) 637.9220 - Telephone
(512) 371.9088 - Facsimile

Electronic Patent Application Fee Transmittal

Application Number:	13599647
Filing Date:	30-Aug-2012
Title of Invention:	SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Filer:	John L. Adair/Delia Narvaiz
Attorney Docket Number:	Simplytapp0002US1

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	2253	1	700	700
Miscellaneous:				
		Total in USD ($)		**700**

Electronic Acknowledgement Receipt	
EFS ID:	25275263
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Customer Number:	122870
Filer:	John L. Adair/Delia Narvaiz
Filer Authorized By:	John L. Adair
Attorney Docket Number:	Simplytapp0002US1
Receipt Date:	22-MAR-2016
Filing Date:	30-AUG-2012
Time Stamp:	19:17:19
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$700
RAM confirmation Number	5661
Deposit Account	503183
Authorized User	ADAIR, JOHN L
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 CFR 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)

Charge any Additional Fees required under 37 CFR 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		STAPP1100-5_ROA_032216.pdf	2927078 18663c7f81df1ac3b668be3f55e17d7b9d372075	yes	41

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Specification	2	17
	Claims	18	24
	Applicant Arguments/Remarks Made in an Amendment	25	41

Warnings:					
Information:					
2	Extension of Time	STAPP1100 5_EOT.pdf	987939 ab3e745544a8eff794a56002f0891522d11625166	no	1
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	31010 d160beb46048bae534da750e91e02ddba77557f6	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	3946027		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/599,647	Filing Date 08/30/2012	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 = *		X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 = *		X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 03/22/2016	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	(Column 3) ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 29	Minus	** 29	= 0	X $40 =	0
Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	(Column 3) ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/DORIS BURNS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/599,647
				Filing Date	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	Puttaiah, Asha
Sheet	1	of	1	Attorney Docket Number	STAPP11100-5

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A21	US 20120317628	12-13-2012	Yeager	
	A22	US 20020026414	02-28-2002	Nakajima et al.	
	A23	US 20100153721	06-17-2010	Mellqvist	
	A24	US 20110099079	04-28-2011	White	
	A25	US 20090210308	08-20-2009	Toomer et al.	
	A26	US 20090143104	06-04-2009	Loh et al.	
	A27	US 20070156436	07-05-2007	Fisher et al.	
	A28	US 20090075592	03-19-2009	Nystrom et al.	
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	B1	WO 2001/008113	02-01-2001	Visa Int'l Service Assn	
	B2	WO 2009/017754	02-05-2009	Ebay Inc.	

Examiner Signature		Date Considered	

Substitute Form PTO/SB/08b

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/599,647
				Filing Date	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	Puttaiah, Asha
Sheet	1	of	1	Atty Docket Number	STAPP1100-5

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C1	International Search Report and Written Opinion for Int'l Application No. PCT/US2012/041670, mailed 08/17/2012, 15 pgs.	
	C2	International Search Report and Written Opinion for Int'l Application No. PCT/US2012/053129, mailed 11/16/2012, 12 pgs.	
	C3	International Preliminary Report on Patentability for Int'l Application No. PCT/US2012/041670, mailed 12/10/2013, 14 pgs.	
	C4	International Preliminary Report on Patentability for Int'l Application No. PCT/US2012/053129, mailed 12/10/2013, 11 pgs.	
	C5	European Search Report for European Patent Application No. 12827026.1, dated 05/05/2015, 14 pgs.	
	C6	Office Action for U.S. Patent Application No. 13/491,922, mailed 07/27/2015, 14 pgs.	

Examiner Signature		Date Considered	

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 67979.W1	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US2012/041670	International filing date *(day/month/year)* 08 June 2012	(Earliest) Priority Date *(day/month/year)* 09 June 2011
Applicant YEAGER, C.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of:

☒ the international application in the language in which it was filed.

☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).

c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. ☐ **Certain claims were found unsearchable** (see Box No. II)

3. ☐ **Unity of invention is lacking** (see Box No. III).

4. With regard to the **title**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,

a. the figure of the **drawings** to be published with the abstract is Figure No. 1

☒ as suggested by the applicant.

☐ as selected by this Authority, because the applicant failed to suggest a figure.

☐ as selected by this Authority, because this figure better characterizes the invention.

b. ☐ none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/041670

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q20/12 (2012.01)
USPC - 705/16
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - G06Q20/02, 20/06, 20/12, 20/18 (2012.01)
USPC - 705/16, 17, 21, 26.1

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
MicroPatent, PatBase, Google Patents, Engineering Village

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X -- Y	US 2007/0075133 A1 (YEAGER) 5 April 2007 (05.04.2007) entire document	1-3 --- 4, 11-34, 36-52, 55-56
X -- Y	US 2009/0044012 A1 (BISHOP et al.) 12 February 2009 (12.02.2009) entire document	53-54 --- 8, 10, 14-15, 21, 24-26, 28-34, 47-52
Y	US 2008/0238610 A1 (ROSENBERG) 2 October 2008 (02.10.2008) entire document	5-34, 36-52, 55-56
Y	US 2010/0274726 A1 (FLOREK et al.) 28 October 2010 (28.10.2010) entire document	5-10
Y	US 6,199,762 B1 (HOHLE) 13 March 2001 (13.03.2001) entire document	4, 16, 22, 39, 45
Y	US 2004/0118914 A1 (SMITH et al.) 24 June 2004 (24.06.2004) entire document	6-8
Y	US 2006/0224470 A1 (GARCIA RUANO et al.) 5 October 2006 (05.10.2006) entire document	7, 27
Y	US 2008/0046367 A1 (BILLMAIER et al.) 21 February 2008 (21.02.2008) entire document	9
Y	US 2003/0163708 A1 (TANG) 28 August 2003 (28.08.2003) entire document	23
Y	US 7,774,231 B2 (POND et al.) 10 August 2010 (10.08.2010) entire document	35, 46

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 July 2012	17 AUG 2012
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: JAMES PALMER
LUEDEKA NEELY GROUP, P.C.
P.O. BOX 1871
KNOXVILLE, TN 37901-1871

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	17 AUG 2012
Applicant's or agent's file reference 67979.W1	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2012/041670	08 June 2012	09 June 2011

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - G06Q20/12 (2012.01)
USPC - 705/16

Applicant YEAGER, C.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	31 July 2012	Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (July 2011)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	4-52, 55-56	YES
	Claims	1-3, 53-54	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-56	NO
Industrial applicability (IA)	Claims	1-56	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-3 lack novelty under PCT Article 33(2) as being anticipated by Yeager.

Regarding Claim 1, Yeager discloses a system (see figs. 3-4 and 6) for acquiring digital credential data (see pgs. 3-4, para. 0026-0029 and 0031-0032; wherein the credential data is interpreted to be tag emulation data associated with portions of a specified user account information that is needed to carry out or complete electronic transactions) comprising: an electronic communication device (host 350; see fig. 3); a [inherent] communication channel (various connections that allow communication and data to be transferred between the adapter 100 and host 350 as well as between server 320 and adapter 100 via host 350 and internet connections; see figs. 3 and 6 as well as pgs. 3-4, para. 0026-0028 and 0031); and a repository (server 320 in combination with database 610; see figs. 3 and 6) remote from the electronic communications device (see figs. 3 and 6; wherein the server and associated database is inherently remote from host 350 since access and communication between the server and communications device is carried out through an internet connection) and having a plurality of secure element representations (see fig. 6 as well pgs. 3-4, para. 0031-0032; wherein a plurality of secure element representations is interpreted to be the stored customer account information associated with a plurality of users/customers), wherein the repository is configured to: a) receive a request for the digital credential data from the electronic communications device using the communication channel (see fig. 6 as well as pgs. 3-4, para. 0031-0032), b) validate [authenticate] the computing device (via inherently checking a secret key associated with a particular adapter 100 in combination with a user or customer entering a username and password; see pg. 3, para. 0031), wherein the electronic communication device is paired with one of the plurality of secure element representations (associated with a specific customer/user; see pgs. 3-4, para. 0031-0032); c) extract at least a portion of the digital credential data from the paired secure element representation (in order to complete a transaction see fig. 6 as well as pgs. 3-4, para. 0031-0032), and d) send a repository response communication with the digital credential data to the electronic communication device over the communication channel (see fig. 6 as well as pgs. 3-4, para. 0031-0032); and wherein the electronic communication device is configured to a) authenticate to the repository (via the use of a secret key associated with a particular adapter 100 in combination with a user or customer entering a username and password; see pg. 3, para. 0031), b) send a request for the acquisition of at least a portion of the digital credential data to the repository as a device command communication over the communication channel (in order to complete a transaction; see fig. 6 as well as pgs. 3-4, para. 0031-0032), and c) receive the repository response containing the digital credential data from the repository over the communication channel (in order to complete a transaction; see fig. 6 as well as pgs. 3-4, para. 0031-0032).

Regarding Claim 2, Yeager discloses all limitations of claim 1 and further discloses the electronic communication device being a mobile device (a pda, mobile phone or laptop; see pg. 3, para. 0027).

Regarding Claim 3, Yeager discloses all limitations of claim 1 and further discloses the electronic communication device being a stationary device (a personal computer; see pg. 4, para. 0035).

Claim 4 lacks an inventive step under PCT Article 33(3) as being obvious over Yeager in view of Hohle.

Regarding Claim 4, Yeager discloses all limitations of claim 1, but does not disclose the repository uses IS07816 to extract at least a portion of the digital credential data from a paired secure element representation.
However, Hohle is in the field of facilitating commercial transactions over a network (Col. 1, lines 7-11) and discloses a repository that uses IS07816 to extract at least a portion of the digital credential data from a paired secure element representation (card object database 116 is the repository; Col. 4, lines 13-24).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Hohle's feature in to Yeager's system. The motivation would have been to provide for the use of an internationally accepted standard (Hohle, Col. 4, lines 13-24).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Claim 5 lacks an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Florek et al., hereinafter referred to as Florek.

Regarding Claim 5, Rosenberg discloses a method (see figs. 9-10 as well as pgs. 8-10, para. 0097-0103 and 0105-0113) for acquiring digital credential data (the necessary portions of the user's financial account information that is needed to complete a transaction; see pgs. 9-10, para. 0102 and 0111) by a point-of-sale terminal (POS device 520 of fig. 9) having access to an internet from a mobile device (smartlink capable device 900 of fig. 9; see also pg. 8, para. 0097) that has access to the internet (in order to establish a communication link between the device and the user's financial institution as well as the payee's financial institution; see figs. 9-10 as well as pg. 10, para. 0111-0112).
But, Rosenberg does not specifically teach the mobile device of the method having a secure element and a secure element reader; and the method comprising: a) reading the secure element in the mobile device using the secure element reader in the mobile device; and b) sending the digital credential data, acquired from reading the secure element in the mobile device, from the mobile device to the point-of-sale terminal over the internet.
However, Florek discloses a system and method of contactless authorization of an electronic payment (see the Abstract, for example); wherein Florek teaches the concept of the method and associated system including a mobile device (mobile communication device 1; see fig. 1) having a secure element (2; see fig. 1) and a secure element reader (NFC communications element 7 in combination with carrier 13; see fig.1 as well as pgs. 2-3, para. 0021-0023 and 0026-0027) in order to carry out electronic transactions between a user and POS terminal (see pgs. 2-3, para. 0025-0027); and wherein the method comprises a) reading the secure element in the mobile device using the secure element reader in the mobile device (in order to complete a transaction or purchase by a user; see pgs. 2-3, para. 0025-0027); and b) sending the digital credential data, acquired from reading the secure element in the mobile device, from the mobile device to the point-of-sale terminal over the internet (in order to complete a transaction or purchase by a user; see pgs. 2-3, para. 0025-0027).
It would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the method of Rosenberg include a mobile device having a secure element and a secure element reader, and the method comprising the steps recited above, as shown by Florek, for the purpose of initiating and complete an electronic transaction or purchase by a user.

Claim 6 lacks an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Florek and futher in view of Smith.

Regarding Claim 6, Rosenberg in view of Florek disclose all limitations of claim 5, but does not disclose acquiring in the mobile device a unique identifier of the point-of-sale terminal as an identified point-of-sale terminal; and establishing a unique network address of the identified point-of-sale terminal, and wherein step b) comprises sending the digital credential data to the identified point-of-sale terminal over the internet.
However, Smith is in the field of acquiring credential data (Par. 0048) and discloses acquiring in the mobile device a unique identifier of the point-of-sale terminal as an identified point-of-sale terminal (the IP address of the terminal is the unique identifier; Par. 0115); and establishing a unique network address of the identified point-of-sale terminal, and wherein step b) comprises sending the digital credential data to the identified point-of-sale terminal over the internet (data sent to the IP address of the terminal is sent over the Internet; Par. 0115).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Smith's feature in to modified Rosenberg's system. The motivation would have been to provide Internet accessibility for point of sale terminals (Smith, Par. 0115).

Claim 7 lacks an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Florek, in view of Garcia Ruano and further in view of Smith.

Regarding Claim 7, Rosenberg in view of Florek disclose all limitations of claim 5, but does not disclose reading a QR code into the mobile device; and translating the QR code in the mobile device to identify an internet address of the point-of-sale terminal, and wherein step b) comprises sending the digital credential data over the internet to the internet address of the point-of-sale terminal.
However, Garcia Ruano is in the field of using a mobile phone as a payment device (Abs.) and discloses reading a QR code into the mobile device; and translating the QR code in the mobile device (the barcode is the QR code; Par. 0040).
Further, Smith is in the field of acquiring credential data (Par. 0048) and discloses sending the digital credential data over the internet to the internet address of the point-of-sale terminal (data sent to the IP address of the terminal is sent over the Internet; Par. 0115).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Garcia Ruano's and Smith's feature in to modified Rosenberg's system. The motivation would have been to allow for the use of barcodes (Garcia Ruano, Par. 0040) and to provide Internet accessibility for point of sale terminals (Smith, Par. 0115).

Claim 8 lacks an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Florek, in view of Bishop and further in view of Smith.

Regarding Claim 8, Rosenberg in view of Florek disclose all limitations of claim 5, but does not disclose reading an RFID tag code into the mobile device; and translating the RFID tag code in the mobile device to identify an internet address of the point-of-sale terminal, and wherein step b) comprises sending the digital credential data over the internet to the internet address of the point-of-sale terminal.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses reading an RFID tag code into the mobile device; and translating the RFID tag code in the mobile device (RFID transaction device, is the mobile device; Par. 0039).
Further, Smith is in the field of acquiring credential data (Par. 0048) and discloses sending the digital credential data over the internet to the internet address of the point-of-sale terminal (data sent to the IP address of the terminal is sent over the Internet; Par. 0115).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's and Smith's feature in to modified Rosenberg's system. The motivation would have been to allow for the use of RFID tags (Bishop, Par. 0039) and to provide Internet accessibility for point of sale terminals (Smith, Par. 0115).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Claim 9 lacks an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Florek and further in view of Billmaier.

Regarding Claim 9, Rosenberg in view of Florek disclose all limitations of claim 5, but does not disclose using a GPS geo-location utility in the mobile device to define an internet address of the point-of-sale terminal, and wherein step b) comprises sending the digital credential data over the internet to the internet address of the point-of-sale terminal.
However, Billmaier is in the field of authenticating commercial transactions (Abs.) and disclose using a GPS geo-location utility in the mobile device to define an internet address of the point-of-sale terminal (GPS is used to detect the IP address; Par. 0008), and wherein step b) comprises sending the digital credential data over the internet to the internet address of the point-of-sale terminal (data sent to the terminal's IP address, is sent over the Internet; Par. 0008).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Billmaier's feature in to modified Rosenberg's system. The motivation would have been to provide security for the user by preventing fraudulent transactions (Billmaier, Par. 0008).

Claim 10 lacks an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Florek and further in view of Bishop.

Regarding claim 10, Rosenberg in view of Florek disclose all limitations of claim 5, but lacks explicitly teaching translating the digital credential data received by the point-of-sale terminal into Track Data, and delivering the Track Data to a field in a transaction authorization system using keyboard emulation.
In the field of RF Transaction authentication, Bishop teaches translating the digital credential data received by the point-of-sale terminal into Track Data, and delivering the Track Data to a field in a transaction authorization system using keyboard emulation (para [0031] account information is stored as track 1 and track 2 data as defined in ISO/IEC 7813; para [0036]-[0037] authentication data may be forwarded or encoded in all or a portion of a data stream, representing data encoded in track 2 or track 3 format; para [0031], wherein the stream of data may look like "0000 0000 00000000" which is a stream of keys).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of Rosenberg in view of Florek to include the method of communicating account related data of Bishop in order to secure customer related information (Bishop, para [0010]).

Claims 11-13, 17-20, 36-38, 40-44 and 55-56 lack an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Yeager.

Regarding Claim 11, Rosenberg discloses a method (see figs. 4-5, 7 and 9-10 as well as pgs. 5-6 and 8-10, para. 0056-0072, 0074, 0097-0103 and 0105-0113) for acquiring digital credential data (a transaction confirmation signal in combination with the necessary portions of the complete user account and credit card information that is associated with the financial institutions of a user and used to complete a transaction; see pg. 10, para. 0111-0113, for example) by a point-of-sale terminal (POS device 420/520; see figs. 4 and 9) comprising: a mobile device (device 110/900 of figs. 4 and 9) in combination/connection with a repository (an inherent memory associated with the smartlink device 100 that is connected to device 110/an inherent memory associated with device 900 that has securely stored user financial account information in combination with a buyer's/user's financial institution 470; see figs. 4 and 9 as well as pgs. 5 and 10, para. 0062-0065 and 0111) having a plurality of secure element representations (the complete user account and credit card information that is associated with various financial institutions and stored in each device as well as in the user's/buyer's financial institution portion of the repository that inherently contains a plurality of stored users' account information; see pgs. 0-10, para. 0102 and 0111) wherein the mobile device is [inherently] paired with one of the secure element representations in the repository (in order to identify the proper accounts associated with a specified user that can be used for electronic transactions; see pgs. 9-10, para. 0102 and 0111); sending through a first communication channel a POS command communication from the point-of-sale terminal to the mobile device requesting the digital credential data (see figs. 4-5, 7 and 9-10 as well as pgs. 5 and 8-9, para. 0059 and 0100-0101); and sending through the first communication channel a device response communication from the mobile device to the point-of-sale terminal wherein the device response communication comprises at least a portion of the digital credential data (see figs. 5 and 10 as well as pgs. 5 and 10, para. 0065-0067 and 0111-0113; wherein the credential data is interpreted to include portions of a user's financial account information that is necessary to complete the transaction as well as a confirmation signal that is received by the POS device).
But, Rosenberg does not specifically discuss the method comprising: authenticating and validating a mobile device at the repository [the user's/buyer's financial institution].
However, Rosenberg discloses the a step of authenticating and validating at the mobile device (see pgs. 5, 7 and 10; para. 0062-0063, 0084 and 0111).
Yeager discloses a method and system for authorizing and implementing electronic transactions (see the Abstract as well as pg. 1, para. 0003, for example); wherein Yeager teaches the concept of authenticating and validating a mobile device at a repository (server 320 in combination with database 610; see figs. 3 and 6 as well as pg. 3, para. 0031).
It would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the method of Rosenberg comprise the step of authenticating and validating a mobile device at the repository, as shown by Yeager, for the purpose of preventing unauthorized transactions and payments.

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding Claim 12, Rosenberg in view of Yeager disclose all limitations of Claim 11. Rosenberg does not disclose the method further comprising: sending through a second communication channel a device command communication from the mobile device to the repository; and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises at least a portion of the digital credential.
However, Yeager discloses the method further comprising: sending through a second communication channel [the communication connection/link between the device 110/900 and the user's/buyer's financial institution 470; see figs. 4 and 9) a device command communication from the mobile device to the repository (in order to initiate transfer of funds from a user's account to a seller's account; see pgs. 5, 10, para. 0062-0064 and 0111, for example; wherein the command is sent to the portion of the repository that comprises the smartlink 100 of device 110/the portion of device 900 that securely contains the user's financial account information); and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises at least a portion of the digital credential data (portions of the user's financial account information that is needed in order to complete the transaction and purchase; see figs. 5 and 7 as well as pgs. 5, para. 0064-0067 and 0081-0085).
It would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the method of Rosenberg comprise the step of authenticating and validating a mobile device at the repository, as shown by Yeager, for the purpose of preventing unauthorized transactions and payments.

Regarding Claim 13, Rosenberg in view of Yeager disclose all limitations of Claim 11. Rosenberg further discloses the method further comprising: caching [storing] at least a portion of the digital credential data in the mobile device (see figs. 5 and 7 as well as pgs. 5, 7 and 10, para. 0062-0064, 0081-0084 and 0111), wherein the device response communication comprises the cached portion of the digital credential data (see fig. 7 as well as pg. 7, para. 0084-0085 and 0111).

Regarding Claim 17, Rosenberg in view of Yeager disclose all limitations of Claim 11. Rosenberg further discloses the mobile device being proximate to the point-of-sale terminal (see figs. 4 and 8).

Regarding Claim 18, Rosenberg in view of Yeager disclose all limitations of Claim 11. Rosenberg further discloses the mobile device being remote from the repository (the portion of the repository associated with the user's/buyer's financial institution 470; see figs. 4 and 9).

Regarding Claim 19, Rosenberg in view of Yeager disclose all limitations of Claim 11. Rosenberg further discloses the point-of-sale terminal being remote from the repository (the portion of the repository associated with the user's/buyer's financial institution 470; see figs. 4 and 9).

Regarding Claim 20, Rosenberg in view of Yeager disclose all limitations of Claim 11. Rosenberg further discloses the mobile device being remote from the repository (the portion of the repository associated with the user's/buyer's financial institution 470; see figs. 4 and 9) and the point-of-sale terminal is remote from the repository (the portion of the repository associated with the user's/buyer's financial institution 470; see figs. 4 and 9) and the digital credential data comprises Track Data (data in the form of account numbers and information that is associated with a user's financial accounts; see pgs. 7 and 10, para. 0084 and 0111).

Regarding Claim 36, Rosenberg discloses a system (see figs. 4 and 9) for acquiring digital credential data (pgs. 5-6 and 8-10, para. 0056-0072, 0074, 0097-0103 and 0105-0113; wherein credential data is interpreted to be a transaction confirmation signal in combination with the necessary portions of the complete user account and credit card information that is associated with the financial institutions of a user and used to complete a transaction; see pg. 10, para. 0111-0113, for example) comprising: a mobile device (device 110/900; see figs. 4 and 9, for example); a first communication channel (a communication link between the POS device 420,410/520,525 via an NFC link; see figs. 4 and 9 as well as pgs. 2-3 and 5, para. 0036 and 0064-0065, for example); a point-of-sale terminal (POS device 420,410/520,525 via an NFC link; see figs. 4 and 9) configured to generate a request for an acquisition of the digital credential data from the mobile device over the first communication channel as a POS command communication (see figs. 4-5, 7 and 9-10 as well as pgs. 5 and 8-9, para. 0059 and 0100-0101), and configured for receiving the digital credential data from the mobile device over the first communication channel as a device response communication (see figs. 5 and 10 as well as pgs. 5 and 10, para. 0065-0067 and 0111-0113; wherein the credential data is interpreted to include portions of a user's financial account information that is necessary to complete the transaction as well as a confirmation signal that is received by the POS device); and a repository (an inherent memory associated with the smartlink device 100 that is connected to device 110/an inherent memory associated with device 900 that has securely stored user financial account information in combination with a buyer's/user's financial institution 470; see figs. 4 and 9 as well as pgs. 5 and 10, para. 0062-0065 and 0111) that is remote from the point-of-sale terminal (see figs. 4 and 9; wherein the portion of the repository corresponding to the user's/buyer's financial institution 470 is disclosed/depicted as being remote from the POS device/terminal), the repository having a plurality of secure element representations (the complete user account and credit card information that is associated with various financial institutions and stored in each device as well as in the user's/buyer's financial institution portion of the repository that inherently contains a plurality of stored users' account information; see pgs. 9-10, para. 0102 and 0111) and [inherently] pair the mobile device with a specific secure element representation (in order to identify the proper accounts associated with a specified user that can be used for electronic transactions; see pgs. 9-10, para. 0102 and 0111); and wherein the mobile device is remote from the repository (see figs. 4 and 9; wherein the portion of the repository corresponding to the user's/buyer's financial institution 470 is disclosed/depicted as being remote from the POS device/terminal) and is configured to a) authenticate at the mobile device (see pgs. 5, 7 and 10; para. 0062-0063, 0084 and 0111); b) receive the POS command communication over the first communication channel (see figs. 4-5, 7 and 9-10 as well as pgs. 5 and 8-9, para. 0059 and 0100-0101), and c) send at least a portion of the digital credential data to the point-of-sale terminal as the device response communication over the first communication channel (see figs. 5 and 10 as well as pgs. 5 and 10, para. 0065-0067 and 0111-0113; wherein the credential data is interpreted to include portions of a user's financial account information that is necessary to complete the transaction as well as a confirmation signal that is received by the POS device).
But, Rosenberg does not specifically discuss the method comprising the following: the repository [the portion of the repository that corresponds to a user's/buyer's financial institution 470 of figs. 4 and 9] being configured to validate the mobile device; and the mobile device being configured to authenticate to the repository.

[cont. on next supplemental box]

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

[Regarding claim 36 -- cont.]
However, Yeager discloses a method and system for authorizing and implementing electronic transactions (see the Abstract as well as pg. 1, para. 0003, for example); wherein Yeager teaches the concept of authenticating and validating a mobile device at a repository (server 320 in combination with database 610; see figs. 3 and 6 as well as pg. 3, para. 0031).
It would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the system of Rosenberg comprise the repository being configured to validate the mobile device; and the mobile device being configured to authenticate to the repository, as shown by Yeager, for the purpose of preventing unauthorized transactions and payments.

Regarding Claim 37, Rosenberg in view of Yeager disclose all limitations of claim 36. Rosenberg further discloses the system further comprising a second communication channel (the communication connection/link between the device 110/900 and the user's/buyer's financial institution 470; see figs. 4 and 9) and wherein: the repository is configured to receive a request for the digital credential data from the mobile device using the second communication channel (in order to initiate transfer of funds from a user's account to a seller's account; see pgs. 5, 10, para. 0062-0064 and 0111, for example; wherein the command is sent to the portion of the repository that comprises the smartlink 100 of device 110/the portion of device 900 that securely contains the user's financial account information) and to send a response with at least a portion of the digital credential data to the mobile device using the second communication channel (portions of the user's financial account information that is needed in order to complete the transaction and purchase; see figs. 5 and 7 as well as pgs. 5, para. 0064-0067 and 0081-0085).

Regarding Claim 38, Rosenberg in view of Yeager disclose all limitations of claim 36. Rosenberg further inherently discloses the mobile device comprises a [inherent] cache memory configured to store at least a portion of the digital credential data as cached data (see figs. 5 and 7 as well as pgs. 5, 7 and 10, para. 0062-0064, 0061-0084 and 0111) and the mobile device is configured to send the cached data as at least a portion of the device response communication (see fig. 7 as well as pg. 7, para. 0084-0085 and 0111).

Regarding Claim 40, Rosenberg in view of Yeager disclose all limitations of claim 36. Rosenberg further discloses the mobile device being proximate to the point-of-sale terminal (see figs. 4 and 8).

Regarding Claim 41, Rosenberg in view of Yeager disclose all limitations of claim 36. Rosenberg further discloses the mobile device being remote from the repository (the portion of the repository associated with the user's/buyer's financial institution 470; see figs. 4 and 9).

Regarding Claim 42, Rosenberg in view of Yeager disclose all limitations of claim 36. Rosenberg further discloses the point-of-sale terminal being remote from the repository (the portion of the repository associated with the user's/buyer's financial institution 470; see figs. 4 and 9).

Regarding Claim 43, Rosenberg in view of Yeager disclose all limitations of claim 36. Rosenberg further discloses the mobile device being remote from the repository (the portion of the repository associated with the user's/buyer's financial institution 470; see figs. 4 and 9) and the point-of-sale terminal is remote from the repository (the portion of the repository associated with the user's/buyer's financial institution 470; see figs. 4 and 9) and the digital credential data comprises Track Data (data in the form of account numbers and information that is associated with a user's financial accounts; see pgs. 7 and 10, para. 0084 and 0111)..

Regarding Claim 44, Rosenberg in view of Yeager disclose all limitations of claim 36. Rosenberg further discloses the first communication channel comprises a near-field communication channel (see pgs. 2-3 and 5, para. 0036 and 0064-0065).

Regarding Claim 55, Rosenberg discloses a method (see figs. 4-5, 7 and 9-10 as well as pgs. 5-6 and 8-10, para. 0056-0072, 0074, 0097-0103 and 0105-0113) for acquiring digital credential data (a transaction confirmation signal in combination with the necessary portions of the complete user account and credit card information that is associated with the financial institutions of a user and used to complete a transaction; see pg. 10, para. 0111-0113, for example) by a point-of-sale terminal (POS device 420/520; see figs. 4 and 9) comprising: a mobile device (device 110/900 of figs. 4 and 9) in combination/connection with a repository (an inherent memory associated with the smartlink device 100 that is connected to device 110/an inherent memory associated with device 900 that has securely stored user financial account information in combination with a buyer's/user's financial institution 470; see figs. 4 and 9 as well as pgs. 5 and 10, para. 0062-0065 and 0111) having a plurality of secure element representations (the complete user account and credit card information that is associated with various financial institutions and stored in each device as well as in the user's/buyer's financial institution portion of the repository that inherently contains a plurality of stored users' account information; see pgs. 9-10, para. 0102 and 0111) wherein the mobile device is [inherently] paired with one of the secure element representations in the repository (in order to identify the proper accounts associated with a specified user that can be used for electronic transactions; see pgs. 9-10, para. 0102 and 0111); sending through a first communication channel a POS command communication from the point-of-sale terminal to the mobile device requesting the digital credential data (see figs. 4-5, 7 and 9-10 as well as pgs. 5 and 8-9, para. 0059 and 0100-0101); and sending through the first communication channel a device response communication from the mobile device to the point-of-sale terminal wherein the device response communication comprises at least a portion of the digital credential data (see figs. 5 and 10 as well as pgs. 5 and 10, para. 0065-0067 and 0111-0113; wherein the credential data is interpreted to include portions of a user's financial account information that is necessary to complete the transaction as well as a confirmation signal that is received by the POS device).
But, Rosenberg does not specifically discuss the method comprising: authenticating and validating a stationary device at the repository [the user's/buyer's financial institution].

[cont. on next supplemental box]

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

[Regarding claim 55 - cont.]
However, Rosenberg discloses the a step of authenticating and validating at the mobile device (see pgs. 5, 7 and 10; para. 0062-0063, 0084 and 0111)
Yeager discloses a method and system for authorizing and implementing electronic transactions (see the Abstract as well as pg. 1, para. 0003, for example); wherein Yeager teaches the concept of authenticating and validating a mobile device at a repository (server 320 in combination with database 610; see figs. 3 and 6 as well as pgs. 3-4, para. 0031 and 0035; wherein the stationary device is interpreted to be a personal computer).
It would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the method of Rosenberg comprise the step of authenticating and validating a stationary device at the repository, as shown by Yeager, for the purpose of preventing unauthorized transactions and payments.

Regarding Claim 56, Rosenberg in view of Yeager disclose all limitations of claim 55. Rosenberg further discloses a second communication channel (the communication connection/link between the device 110/900 and the user's/buyer's financial institution 470; see figs. 4 and 9) and wherein: the repository is configured to receive a request for the digital credential data from the stationary device using the second communication channel (in order to initiate transfer of funds from a user's account to a seller's account; see pgs. 5, 10, para. 0062-0064 and 0111, for example; wherein the command is sent to the portion of the repository that comprises the smartlink 100 of device 110/the portion of device 900 that securely contains the user's financial account information) and to send a response with at least a portion of the digital credential data to the stationary device using the second communication channel (portions of the user's financial account information that is needed in order to complete the transaction and purchase; see figs. 5 and 7 as well as pgs. 5, para. 0064-0067 and 0081-0085).

Claims 14-15, 21, 24-26, 28-34 & 47-52 lack an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Yeager and further in view of Bishop.

Regarding Claims 14 & 24, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose the POS command communication comprises a plurality of command communications conforming to IS07816-4 protocol, the device response communication comprises the plurality of the response communications conforming to IS07816-4 protocol, and the method further comprises: interpreting in the mobile device the POS command communications wherein, for at least one POS command communication the mobile device returns to the point-of-sale terminal as a portion of the device response communication a cached IS07816-4 protocol response communication from a cache located in the mobile device.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses the POS command communication comprises a plurality of command communications conforming to IS07816-4 protocol (ISO7816-4 is used since ISO7816 protocol is disclosed and the protocol is used to control communications between devices; Par. 0043), the device response communication comprises the plurality of the response communications conforming to IS07816-4 protocol, and the method further comprises: interpreting in the mobile device the POS command communications wherein, for at least one POS command communication the mobile device returns to the point-of-sale terminal as a portion of the device response communication a cached IS07816-4 protocol response communication from a cache located in the mobile device (the transaction device 102 is the mobile device, and the command communications originate from the database but are moved to cache upon execution by t he device's processor; Par. 0043).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's feature in to modified Rosenberg's system. The motivation would have been to allow for the use of an internationally accepted commercial communications standard (Bishop, Par. 0039).

Regarding Claim 15, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose sending through a second communication channel a device command communication from the mobile device to the repository; and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises the at least a portion of the digital credential data.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses sending through a second communication channel a device command communication from the mobile device to the repository (the Internet is the second communication channel; Par. 0024); and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises the at least a portion of the digital credential data (the response can also be sent through the Internet; Par. 0024).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's feature in to modified Rosenberg's system. The motivation would have been to take advantage of the Internet to complete commercial transactions (Bishop, Par. 0024).

Regarding Claim 21, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose the first communication channel comprises a near-field communication channel.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses the first communication channel comprises a near-field communication channel (the RFID system includes a near-field communication channel; Par. 0039).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's feature in to modified Rosenberg's system. The motivation would have been to facilitate point of sale transactions (Bishop, Par. 0006).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding Claims 25 & 29, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose sending through a second communication channel from the mobile device to the repository a device command communication conforming to any part of ISO 7816 part 1, 2, 3, or 4; and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises the at least a portion of the digital credential data.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses sending through a second communication channel from the mobile device to the repository (the Internet is the second communication channel; Par. 0024) a device command communication conforming to any part of ISO 7816 part 1, 2, 3, or 4 (ISO 7816 part 4 is used, since communications is controlled; Par. 0043); and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises the at least a portion of the digital credential data (the response is sent through the Internet; Par. 0024).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's feature in to modified Rosenberg's system. The motivation would have been to facilitate point of sale transactions (Bishop, Par. 0006).

Regarding Claim 26, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose the mobile device is remote from the repository and the method further comprises: sending through a second communication channel using TCP/UDP/IP protocol from the mobile device to the repository a device command communication; and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises the at least a portion of the digital credential data.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses the mobile device is remote from the repository and the method further comprises: sending through a second communication channel using TCP/UDP/IP protocol from the mobile device to the repository a device command communication (the Internet is the second communiation channel; Par. 0024); and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises the at least a portion of the digital credential data (the response can also travel through the internet; Par. 0024).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's feature in to modified Rosenberg's system. The motivation would have been to facilitate point of sale transactions (Bishop, Par. 0006).

Regarding Claim 28, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose the POS command communication conforms to IS07816-4 protocol, the device response communication conforms to IS07816-4 protocol and the method further comprises: sending through a second communication channel from the mobile device to the repository a device command communication that conforms to IS07816-4 protocol; and sending through the second communication channel a repository response communication from the repository to the mobile device a repository response communication that conforms to IS07816-4 protocol.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses the POS command communication conforms to IS07816-4 protocol, the device response communication conforms to IS07816-4 protocol (ISO7816 protocol is used for communications between the devices, thus the ISO7816-4 is used; Par. 0043) and the method further comprises: sending through a second communication channel from the mobile device to the repository a device command communication that conforms to IS07816-4 protocol (the Internet is the second communication channel; Par. 0024); and sending through the second communication channel a repository response communication from the repository to the mobile device a repository response communication that conforms to IS07816-4 protocol (response conforms to ISO7816-4 since the response is a communication between devices; Par. 0043).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's feature in to modified Rosenberg's system. The motivation would have been to facilitate point of sale transactions (Bishop, Par. 0006).

Regarding claim 30, Rosenberg in view of Yeager disclose all limitations of claim 11, but lack explicitly teaching the method further comprises converting inside the mobile device at least a portion of the credential data into Track Data.
In the field of RF Transaction authentication, Bishop teaches the method further comprises converting inside the mobile device at least a portion of the credential data into Track Data (para [0031], [0036]-[0037] forwarded and encoding account related information in a portion of a data stream in track format).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of modified Rosenberg to include the method of communicating account related data of Bishop in order to secure customer related information (Bishop, para [0010]).

Regarding claim 31, Rosenberg in view of Yeager disclose all limitations of claim 11, but lack explicitly teaching the mobile device is remote from the point-of-safe terminal, and wherein the method further comprises: converting inside the mobile device at least a portion of the credential data into Track Data; and providing the Track Data formatted as digital credential data according to IS07813 as at least a portion of the device response communication.
In the field of RF Transaction authentication, Bishop teaches the mobile device is remote from the point-of-sale terminal (para [0027], input device may be a cellular phone interfacing with.. para [0028] POS device and host network interfaces to a remote network for authorization), and wherein the method further comprises: converting inside the mobile device at least a portion of the credential data into Track Data (para [0036]-[0037] forwarding and encoding account related information in a portion of a data stream in track format); and providing the Track Data formatted as digital credential data according to IS07813 as at least a portion of the device response communication (para [0031] account information is stored as track 1 and track 2 data as defined in ISO/IEC 7813; para [0036]-[0037] authentication data may be forwarded or encoded in all or a portion of a data stream, representing data encoded in track 2 or track 3 format; para [0031], wherein the stream of data may look like "0000 0000 00000000" which is a stream of keys).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of Rosenberg in view of Yeager to include the method of communicating account related data of Bishop in order to secure customer related information (Bishop, para [0010]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding claim 32, Rosenberg in view of Yeager disclose all limitations of claim 11, but lack explicitly teaching the mobile device is remote from the repository, the point-of-sale terminal is remote from the repository, the repository comprises a database of static Track Data, and the method further comprises: constructing in the repository cache data or at least a portion of a repository response communication using the database of static Track Data.
In the field of RF Transaction authentication, Bishop teaches the mobile device is remote from the repository, the point-of-sale terminal is remote from the repository (para [0027], input device may be a cellular phone interfacing with.. para [0028] POS device and host network interfaces to a remote network for authorization), the repository comprises a database of static Track Data (para [0032],[0041], host network utilizes a database containing account data; para [0031], wherein account data can be in Track 1 or Track 2 format), and the method further comprises: constructing in the repository cache data or at least a portion of a repository response communication using the database of static Track Data (para [0032] database may be configured to store account information; para [0031] wherein account information is stored as Track 1 or Track 2 data).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of Rosenberg in view of Yeager to include the method of communicating account related data of Bishop in order to secure customer related information (Bishop, para [0010]).

Regarding claim 33, Rosenberg in view of Yeager disclose all limitations of claim 11, but lack explicitly teaching the first communication channel comprises an NFC communication channel; the POS command communication comprises a select file command conforming to IS07816-4 protocol using a VISA AID starting with A000000003; and the device response communication comprises digital credential data that does not have a beginning PAN digit, as defined in IS07813, equal to a numeral "4".
In the field of RF Transaction authentication, Bishop teaches the first communication channel comprises an NFC communication channel (para [0027]-[0028] user communicates with network over a communications protocol; para [0032] wherein the communications protocol may be RFID [RFID is a type of NFC communications protocol]); the POS command communication comprises a select file command conforming to IS07816-4 protocol using a VISA AID starting with A000000003 (para [0043] storing transaction device information according to ISO 7816 file structure standards; para [0050] wherein such values can be in numeric units such as "0,1,2,3,..n," or similar); and the device response communication comprises digital credential data that does not have a beginning PAN digit, as defined in IS07813, equal to a numeral "4" (para [0033] device uses PIN but not PAN; para [0031] as defined by ISO/IEC 7813).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of Rosenberg in view of Yeager to include the method of communicating account related data of Bishop in order to secure customer related information (Bishop, para [0010]).

Regarding claim 34, Rosenberg in view of Yeager disclose all limitations of claim 11, but lack explicitly teaching the first communication channel comprises an NFC communication channel; the POS command communication comprises a select file command conforming to IS07816-4 protocol using a VISA AID starting with A000000003; the device response communication comprises digital credential data that does not have a beginning PAN digit, as defined in IS07813, equal to a numeral "4"; and the method further comprises formatting the digital credential data in the point-of-sale terminal into a digital credential that is identical to a static magnetic stripe card that conforms to IS07813.
In the field of RF Transaction authentication, Bishop teaches the first communication channel comprises an NFC communication channel (para [0027]-[0028] user communicates with network over a communications protocol; para [0032] wherein the communications protocol may be RFID [RFID is a type of NFC communications protocol]); the POS command communication comprises a select file command conforming to IS07816-4 protocol using a VISA AID starting with A000000003 (para [0043] storing transaction device information according to ISO 7816 file structure standards; para [0050] wherein such values can be in numeric units such as "0,1,2,3,..n," or similar); the device response communication comprises digital credential data that does not have a beginning PAN digit, as defined in IS07813, equal to a numeral "4"; and the method further comprises formatting the digital credential data in the point-of-sale terminal into a digital credential that is identical to a static magnetic stripe card that conforms to IS07813 (para [0033] device uses PIN but not PAN; para [0031] as defined by ISO/IEC 7813; para [0035]-[0036] account data is communicated by magnetic stripe format conforming to the aforementioned ISO standards).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of Rosenberg in view of Yeager to include the method of communicating account related data of Bishop in order to secure customer related information (Bishop, para [0010]).

Regarding claim 47, Rosenberg in view of Yeager disclose all limitations of claim 36, but lack explicitly teaching the repository comprises a digital database of a plurality of mobile device identifications and at least one secure element representation identifier associated with each mobile device and the repository is configured to validate the mobile device using the digital database.
In the field of RF Transaction authentication, Bishop teaches the repository comprises a digital database of a plurality of mobile device identifications and at least one secure element representation identifier associated with each mobile device and the repository is configured to validate the mobile device using the digital database (para [0031]-[0032] an account identifier may be used to validate the account using the database).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of modified Rosenberg to include the method of communicating account related data of Bishop in order to secure customer related information (Bishop, para [0010]).

Regarding claim 48, Rosenberg in view of Yeager disclose all limitations of claim 36, but lack explicitly teaching the mobile device comprises non-persistent memory for caching a cached portion of the digital credential data and the mobile device is configured to provide the cached portion to the point-of-sale terminal through the first communication channel.
In the field of RF Transaction authentication, Bishop teaches the mobile device comprises non-persistent memory for caching a cached portion of the digital credential data and the mobile device is configured to provide the cached portion to the point-of-sale terminal through the first communication channel (para [0023] information can be stored in memory elements such as look up tables and data structures [which are commonly non-persistent memory elements]; para [0036] wherein data stored in such memory elements may be account related information).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of modified Rosenberg to include the method of communicating account related data of Bishop in order to secure customer related information (Bishop, para [0010]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding claim 49, Rosenberg in view of Yeager disclose all limitations of claim 36, but lack explicitly teaching there is a plurality of command communications and a plurality of response communications over the first communication channel.
In the field of RF Transaction authentication, Bishop teaches there is a plurality of command communications and a plurality of response communications over the first communication channel (para [0027]-[0028] user communicates with network over a communications protocol; para [0032] wherein the communications protocol may be RFID [RFID is a type of NFC communications protocol]).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of Rosenberg in view of Yeager to include the method of communicating account related data of Bishop in order to secure customer related information (Bishop, para [0010]).

Regarding Claim 50, Rosenberg in view of Yeager disclose all limitations of claim 36, but do not disclose the request for the acquisition of the digital credential data and the device response communication comprise 7816-4 data.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses the request for the acquisition of the digital credential data and the device response communication comprise 7816-4 data (the communications between devices conform to the ISO 7816-4 protocol and thus comprise 7816-4 data; Par. 0043).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's feature in to modified Rosenberg's system. The motivation would have been to expedite point of sale transactions (Bishop, Par. 0006).

Regarding Claim 51, Rosenberg in view of Yeager disclose all limitations of claim 36, but do not disclose a second communication channel wherein, the repository is configured to receive a request for the digital credential data from the mobile device using the second communication channel and to send a response with at least a portion of the digital credential data to the mobile device using the second communication channel; and wherein the device command communication and the repository response communication comprise 7816-4 data.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses a second communication channel wherein, the repository is configured to receive a request for the digital credential data from the mobile device using the second communication channel (the Internet is the second communication channel; Par. 0024) and to send a response with at least a portion of the digital credential data to the mobile device using the second communication channel; and wherein the device command communication and the repository response communication comprise 7816-4 data (ISO7816 protocol is disclosed for controlling communications between the devices, thus ISO7816-4 is used; Par. 0043).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's feature in to modified Rosenberg's system. The motivation would have been to expedite point of sale transactions (Bishop, Par. 0006).

Regarding Claim 52, Rosenberg in view of Yeager disclose all limitations of claim 36, but do not disclose a second communication channel and wherein: the repository is configured to receive a request for the digital credential data from the mobile device using the second communication channel and to send a response with at least a portion of the digital credential data to the mobile device using the second communication channel; and wherein the first communication channel and the second communication channel comprise TCP/UDP/IP communication channels.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses a second communication channel and wherein: the repository is configured to receive a request for the digital credential data from the mobile device using the second communication channel and to send a response with at least a portion of the digital credential data to the mobile device using the second communication channel (the Internet is the second communication channel; Par. 0043); and wherein the first communication channel and the second communication channel comprise TCP/UDP/IP communication channels (TCP/UDP/IP is used over the Internet; Par. 0027).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's feature in to modified Rosenberg's system. The motivation would have been to expedite point of sale transactions (Bishop, Par. 0006).

Claims 16, 22, 39 & 45 lack an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Yeager and further in view of Hohle.

Regarding Claim 16, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose the repository uses ISO 7816 to extract at least a portion of the digital credential data from the paired secure element representation.
However, Hohle is in the field of facilitating commercial transactions over a network (Col. 1, lines 7-11) and discloses the repository uses ISO 7816 to extract at least a portion of the digital credential data from the paired secure element representation (card object database 116 is the repository; Col. 4, lines 13-24).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Hohle's feature in to modified Rosenberg's system. The motivation would have been to provide for the use of an internationally accepted standard (Hohle, Col. 4, lines 13-24).

Regarding Claim 22, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose the first communication channel comprises a TCP/UDP/IP communication channel.
However, Hohle is in the field of facilitating commercial transactions over a network (Col. 1, lines 7-11) and discloses the first communication channel comprises a TCP/UDP/IP communication channel (the TCP/IP connection is the communication channel; Col. 8, lines 51-63).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Hohle's feature in to modified Rosenberg's system. The motivation would have been to allow for usage of the Internet to facilitate commercial transactions (Hohle, Col. 8, lines 51-63).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding Claim 39, Rosenberg in view of Yeager disclose all limitations of claim 36, but does not disclose the repository uses IS07816 to extract the at least a portion of the digital credential data from the paired secure element representation.
However, Hohle is in the field of facilitating commercial transactions over a network (Col. 1, lines 7-11) and discloses a repository that uses IS07816 to extract at least a portion of the digital credential data from a paired secure element representation (card object database 116 is the repository; Col. 4, lines 13-24).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Hohle's feature in to modified Rosenberg's system. The motivation would have been to provide for the use of an internationally accepted standard (Hohle, Col. 4, lines 13-24).

Regarding Claim 45, Rosenberg in view of Yeager disclose all limitations of claim 36, but do not disclose the mobile device is remote from the point-of-sale terminal and the first communication channel comprises a TCP/UDP/IP communication channel.
However, Hohle is in the field of facilitating commercial transactions over a network (Col. 1, lines 7-11) and discloses the mobile device is remote from the point-of-sale terminal the first communication channel comprises a TCP/UDP/IP communication channel (the TCP/IP connection is the communication channel; Col. 8, lines 51-63).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Hohle's feature in to modified Rosenberg's system. The motivation would have been to allow for usage of the Internet to facilitate commercial transactions (Hohle, Col. 8, lines 51-63).

Claim 23 lacks an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Yeager and further in view of Tang.

Regarding Claim 23, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose the authenticating step comprises matching a gesture signal with a valid gesture signal.
However, Tang is in the field of detecting and eliminating fraud in a transaction (Abs.) and discloses the authenticating step comprises matching a gesture signal with a valid gesture signal (the secret gesture, is the gesture signal; Par. 0029).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Tang's feature in to modified Rosenberg's system. The motivation would have been to provide security for the user by preventing fraud (Tang, Par. 0029).

Claim 27 lacks an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Yeager and further in view of Garcia Ruano.

Regarding Claim 27, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose the mobile device is remote from the repository and the method further comprises: sending through a second communication channel using a Secure Socket Layer and TCP/UDP/IP protocol from the mobile device to the repository a device command communication; and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises the at least a portion of the digital credential data.
However, Garcia Ruano is in the field of using a mobile phone as a payment device (Abs.) and discloses the mobile device is remote from the repository and the method further comprises: sending through a second communication channel using a Secure Socket Layer and TCP/UDP/IP protocol from the mobile device to the repository a device command communication (the Internet is the second channel, and a secure connection using TCP/IP protocol is used; Par. 0155); and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises the at least a portion of the digital credential data (the response is sent from the operations processor; Par. 0066).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Garcia Ruano's feature in to modified Rosenberg's system. The motivation would have been to allow for secure transactions over the Internet (Garcia Ruano, Par. 0155).

Claim 35 lacks an inventive step under PCT Article 33(3) as being obvious over Bishop in view of Pond.

Regarding claim 35, Bishop teaches a system for acquiring digital credential data using a mobile device comprising: a point-of-sale terminal having a NFC interface using IS07816-4 protocol to transmit a request for the digital credential data and to receive digital credential data (para [0043]-[0045] RFID transaction device [wherein RFID is an NFC interface] is used to store and communicate account and transaction-related information, and conforms to ISO7816 file structure standards); and a mobile device having a NFC interface using IS07816-4 protocol configured to (para [0027] input device being a cellular phone, para [0043] conforming to the ISO7816 standards) receive the request from the point-of-sale terminal for an acquisition of the digital credential data, interpret the request from the point-of-sale within an operating system of the mobile device and within an application running in that operating system (Fig. 2, items 210-218, send and receiving requests [pertaining to transactions] between POS and Acquirer; para [0043] wherein one of the communicating devices may be a cellular phone), but does not disclose sending the digital credential data to the point-of-sale terminal using IS08916-4 protocol generated from an application running in an operating system in the mobile device.
However, Pond is in the field mobile device payment methods, and Pond teaches sending the digital credential data to the point-of-sale terminal using IS08916-4 protocol generated from an application running in an operating system in the mobile device (col. 7, ln. 15-40, data can be communicated according to ISP 7816 standards).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the RF transaction system of Bishop to include the use of the ISO8916 protocol of Pond in order to use a structure that is based on a standard (Pond, col. 7, ln. 29-33).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Claim 46 lacks an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Yeager and further in view of Pond.

Regarding claim 46, Rosenberg in view of Yeager disclose all limitations of claim 36, but lack explicitly teaching the mobile device is configured for generating a gesture signal and to authenticate to the repository by matching the gesture signal with a valid gesture signal. In the field mobile device payment methods, Pond teaches the mobile device is configured for generating a gesture signal and to authenticate to the repository by matching the gesture signal with a valid gesture signal (col. 12, ln. 1-13, RFID transponder interrogator window may also be comprised of an array of interrogators and other sensors to allow for gestures to be used as input into the Commerce system. If a certain hand gesture, for example is valid, then the commerce system would authorize a transaction).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of modified Rosenberg to include the use of specific gestures of Pond in order to provide more security for the user (Pond, col. 12, ln. 10-11).

Claims 53-54 lack novelty under PCT Article 33(2) as being anticipated by Bishop.

Regarding claim 53, Bishop teaches a repository for secure element representations (para [0044] database 116 may be in communication with a transaction device for communicating account related information) comprising: at least one secure element reader (para [0045] RFID transaction device 102 and RFID reader 104); a plurality of secure element representations disposed proximate to the secure element reader (para [0045] RFID transaction device 102 communicates with RFID reader 104; wherein each of these devices may be based on elements as per para [0023]); a server disposed proximate to the secure element reader, the server having a multitasking processor to communicate with the plurality of secure element representations through the secure element reader and conduct a plurality of command/response time-wise overlapping sessions with the plurality of secure element representations (para [0044) the RFID device and reader communicate secure account and transaction related information according to interrogation signaling methods [wherein RFID is a type of NFC protocol]); and an internet connection to the server wherein each of the secure element representations is addressable over the internet (para [0024]-[0025] transaction methods performed using internet).

Regarding claim 54, Bishop discloses all limitations of claim 53 and further discloses the plurality of secure element representations is selected from the group consisting of hardware representations, virtual hardware representations, and a combination thereof (para [0023] the elements representing the data can be any number of hardware and/or software components configured to perform to specified functions).

Claims 1-56 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 67979.W2	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US2012/053129	International filing date *(day/month/year)* 30 August 2012	(Earliest) Priority Date *(day/month/year)* 30 August 2011
Applicant YEAGER, C.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 9 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of:

☒ the international application in the language in which it was filed.

☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).

c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. ☐ **Certain claims were found unsearchable** (see Box No. II).

3. ☐ **Unity of invention is lacking** (see Box No. III).

4. With regard to the **title**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,

a. the figure of the **drawings** to be published with the abstract is Figure No. 1

☒ as suggested by the applicant.

☐ as selected by this Authority, because the applicant failed to suggest a figure.

☐ as selected by this Authority, because this figure better characterizes the invention.

b. ☐ none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/053129

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 20/00 (2012.01)
USPC - 705/64
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - G06Q 20/00, H04L 09/00, G06K 05/00 (2012.01)
USPC - 705/64-69, 72-78, 380/42-43, 235/380

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
MicroPatent, Google Patents, Google Scholar

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y -- A	US 2007/0075133 A1 (YEAGER) 05 April 2007 (05.04.2007) entire document	1 --- 2, 27 ----- 28
Y --- A	US 2010/0185545 A1 (ROYYURU et al) 22 July 2010 (22.07.2010) entire document	3-7, 12-14, 17-18, 24-27 ---- 28
Y	US 2009/0006262 A1 (BROWN et al) 01 January 2009 (01.01.2009) entire document	3, 7, 12-14, 17-18, 24-27
Y	US 2009/0124234 A1 (FISHER et al) 14 May 2009 (14.05.2009) entire document	12-14, 18
Y	US 2006/0022033 A1 (SMETS et al) 02 February 2006 (02.02.2006) entire document	2, 7, 17
Y	US 2010/0207742 A1 (BUHOT et al) 19 August 2010 (19.08.2010) entire document	25
A	US 2007/0278291 A1 (RANS et al) 06 December 2007 (06.12.2007) entire document	1-29
A	US 2011/0140841 A1 (BONA et al) 16 June 2011 (16.06.2011) entire document	1-29
A	US 2011/0112918 A1 (MESTRE et al) 12 May 2011 (12.05.2011) entire document	1-29
A	US 2008/0219444 A1 (BENTEO et al) 11 September 2008 (11.09.2008) entire document	1-29
A	US 2007/0266131 A1 (MAZUR et al) 15 November 2007 (15.11.2007) entire document	1-29

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 October 2012	16 NOV 2012
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: JAMES PALMER
LUEDEKA NEELY GROUP, P.C.
P.O. BOX 1871
KNOXVILLE, TN 37901-1871

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	16 NOV 2012
Applicant's or agent's file reference 67979.W2	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2012/053129	30 August 2012	30 August 2011

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - G06Q 20/00 (2012.01)
USPC - 705/64

Applicant YEAGER, C.

1. This opinion contains indications relating to the following items:

- [x] Box No. I Basis of the opinion
- [ ] Box No. II Priority
- [ ] Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- [ ] Box No. IV Lack of unity of invention
- [x] Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- [ ] Box No. VI Certain documents cited
- [ ] Box No. VII Certain defects in the international application
- [ ] Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	24 October 2012	Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (July 2011)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

   ☐ on paper

   ☐ in electronic form

   b. (time)

   ☐ in the international application as filed

   ☐ together with the international application in electronic form

   ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	2-29	YES
	Claims	1	NO
Inventive step (IS)	Claims	8-11, 15-16, 19-23, 28-29	YES
	Claims	1-7, 12-14, 17-18, 24-27	NO
Industrial applicability (IA)	Claims	1-29	YES
	Claims	None	NO

2. Citations and explanations:

Claim 1 lacks novelty under PCT Article 33(2) as being anticipated by Yeager (US 2007/0075133 A1).

Regarding claim 1, Yeager discloses a method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction (method, system and computer-readable medium for radio frequency identification device, title; the adapter is connected to a host device like a mobile phone to construct a mobile device capable of financial transactions, Fig. 3 and [0027]-[0029], in which the mobile device communicates with a terminal such as the Mastercard PayPass system, Fig. 5 and [0030]) comprising:
using a remote permanent cryptographic key to calculate an expected cryptogram that is expected to comprise at least a portion of the digital credential data (a secret key on a remote server, Fig. 6 and [0031]-[0032], which is a remote permanent cryptographic key, is used to calculate an expected cryptogram that comprises, and hence encrypts, digital credential data such as credit card information, [0022]), wherein the remote permanent cryptographic key is persistently stored at a remote source that is remote from the mobile device (the secret key is stored in a remote location that is remote from the mobile device/host, Fig. 6 and [0031]-[0032]) and wherein the mobile device does not access a duplicate local permanent cryptographic key persistently stored locally to the mobile device (the mobile device/host also shares the secret key, Fig. 6 and [0031]-[0032], and the mobile device/host does not access the secret key; only the server and the adapter have access to the secret key, because they're the only two entities that know the key, [0031]-[0032]);performing an interrogation between the point-of-sale terminal and the mobile device (the adapter is connected to a host device like a mobile phone to construct a mobile device capable of financial transactions, Fig. 3 and [0027]-[0029], in which the mobile device communicates with a terminal such as the Mastercard PayPass system, Fig. 5 and [0030]) comprising: sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device requesting the digital credential data (the digital credential data is credit card information, [0022], and is requested by the terminal to the mobile device in order to facilitate a transaction, Fig. 9 and [0036]); and
sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal comprising the expected cryptogram as the at least a portion of the digital credential data (credenttial data is sent to a server via the terminal, Fig. 9 and [0036], in which the credential data is encrypted using the encryption key for the purpose of communication between an adapter and server, [0031]-[0032], and hence the encrypted credential data is the expected cryptogram comprising at least a portion of the digital credential data); wherein the financial transaction is authorized (the transaction is determined to be successful or not, hence authorized, and then the user account may then be updated by deducting the transaction amount, Fig. 9 and [0036]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Claim 2 lacks an inventive step under PCT Article 33(3) as being obvious over Yeager (US 2007/0075133 A1) and further in view of Smets et al (US 2006/0022033 A1), hereinafter referred to as Smets.

Regarding claim 2 of claim 1, Yeager further discloses a further step that precedes the performing the interrogation step, the further step comprising:
sending the remote permanent cryptographic key to the mobile device from the remote source (the secret key is chosen by the server sent from a server to the mobile host, [0031]-[0032]); and transiently caching the remote permanent cryptographic key in the mobile device as a cached transient permanent cryptographic key (the server may change the secret key after each transaction, [0031]-[0032], and hence the secret key is actually a temporary session key or cached transient permanent cryptographic key, [0031]-[0032]), sending the expected cryptogram calculated, at least in part, from the cached transient cryptographic key (communications is encrypted with the session key, and hence results in an expected cryptogram, [0031]-[0032]).
Yeager does not adequately disclose:
the step of sending through the communication channel the at least one POS command communication comprises sending unpredictable data; the step of sending through the communication channel the at least one POS command communication comprises sending a request for an expected cryptogram that is expected to be calculated by the mobile device, at least in part, from the unpredictable data; and the step of sending through the communication channel the at least one device response communication from the mobile device to the point-of-sale terminal comprises sending the expected cryptogram calculated, at least in part, from the unpredictable data. However, Smets is also in the field of electronic payment systems (abstract) and further teaches:
the step of sending through the communication channel the at least one POS command communication comprises sending unpredictable data (an unpredicatable number UN, which is unpredictable data, is sent from the POS terminal, Fig. 5 and [0026]); the step of sending through the communication channel the at least one POS command communication comprises sending a request for an expected cryptogram that is expected to be calculated by the mobile device, at least in part, from the unpredictable data (using the unpredictable number, a mobile device, such as the card, calculates a CVC3 number based on a portion of the unpredictable number and transmits the result to the terminal, Fig. 5 and [0026]); and the step of sending through the communication channel the at least one device response communication from the mobile device to the point-of-sale terminal comprises sending the expected cryptogram calculated, at least in part, from the unpredictable data (the resulting cryptogram CVC3 is calculated in part from the unpredictable number and transmitted to the terminal, Fig. 5 and [0026]). Therefore, it would have been obvious to a person having ordinary skill in the art wherein: the step of sending through the communication channel the at least one POS command communication comprises sending unpredictable data; the step of sending through the communication channel the at least one POS command communication comprises sending a request for an expected cryptogram that is expected to be calculated by the mobile device, at least in part, from the unpredictable data; and the step of sending through the communication channel the at least one device response communication from the mobile device to the point-of-sale terminal comprises sending the expected cryptogram calculated, at least in part, from the unpredictable data, as taught by Smets, in which the mobile device may also comprise a mobile card device for an electronic payment system of Royyuru. This combination increase the security of the electronic payment system in the event that an unauthorized person obtains the CVC3 number for a particular transaction (Smets [0010]).

Claims 3-6, 24, 26 lack an inventive step under PCT Article 33(3) as being obvious over Royyuru et al (US 2010/0185545 A1), hereinafter referred to as Royyuru and further in view of Brown et al (US 2009/0006262 A1), hereinafter referred to as Brown.

Regarding claim 3, Royyuru discloses a method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction (dynamic primary account number and unique key per card, title; financial transaction authorization, abstract, Fig. 3) comprising:
performing an interrogation between the point-of-sale terminal and the mobile device (in NFC technology, a mobile device is in communication with a point-of-sale POS terminal, [0022]) comprising: sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device (commands and responses are communicated between a terminal and mobile device in order to perform a financial transaction, [0057]), the at least one POS command communication comprising (a) a request for the digital credential data that is expected to comprise an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data, and, at least in part, from a permanent cryptographic key (transaction requests comprise credit card numbers, which is digital credential data, and is calculated from a unpredictable number, which is unpredictable data, and the message is encrypted with a key, [0049]-[0051]) and (b) the unpredictable data (an unpredictable number UN, which is unpredictable data, is generated by the NFC terminal and transmitted to the device, [0057]); and sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal (commands and responses are communicated between a terminal and mobile device in order to perform a financial transaction, [0057]), the at least one device response communication comprising at least a portion of the digital credential data that comprises an unexpected cryptogram (encrypting the credit card numbers with an unpredictable number will result in a dynamic PAN, which is an unexpected cryptogram, [0049]-[0051]), wherein the financial transaction is authorized (the financial transaction may be authorized or denied, [0050]).
Royyuru may not adequately describe that an unexpected cryptogram is substituted in place of the expected cryptogram. However, Brown is also in the field of financial transactions (abstract) and further teaches cryptogram substitution of one cryptogram for another cryptogram ([0134]-[0141]; Once the data format is known, it is effectively a template, like an invoice sheet, in which there is a location where information like a price of an item is shown. This is similar to substituting one value for another value given that the data is of the same type, like price). Therefore, it would have been obvious to a person having ordinary skill in the art that: an unexpected cryptogram is substituted in place of the expected cryptogram, as taught by Brown, in a financial transaction system of Royyuru. This combination allows for a a less expensive microcontroller to be required (Brown [0134]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Regarding claim 4 of Claim 3, Royyuru further discloses wherein the unpredictable data comprises an unpredictable number (unpredictable number UN, [0049]-[0051] and [0057]).

Regarding claim 5 of Claim 3, Royyuru discloses that the unpredictable data may be any number, such as a random number, a time of day, or another number generated or received by the presentation instrument ([0051]). Royyuru does not specifically state wherein the unpredictable data comprises a transaction amount. However, it is notoriously well known that a transaction amount is a number. A transaction amount is also unpredictable in the sense that the number is not known as opposed to a credit card number which is already predetermined. Therefore, it would have been obvious to a person having ordinary skill in the art for the unpredictable data of Royyuru to comprise any number, such that the number may be a transaction amount, because a transaction amount is a number that is unpredictable and changes with each transaction.

Regarding claim 6 of Claim 3, Royyuru further discloses a mobile device preparation step that precedes the performing an interrogation step, the mobile device preparation step comprising sending critical data from a remote source to a mobile device, wherein the critical data comprises data used to formulate at least a portion of the digital credential data as a local portion of the digital credential data (before a financial transaction may occur, the mobile device needs to be programmed with a key and information regarding a primary account number PAN that can be mapped to a dynamic PAN, [0004]-[0006] and [0047]-[0048]).

Regarding claim 24 of Claim 3, Royyuru further discloses an authorizing step that follows the step of performing an interrogation, the authorizing step comprising sending the unpredictable data from the mobile device to a remote application system (the mobile device may send the unpredictable number to a remote system as Track-1 data, because the unpredictable number is contained in the Track-1 data format, [0049]-[0051]).

Regarding claim 26 of Claim 3, Royyuru further discloses wherein the communication channel comprises a near-field communication channel (communication via NFC technology is used, [0002]-[0003] and [0022]).

Claims 7, 17 lack an inventive step under PCT Article 33(3) as being obvious over Royyuru et al (US 2010/0185545 A1), hereinafter referred to as Royyuru and further in view of Brown et al (US 2009/0006262 A1), hereinafter referred to as Brown, and further in view of Smets et al (US 2006/0022033 A1), hereinafter referred to as Smets.

Regarding claim 7 of Claim 6, Royyuru may not specifically state: wherein the local portion of the digital credential data comprises a predetermined cryptogram, which is calculated without the use of the unpredictable data, as the unexpected cryptogram. However, Smets is also in the field of electronic payment systems (abstract) and further teaches: wherein the local portion of the digital credential data comprises a predetermined cryptogram (a bitmap is created which serves as a type of template that defines data that is used or unused/discretionary, [0013]-[0014], and hence the bitmap creates a cryptogram that is predetermined and as-of-yet unexpected), which is calculated without the use of the unpredictable data, as the unexpected cryptogram (the unpredictable number is not placed in the bitmap yet, because it is considered to be discretionary, [0026] and [0031]-[0033]). Therefore, it would have been obvious to a person having ordinary skill in the art: wherein the local portion of the digital credential data comprises a predetermined cryptogram, which is calculated without the use of the unpredictable data, as the unexpected cryptogram, as taught by Smets, in an electronic payment system of Royyuru. This combination allows for financial transaction data to be standardized (Smets [0013]-[0014]).

Regarding claim 17 of Claim 3, Royyuru may not specifically state: creating a predetermined cryptogram on the mobile device as the unexpected cryptogram; wherein the predetermined cryptogram is calculated without the use of the unpredictable data; and sending at least a portion of the predetermined cryptogram from the mobile device to a remote application system. However, Smets is also in the field of electronic payment systems (abstract) and further teaches: creating a predetermined cryptogram on the mobile device as the unexpected cryptogram (a bitmap is created which serves as a type of template that defines data that is used or unused/discretionary, [0013]-[0014], and hence the bitmap creates a cryptogram that is predetermined and as-of-yet unexpected); wherein the predetermined cryptogram is calculated without the use of the unpredictable data (the unpredictable number is not placed in the bitmap yet, because it is considered to be discretionary, [0026] and [0031]-[0033]); and sending at least a portion of the predetermined cryptogram from the mobile device to a remote application system (at least a portion of the cryptogram is sent from the mobile device to a remote system for authorization of the transaction, Fig. 5 and [0026]). Therefore, it would have been obvious to a person having ordinary skill in the art for: creating a predetermined cryptogram on the mobile device as the unexpected cryptogram; wherein the predetermined cryptogram is calculated without the use of the unpredictable data; and sending at least a portion of the predetermined cryptogram from the mobile device to a remote application system, as taught by Smets, in an electronic payment system of Royyuru. This combination allows for financial transaction data to be standardized (Smets [0013]-[0014]).

Claims 12-14, 18 lack an inventive step under PCT Article 33(3) as being obvious over Royyuru et al (US 2010/0185545 A1), hereinafter referred to as Royyuru and further in view of Brown et al (US 2009/0006262 A1), hereinafter referred to as Brown, and further in view of Fisher et al (US 2009/0124234 A1), hereinafter referred to as Fisher.

Regarding claim 12 of Claim 6, Royyuru may not adequately disclose: wherein the mobile device preparation step further comprises transiently storing at least a portion of the critical data on the mobile device, wherein the mobile device does not persistently store the at least a portion of critical data. However, Fisher is also in the field of payment transactions ([0011]) and further teaches: wherein the mobile device preparation step further comprises transiently storing at least a portion of the critical data on the mobile device (critical data like a cryptographic key, is transiently stored in the mobile device, because it is only valid for the duration the session, Fig. 4 and [[0016]]), wherein the mobile device does not persistently store the at least a portion of critical data (the cached key data may be flushed, and hence the mobile device does not persistently store the key, Fig.4 and [0017]-[0018]). Therefore, it would have been obvious to a person having ordinary skill in the art: wherein the mobile device preparation step further comprises transiently storing at least a portion of the critical data on the mobile device, wherein the mobile device does not persistently store the at least a portion of critical data, as taught by Fisher, in a payment transaction system of Royyuru. This combination allows for a financial transaction system that is more secure in the event that the mobile device is lost or stolen (Fisher [0013]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding claim 13 of Claim 6, Royyuru further discloses wherein the local portion of the digital credential data comprises an unpredictable cryptogram as the unexpected cryptogram (the Primary Account Number PAN, which is digital credential data, is not sent to the remote system; instead a dynamic PAN is generated and sent as the unpredictable, unexpected cryptogram, Fig. 4 and [0051]-[0055]).
Royyuru may not best disclose: wherein the unpredictable cryptogram is calculated, at least in part, using a temporary cryptographic key.
However, Fisher is also in the field of payment transactions ([0011]) and further teaches: wherein the unpredictable cryptogram is calculated, at least in part, using a temporary cryptographic key (a session key, which is a temporary cryptographic key, is created for the mobile device, Fig. 3 and [0016], and the session key is used to encrypt data for the session, [0016]). Therefore, it would have been obvious to a person having ordinary skill in the art: wherein the unpredictable cryptogram is calculated, at least in part, using a temporary cryptographic key, as taught by Fisher, in a payment transaction system of Royyuru. This combination allows for a financial transaction system that is more secure in the event that the mobile device is lost or stolen (Fisher [0013]).

Regarding claim 14 of Claim 6, Royyuru further discloses wherein the mobile device preparation step further comprises:
Royyuru further discloses wherein the local portion of the digital credential data comprises an unpredictable cryptogram as the unexpected cryptogram (the Primary Account Number PAN, which is digital credential data, is not sent to the remote system; instead a dynamic PAN is generated and sent as the unpredictable, unexpected cryptogram, Fig. 4 and [0051]-[0055]).
Royyuru may not best disclose: creating a temporary cryptographic key in a remote application system wherein the remote application system is the remote source; sending at least a portion of the temporary cryptographic key from the remote application system to the mobile device as a portion of the critical data; and wherein the unpredictable cryptogram is calculated, at least in part, using the temporary cryptographic key. However, Fisher is also in the field of payment transactions ([0011]) and further teaches:
creating a temporary cryptographic key in a remote application system wherein the remote application system is the remote source (a session key, which is a temporary cryptographic key, is server-generated and created for the mobile device, Fig. 3 and [0016]); sending at least a portion of the temporary cryptographic key from the remote application system to the mobile device as a portion of the critical data (at least a portion of session key is sent from the server to the mobile device, because the session key is server generated, Fig. 3 and [0016]); and wherein the unpredictable cryptogram is calculated, at least in part, using the temporary cryptographic key (the session key is used to encrypt data for the session including cryptograms communicated during the session, [0016]). Therefore it would have been obvious to a person having ordinary skill in the art for: creating a temporary cryptographic key in a remote application system wherein the remote application system is the remote source; sending at least a portion of the temporary cryptographic key from the remote application system to the mobile device as a portion of the critical data; and wherein the unpredictable cryptogram is calculated, at least in part, using the temporary cryptographic key, as taught by Fisher, in a payment transaction system of Royyuru. This combination allows for a financial transaction system that is more secure in the event that the mobile device is lost or stolen (Fisher [0013]).

Regarding claim 18 of Claim 3, Royyuru may not adequately disclose: creating a temporary cryptographic key on the mobile device; wherein the temporary cryptographic key is used to calculate, at least in part, an unpredictable cryptogram as the unexpected cryptogram; sending at least a portion of the unpredictable cryptogram from the mobile device to a remote application system. However, Fisher is also in the field of payment transactions ([0011]) and further teaches: creating a temporary cryptographic key on the mobile device (a session key, which is a temporary cryptographic key, is created for the mobile device, Fig. 3 and [0016]); wherein the temporary cryptographic key is used to calculate, at least in part, an unpredictable cryptogram as the unexpected cryptogram (the session key is used to encrypt data for the session, [0016], and hence constitutes an unpredictable cryptogram calculated at least in part with a temporary session key); sending at least a portion of the unpredictable cryptogram from the mobile device to a remote application system (at least a portion of the cryptogram is sent to a remote server in order to conduct payment transactions, Fig. 1 and [0011]-[0013]). Therefore it would have been obvious to a person having ordinary skill in the art for: creating a temporary cryptographic key on the mobile device; wherein the temporary cryptographic key is used to calculate, at least in part, an unpredictable cryptogram as the unexpected cryptogram; sending at least a portion of the unpredictable cryptogram from the mobile device to a remote application system, as taught by Fisher, in a payment transaction system of Royyuru. This combination allows for a financial transaction system that is more secure in the event that the mobile device is lost or stolen (Fisher [0013]).

Claim 25 lacks an inventive step under PCT Article 33(3) as being obvious over Royyuru et al (US 2010/0185545 A1), hereinafter referred to as Royyuru and further in view of Brown et al (US 2009/0006262 A1), hereinafter referred to as Brown, and further in view of Buhot et al (US 2010/0207742 A1), hereinafter referred to as Buhot.

Regarding claim 25 of Claim 3, Royyuru further discloses that the POS command communication conforms to a data protocol and the device response communication conforms to a data protocol (in order to communicate, [0057] and [0037]). Royyuru lacks wherein the data protocol is the ISO 7816-4 protocol. However, Buhot is also in the field of near field communications (abstract) and further teaches the ISO 7816-4 data protocol ([0052] and [0085]). Therefore, it would have been obvious to a person having ordinary skill in the art to substitute a data protocol for the ISO 7816-4 protocol of Buhot wherein the POS command communication conforms to a data protocol and the device response communication conforms to a data protocol of Royyuru. This combination allows for an electronic payment system using NFC technology (Buhot [0018]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Claim 27 lacks an inventive step under PCT Article 33(3) as being obvious over Royyuru et al (US 2010/0185545 A1), hereinafter referred to as Royyuru and further in view of Brown et al (US 2009/0006262 A1), hereinafter referred to as Brown, and further in view of Yeager (US 2007/0075133 A1).

Regarding claim 27 of Claim 3, Royyuru does not specifically state: wherein the mobile device does not access a local persistently stored permanent cryptographic key that is expected to be used to calculate the expected cryptogram wherein the expected cryptogram is expected to be contained within the at least a portion of the digital credential. However, Yeager is also in the field of NFC devices ([0003]) and further teaches: wherein the mobile device does not access a local persistently stored permanent cryptographic key that is expected to be used to calculate the expected cryptogram wherein the expected cryptogram is expected to be contained within the at least a portion of the digital credential (a mobile device, like a mobile phone, [0027], does not actually access the keys, because the keys for encrypting the credential data are only shared between the server and adapter, Fig. 6 and [0031]-[0032]). Therefore, it would have been obvious to a person having ordinary skill in the art: wherein the mobile device does not access a local persistently stored permanent cryptographic key that is expected to be used to calculate the expected cryptogram wherein the expected cryptogram is expected to be contained within the at least a portion of the digital credential, as taught by Yeager, in a financial transaction system of Royyuru. This combination better ensures the confidentiality and security of the keys (Yeager [0031]).

Claims 8-11, 15-16, 19-23 meet the criteria set out in PCT Article 33(2)-(3), because the prior art does not teach or fairly suggest:

Regarding claim 8 creating remote unpredictable data in a remote application system wherein the remote application system is the remote source; sending the remote unpredictable data from application system to an HSM; calculating a predetermined cryptogram in the HSM; sending the predetermined cryptogram from the HSM to the remote application system; sending at least a portion of the predetermined cryptogram from the remote application system to the mobile device as a portion of the critical data; and wherein the local portion of the digital credential data comprises the predetermined cryptogram as the unexpected cryptogram.

Regarding claim 9 creating a predetermined cryptogram, which is calculated without the use of the unpredictable data, in a remote application system wherein the remote application system as the remote source; sending at least a portion the predetermined cryptogram from the remote application system to the mobile device as a portion of the critical data; and wherein the local portion of the digital credential data comprises the predetermined cryptogram as the unexpected cryptogram.

Regarding claim 10 wherein the critical data comprises a set of possible predetermined cryptograms; and the method further comprises a logical step of logically determining, in the mobile device, which of the possible predetermined cryptograms within the set of predetermined cryptograms to designate as the unexpected cryptogram; wherein the logical step is based, at least in part, on the unpredictable data; and wherein the local portion of the digital credential data comprises the designated predetermined cryptogram as the unexpected cryptogram.

Regarding claim 11: wherein the critical data comprises a set of possible predetermined cryptograms and card risk management data; and the method further comprises a logical step of logically determining, in the mobile device, which of the possible predetermined cryptograms within the set of possible predetermined cryptograms to designate as the unexpected cryptogram; wherein the logical step of is based, at least in part, on the unpredictable data or based, at least in part, on the card risk management data; and wherein the local portion of the digital credential data comprises the designated predetermined cryptogram as the unexpected cryptogram.

Regarding claim 15 wherein the critical data comprises a temporary cryptographic key; and the method further comprises a step of calculating at least one local unpredictable cryptogram that is calculated, in at least part, using the temporary cryptographic key, and, in at least part, using a calculation formula determined from a set of calculation formulas; and the method further comprises a logical step of logically determining, in the mobile device, which local unpredictable cryptogram to designate as the unpredictable cryptogram; wherein the step of logically determining a decision is made based, at least in part, on the unpredictable data; and wherein the local portion of the digital credential data comprises the designated local unpredictable cryptogram as the unexpected cryptogram.

Regarding claim 16 wherein the critical data comprises a temporary cryptographic key and card risk management data; and the method further comprises a step of calculating at least one local unpredictable cryptogram that is calculated, in at least part, using the temporary cryptographic key, and, in at least part, using a calculation formula determined from a set of calculation formulas; and the method further comprises a logical step of logically determining, in the mobile device, which local unpredictable cryptogram to designate as the unpredictable cryptogram;
wherein the logical step is made based, at least in part, on the unpredictable data or based, at least in part, on the card risk management data; and wherein the local portion of the digital credential data comprises the designated local unpredictable cryptogram as the unexpected cryptogram.

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Regarding claim 19: an authorizing step that follows the step of performing the interrogation, the authorizing step comprising: sending an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system, wherein the unexpected cryptogram comprises a predetermined cryptogram; verifying a correctness of the predetermined cryptogram by the application system
(a) by comparing the predetermined cryptogram with a previously stored reference predetermined cryptogram and
(b) without reference to the unpredictable data from the point-of-sale terminal; and sending an authorization response from the remote application system to the point-of-sale wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the predetermined cryptogram.

Regarding claim 20 an authorizing step that follows the step of performing the interrogation, the authorizing step comprising: sending an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system, wherein the unexpected cryptogram comprises an unpredictable cryptogram; verifying a correctness of the unpredictable cryptogram by the application system wherein the unpredictable cryptogram is compared with a result of an unpredictable cryptogram calculation; wherein the unpredictable cryptogram calculation is calculated using, at least in part, a temporary cryptographic key; and sending an authorization response from the remote application system to the point-of-sale wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable cryptogram.

Regarding claim 21 a corroborative authorizing step that follows the step of performing the interrogation, the corroborative authorizing step comprising: sending through a second communication channel an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system; sending through a third communication channel the unpredictable data from the mobile device to the remote application system; verifying a correctness of the unexpected cryptogram in the remote application system;
verifying a correctness of the unpredictable data in the remote application system by comparing the unpredictable data sent through the second communication channel with the unpredictable data sent through the third communication channel; sending through the second communication channel an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable data and, at least in part, by the verifying of the correctness of the unexpected cryptogram.

Regarding claim 22 a verifying a transaction amount step that follows the step of performing an interrogation and precedes the corroborative
authorizing step, the verifying a transaction amount step comprising: displaying transaction amount data to a display on the mobile device wherein the transaction amount data is at least a portion of the unpredictable data; requesting verification of the transaction amount data from a card holder by the mobile device display screen; sending the result of the requesting verification of the transaction amount data to a remote application system as input transaction amount data; and wherein the corroborative authorizing step comprises determining, at least in part, an accuracy of the result of the verification step by using the input of the transaction amount data.

Regarding claim 23 an authorizing step that follows the step of performing an interrogation, the authorizing step comprising: sending an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system, wherein the unexpected cryptogram comprises a predetermined cryptogram; verifying a correctness of the predetermined cryptogram wherein the unpredictable data from the point-of sale (a) is substituted by the application system with a previously created unpredictable data that was previously used to calculate the predetermined cryptogram; and subsequently (b) is sent with the predetermined cryptogram to the HSM for cryptogram correctness verification; and sending an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the predetermined cryptogram.

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding claim 28: A method for acquiring digital credential data by a point-of-sale terminal from a secure mobile device for authorization of a financial transaction comprising: performing an interrogation between the point-of-sale terminal and the secure mobile device comprising: sending through a communication channel at least one POS command communication from the point-of-sale terminal to the secure mobile device,
the at least one POS command communication comprising (a) a request for the digital credential data that is expected to comprise an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data, and, at least in part, from a permanent cryptographic key and (b) the unpredictable data; and sending through the communication channel at least one device response communication from the secure mobile device to the point-of-sale terminal, the at least one device response communication comprising at least a portion of the digital credential data that comprises the expected cryptogram; in a step that follows the step of performing an interrogation, a secure mobile device transmitting step comprising sending over a second communication channel the unpredictable data from the secure mobile device to a remote application system; in a step that follows the step of performing an interrogation, a point-of-sale terminal transmitting step comprising sending over a third communication channel an authorization request from the point of sale terminal to the remote application system, the authorization request comprising the expected cryptogram and the unpredictable data; in a step that follows the secure mobile device transmitting step and the point-of-sale terminal transmitting step, a corroborative authorizing step comprising: verifying a correctness of the expected cryptogram by the application system; verifying a correctness of the unpredictable data by the application system by comparing the unpredictable data sent over the second communication channel with the unpredictable data sent over the third communication channel; and sending through the third communication channel an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable data and at least in part by the verifying of the correctness of the expected cryptogram; wherein the financial transaction is authorized.

Claim 29 meets the criteria due to their dependence on novel claim 28.

The prior art, as shown below, details some of the aspects of the invention, however none of the prior art teaches all the missing limitations either alone or in combination as specified:

Royyuru et al (US 2010/0185545 A1), discloses a method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction (dynamic primary account number and unique key per card, title: financial transaction authorization, abstract, Fig. 3) comprising:
performing an interrogation between the point-of-sale terminal and the mobile device (in NFC technology, a mobile device is in communication with a point-of-sale POS terminal, [0022]) comprising: sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device (commands and responses are communicated between a terminal and mobile device in order to perform a financial transaction, [0057]), the at least one POS command communication comprising (a) a request for the digital credential data that is expected to comprise an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data, and, at least in part, from a permanent cryptographic key (transaction requests comprise credit card numbers, which is digital credential data, and is calculated from a unpredictable number, which is unpredictable data, and the message is encrypted with a key, [0049]-[0051]) and (b) the unpredictable data (an unpredictable number UN, which is unpredictable data, is generated by the NFC terminal and transmitted to the device, [0057]); and sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal (commands and responses are communicated between a terminal and mobile device in order to perform a financial transaction, [0057]), the at least one device response communication comprising at least a portion of the digital credential data that comprises an unexpected cryptogram (encrypting the credit card numbers with an unpredictable number will result in a dynamic PAN, which is an unexpected cryptogram, [0049]-[0051]), wherein the financial transaction is authorized (the financial transaction may be authorized or denied, [0050]).Royyuru may not adequately describe that an unexpected cryptogram is substituted in place of the expected cryptogram, or the verifying correctness features.

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Yeager discloses a method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction (method, system and computer-readable medium for radio frequency identification device, title; the adapter is connected to a host device like a mobile phone to construct a mobile device capable of financial transactions, Fig. 3 and [0027]-[0029], in which the mobile device communicates with a terminal such as the Mastercard PayPass system, Fig. 5 and [0030]) comprising: using a remote permanent cryptographic key to calculate an expected cryptogram that is expected to comprise at least a portion of the digital credential data (a secret key on a remote server, Fig. 6 and [0031]-[0032], which is a remote permanent cryptographic key, is used to calculate an expected cryptogram that comprises, and hence encrypts, digital credential data such as credit card information, [0022]). Yeager does not disclose the unpredictable data; and sending through the communication channel at least one device response communication from the secure mobile device to the point-of-sale terminal, the at least one device response communication comprising at least a portion of the digital credential data that comprises the expected cryptogram; in a step that follows the step of performing an interrogation, a secure mobile device transmitting step comprising sending over a second communication channel the unpredictable data from the secure mobile device to a remote application system; in a step that follows the step of performing an interrogation, a point-of-sale terminal transmitting step comprising sending over a third communication channel an authorization request from the point of sale terminal to the remote application system, the authorization request comprising the expected cryptogram and the unpredictable data; in a step that follows the secure mobile device transmitting step and the point-of-sale terminal transmitting step, a corroborative authorizing step comprising: verifying a correctness of the expected cryptogram by the application system; verifying a correctness of the unpredictable data by the application system by comparing the unpredictable data sent over the second communication channel with the unpredictable data sent over the third communication channel; and sending through the third communication channel an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable data and at least in part by the verifying of the correctness of the expected cryptogram; wherein the financial transaction is authorized.

Claims 1-29 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 67979.W1	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2012/041670	International filing date *(day/month/year)* 08 June 2012 (08.06.2012)	Priority date *(day/month/year)* 09 June 2011 (09.06.2011)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant YEAGER, C., Douglas		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 14 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 10 December 2013 (10.12.2013)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Simin Baharlou e-mail: pt09.pct@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: JAMES PALMER
LUEDEKA NEELY GROUP, P.C.
P.O. BOX 1871
KNOXVILLE, TN 37901-1871

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	17 AUG 2012
Applicant's or agent's file reference 67979.W1	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2012/041670	08 June 2012	09 June 2011

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - G06Q20/12 (2012.01)
USPC - 705/16

Applicant YEAGER, C.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	31 July 2012	Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (July 2011)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

   ☐ on paper

   ☐ in electronic form

   b. (time)

   ☐ in the international application as filed

   ☐ together with the international application in electronic form

   ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	4-52, 55-56	YES
	Claims	1-3, 53-54	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-56	NO
Industrial applicability (IA)	Claims	1-56	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-3 lack novelty under PCT Article 33(2) as being anticipated by Yeager.

Regarding Claim 1, Yeager discloses a system (see figs. 3-4 and 6) for acquiring digital credential data (see pgs. 3-4, para. 0026-0029 and 0031-0032; wherein the credential data is interpreted to be tag emulation data associated with portions of a specified user account information that is needed to carry out or complete electronic transactions) comprising: an electronic communication device (host 350; see fig. 3); a [inherent] communication channel (various connections that allow communication and data to be transferred between the adapter 100 and host 350 as well as between server 320 and adapter 100 via host 350 and internet connections; see figs. 3 and 6 as well as pgs. 3-4, para. 0026-0028 and 0031); and a repository (server 320 in combination with database 610; see figs. 3 and 6) remote from the electronic communications device (see figs. 3 and 6; wherein the server and associated database is inherently remote from host 350 since access and communication between the server and communications device is carried out through an internet connection) and having a plurality of secure element representations (see fig. 6 as well pgs. 3-4, para. 0031-0032; wherein a plurality of secure element representations is interpreted to be the stored customer account information associated with a plurality of users/customers), wherein the repository is configured to: a) receive a request for the digital credential data from the electronic communications device using the communication channel (see fig. 6 as well as pgs. 3-4, para. 0031-0032), b) validate [authenticate] the computing device (via inherently checking a secret key associated with a particular adapter 100 in combination with a user or customer entering a username and password; see pg. 3, para. 0031), wherein the electronic communication device is paired with one of the plurality of secure element representations (associated with a specific customer/user; see pgs. 3-4, para. 0031-0032); c) extract at least a portion of the digital credential data from the paired secure element representation (in order to complete a transaction see fig. 6 as well as pgs. 3-4, para. 0031-0032), and d) send a repository response communication with the digital credential data to the electronic communication device over the communication channel (see fig. 6 as well as pgs. 3-4, para. 0031-0032); and wherein the electronic communication device is configured to a) authenticate to the repository (via the use of a secret key associated with a particular adapter 100 in combination with a user or customer entering a username and password; see pg. 3, para. 0031), b) send a request for the acquisition of at least a portion of the digital credential data to the repository as a device command communication over the communication channel (in order to complete a transaction; see fig. 6 as well as pgs. 3-4, para. 0031-0032), and c) receive the repository response containing the digital credential data from the repository over the communication channel (in order to complete a transaction; see fig. 6 as well as pgs. 3-4, para. 0031-0032).

Regarding Claim 2, Yeager discloses all limitations of claim 1 and further discloses the electronic communication device being a mobile device (a pda, mobile phone or laptop; see pg. 3, para. 0027).

Regarding Claim 3, Yeager discloses all limitations of claim 1 and further discloses the electronic communication device being a stationary device (a personal computer; see pg. 4, para. 0035).

Claim 4 lacks an inventive step under PCT Article 33(3) as being obvious over Yeager in view of Hohle.

Regarding Claim 4, Yeager discloses all limitations of claim 1, but does not disclose the repository uses IS07816 to extract at least a portion of the digital credential data from a paired secure element representation.
However, Hohle is in the field of facilitating commercial transactions over a network (Col. 1, lines 7-11) and discloses a repository that uses IS07816 to extract at least a portion of the digital credential data from a paired secure element representation (card object database 116 is the repository; Col. 4, lines 13-24).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Hohle's feature in to Yeager's system. The motivation would have been to provide for the use of an internationally accepted standard (Hohle, Col. 4, lines 13-24).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Claim 5 lacks an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Florek et al., hereinafter referred to as Florek.

Regarding Claim 5, Rosenberg discloses a method (see figs. 9-10 as well as pgs. 8-10, para. 0097-0103 and 0105-0113) for acquiring digital credential data (the necessary portions of the user's financial account information that is needed to complete a transaction; see pgs. 9-10, para. 0102 and 0111) by a point-of-sale terminal (POS device 520 of fig. 9) having access to an internet from a mobile device (smartlink capable device 900 of fig. 9; see also pg. 8, para. 0097) that has access to the internet (in order to establish a communication link between the device and the user's financial institution as well as the payee's financial institution; see figs. 9-10 as well as pg. 10, para. 0111-0112).
But, Rosenberg does not specifically teach the mobile device of the method having a secure element and a secure element reader; and the method comprising: a) reading the secure element in the mobile device using the secure element reader in the mobile device; and b) sending the digital credential data, acquired from reading the secure element in the mobile device, from the mobile device to the point-of-sale terminal over the internet.
However, Florek discloses a system and method of contactless authorization of an electronic payment (see the Abstract, for example); wherein Florek teaches the concept of the method and associated system including a mobile device (mobile communication device 1; see fig. 1) having a secure element (2; see fig. 1) and a secure element reader (NFC communications element 7 in combination with carrier 13; see fig.1 as well as pgs. 2-3, para. 0021-0023 and 0026-0027) in order to carry out electronic transactions between a user and POS terminal (see pgs. 2-3, para. 0025-0027); and wherein the method comprises a) reading the secure element in the mobile device using the secure element reader in the mobile device (in order to complete a transaction or purchase by a user; see pgs. 2-3, para. 0025-0027); and b) sending the digital credential data, acquired from reading the secure element in the mobile device, from the mobile device to the point-of-sale terminal over the internet (in order to complete a transaction or purchase by a user; see pgs. 2-3, para. 0025-0027).
It would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the method of Rosenberg include a mobile device having a secure element and a secure element reader, and the method comprising the steps recited above, as shown by Florek, for the purpose of initiating and complete an electronic transaction or purchase by a user.

Claim 6 lacks an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Florek and futher in view of Smith.

Regarding Claim 6, Rosenberg in view of Florek disclose all limitations of claim 5, but does not disclose acquiring in the mobile device a unique identifier of the point-of-sale terminal as an identified point-of-sale terminal; and establishing a unique network address of the identified point-of-sale terminal, and wherein step b) comprises sending the digital credential data to the identified point-of-sale terminal over the internet.
However, Smith is in the field of acquiring credential data (Par. 0048) and discloses acquiring in the mobile device a unique identifier of the point-of-sale terminal as an identified point-of-sale terminal (the IP address of the terminal is the unique identifier; Par. 0115); and establishing a unique network address of the identified point-of-sale terminal, and wherein step b) comprises sending the digital credential data to the identified point-of-sale terminal over the internet (data sent to the IP address of the terminal is sent over the Internet; Par. 0115).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Smith's feature in to modified Rosenberg's system. The motivation would have been to provide Internet accessibility for point of sale terminals (Smith, Par. 0115).

Claim 7 lacks an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Florek, in view of Garcia Ruano and further in view of Smith.

Regarding Claim 7, Rosenberg in view of Florek disclose all limitations of claim 5, but does not disclose reading a QR code into the mobile device; and translating the QR code in the mobile device to identify an internet address of the point-of-sale terminal, and wherein step b) comprises sending the digital credential data over the internet to the internet address of the point-of-sale terminal.
However, Garcia Ruano is in the field of using a mobile phone as a payment device (Abs.) and discloses reading a QR code into the mobile device; and translating the QR code in the mobile device (the barcode is the QR code; Par. 0040).
Further, Smith is in the field of acquiring credential data (Par. 0048) and discloses sending the digital credential data over the internet to the internet address of the point-of-sale terminal (data sent to the IP address of the terminal is sent over the Internet; Par. 0115).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Garcia Ruano's and Smith's feature in to modified Rosenberg's system. The motivation would have been to allow for the use of barcodes (Garcia Ruano, Par. 0040) and to provide Internet accessibility for point of sale terminals (Smith, Par. 0115).

Claim 8 lacks an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Florek, in view of Bishop and further in view of Smith.

Regarding Claim 8, Rosenberg in view of Florek disclose all limitations of claim 5, but does not disclose reading an RFID tag code into the mobile device; and translating the RFID tag code in the mobile device to identify an internet address of the point-of-sale terminal, and wherein step b) comprises sending the digital credential data over the internet to the internet address of the point-of-sale terminal.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses reading an RFID tag code into the mobile device; and translating the RFID tag code in the mobile device (RFID transaction device, is the mobile device; Par. 0039).
Further, Smith is in the field of acquiring credential data (Par. 0048) and discloses sending the digital credential data over the internet to the internet address of the point-of-sale terminal (data sent to the IP address of the terminal is sent over the Internet; Par. 0115).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's and Smith's feature in to modified Rosenberg's system. The motivation would have been to allow for the use of RFID tags (Bishop, Par. 0039) and to provide Internet accessibility for point of sale terminals (Smith, Par. 0115).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Claim 9 lacks an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Florek and further in view of Billmaier.

Regarding Claim 9, Rosenberg in view of Florek disclose all limitations of claim 5, but does not disclose using a GPS geo-location utility in the mobile device to define an internet address of the point-of-sale terminal, and wherein step b) comprises sending the digital credential data over the internet to the internet address of the point-of-sale terminal.
However, Billmaier is in the field of authenticating commercial transactions (Abs.) and disclose using a GPS geo-location utility in the mobile device to define an internet address of the point-of-sale terminal (GPS is used to detect the IP address; Par. 0008), and wherein step b) comprises sending the digital credential data over the internet to the internet address of the point-of-sale terminal (data sent to the terminal's IP address, is sent over the Internet; Par. 0008).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Billmaier's feature in to modified Rosenberg's system. The motivation would have been to provide security for the user by preventing fraudulent transactions (Billmaier, Par. 0008).

Claim 10 lacks an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Florek and further in view of Bishop.

Regarding claim 10, Rosenberg in view of Florek disclose all limitations of claim 5, but lacks explicitly teaching translating the digital credential data received by the point-of-sale terminal into Track Data, and delivering the Track Data to a field in a transaction authorization system using keyboard emulation.
In the field of RF Transaction authentication, Bishop teaches translating the digital credential data received by the point-of-sale terminal into Track Data, and delivering the Track Data to a field in a transaction authorization system using keyboard emulation (para [0031] account information is stored as track 1 and track 2 data as defined in ISO/IEC 7813; para [0036]-[0037] authentication data may be forwarded or encoded in all or a portion of a data stream, representing data encoded in track 2 or track 3 format; para [0031], wherein the stream of data may look like "0000 0000 00000000" which is a stream of keys).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of Rosenberg in view of Florek to include the method of communicating account related data of Bishop in order to secure customer related information (Bishop, para [0010]).

Claims 11-13, 17-20, 36-38, 40-44 and 55-56 lack an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Yeager.

Regarding Claim 11, Rosenberg discloses a method (see figs. 4-5, 7 and 9-10 as well as pgs. 5-6 and 8-10, para. 0056-0072, 0074, 0097-0103 and 0105-0113) for acquiring digital credential data (a transaction confirmation signal in combination with the necessary portions of the complete user account and credit card information that is associated with the financial institutions of a user and used to complete a transaction; see pg. 10, para. 0111-0113, for example) by a point-of-sale terminal (POS device 420/520; see figs. 4 and 9) comprising: a mobile device (device 110/900 of figs. 4 and 9) in combination/connection with a repository (an inherent memory associated with the smartlink device 100 that is connected to device 110/an inherent memory associated with device 900 that has securely stored user financial account information in combination with a buyer's/user's financial institution 470; see figs. 4 and 9 as well as pgs. 5 and 10, para. 0062-0065 and 0111) having a plurality of secure element representations (the complete user account and credit card information that is associated with various financial institutions and stored in each device as well as in the user's/buyer's financial institution portion of the repository that inherently contains a plurality of stored users' account information; see pgs. 0-10, para. 0102 and 0111) wherein the mobile device is [inherently] paired with one of the secure element representations in the repository (in order to identify the proper accounts associated with a specified user that can be used for electronic transactions; see pgs. 9-10, para. 0102 and 0111); sending through a first communication channel a POS command communication from the point-of-sale terminal to the mobile device requesting the digital credential data (see figs. 4-5, 7 and 9-10 as well as pgs. 5 and 8-9, para. 0059 and 0100-0101); and sending through the first communication channel a device response communication from the mobile device to the point-of-sale terminal wherein the device response communication comprises at least a portion of the digital credential data (see figs. 5 and 10 as well as pgs. 5 and 10, para. 0065-0067 and 0111-0113; wherein the credential data is interpreted to include portions of a user's financial account information that is necessary to complete the transaction as well as a confirmation signal that is received by the POS device).
But, Rosenberg does not specifically discuss the method comprising: authenticating and validating a mobile device at the repository [the user's/buyer's financial institution].
However, Rosenberg discloses the a step of authenticating and validating at the mobile device (see pgs. 5, 7 and 10; para. 0062-0063, 0084 and 0111).
Yeager discloses a method and system for authorizing and implementing electronic transactions (see the Abstract as well as pg. 1, para. 0003, for example); wherein Yeager teaches the concept of authenticating and validating a mobile device at a repository (server 320 in combination with database 610; see figs. 3 and 6 as well as pg. 3, para. 0031).
It would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the method of Rosenberg comprise the step of authenticating and validating a mobile device at the repository, as shown by Yeager, for the purpose of preventing unauthorized transactions and payments.

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding Claim 12, Rosenberg in view of Yeager disclose all limitations of Claim 11. Rosenberg does not disclose the method further comprising: sending through a second communication channel a device command communication from the mobile device to the repository; and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises at least a portion of the digital credential.
However, Yeager discloses the method further comprising: sending through a second communication channel [the communication connection/link between the device 110/900 and the user's/buyer's financial institution 470; see figs. 4 and 9) a device command communication from the mobile device to the repository (in order to initiate transfer of funds from a user's account to a seller's account; see pgs. 5, 10, para. 0062-0064 and 0111, for example; wherein the command is sent to the portion of the repository that comprises the smartlink 100 of device 110/the portion of device 900 that securely contains the user's financial account information); and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises at least a portion of the digital credential data (portions of the user's financial account information that is needed in order to complete the transaction and purchase; see figs. 5 and 7 as well as pgs. 5, para. 0064-0067 and 0081-0085).
It would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the method of Rosenberg comprise the step of authenticating and validating a mobile device at the repository, as shown by Yeager, for the purpose of preventing unauthorized transactions and payments.

Regarding Claim 13, Rosenberg in view of Yeager disclose all limitations of Claim 11. Rosenberg further discloses the method further comprising: caching [storing] at least a portion of the digital credential data in the mobile device (see figs. 5 and 7 as well as pgs. 5, 7 and 10, para. 0062-0064, 0081-0084 and 0111), wherein the device response communication comprises the cached portion of the digital credential data (see fig. 7 as well as pg. 7, para. 0084-0085 and 0111).

Regarding Claim 17, Rosenberg in view of Yeager disclose all limitations of Claim 11. Rosenberg further discloses the mobile device being proximate to the point-of-sale terminal (see figs. 4 and 8).

Regarding Claim 18, Rosenberg in view of Yeager disclose all limitations of Claim 11. Rosenberg further discloses the mobile device being remote from the repository (the portion of the repository associated with the user's/buyer's financial institution 470; see figs. 4 and 9).

Regarding Claim 19, Rosenberg in view of Yeager disclose all limitations of Claim 11. Rosenberg further discloses the point-of-sale terminal being remote from the repository (the portion of the repository associated with the user's/buyer's financial institution 470; see figs. 4 and 9).

Regarding Claim 20, Rosenberg in view of Yeager disclose all limitations of Claim 11. Rosenberg further discloses the mobile device being remote from the repository (the portion of the repository associated with the user's/buyer's financial institution 470; see figs. 4 and 9) and the point-of-sale terminal is remote from the repository (the portion of the repository associated with the user's/buyer's financial institution 470; see figs. 4 and 9) and the digital credential data comprises Track Data (data in the form of account numbers and information that is associated with a user's financial accounts; see pgs. 7 and 10, para. 0084 and 0111).

Regarding Claim 36, Rosenberg discloses a system (see figs. 4 and 9) for acquiring digital credential data (pgs. 5-6 and 8-10, para. 0056-0072, 0074, 0097-0103 and 0105-0113; wherein credential data is interpreted to be a transaction confirmation signal in combination with the necessary portions of the complete user account and credit card information that is associated with the financial institutions of a user and used to complete a transaction; see pg. 10, para. 0111-0113, for example) comprising: a mobile device (device 110/900; see figs. 4 and 9, for example); a first communication channel (a communication link between the POS device 420,410/520,525 via an NFC link; see figs. 4 and 9 as well as pgs. 2-3 and 5, para. 0036 and 0064-0065, for example); a point-of-sale terminal (POS device 420,410/520,525 via an NFC link; see figs. 4 and 9) configured to generate a request for an acquisition of the digital credential data from the mobile device over the first communication channel as a POS command communication (see figs. 4-5, 7 and 9-10 as well as pgs. 5 and 8-9, para. 0059 and 0100-0101), and configured for receiving the digital credential data from the mobile device over the first communication channel as a device response communication (see figs. 5 and 10 as well as pgs. 5 and 10, para. 0065-0067 and 0111-0113; wherein the credential data is interpreted to include portions of a user's financial account information that is necessary to complete the transaction as well as a confirmation signal that is received by the POS device); and a repository (an inherent memory associated with the smartlink device 100 that is connected to device 110/an inherent memory associated with device 900 that has securely stored user financial account information in combination with a buyer's/user's financial institution 470; see figs. 4 and 9 as well as pgs. 5 and 10, para. 0062-0065 and 0111) that is remote from the point-of-sale terminal (see figs. 4 and 9; wherein the portion of the repository corresponding to the user's/buyer's financial institution 470 is disclosed/depicted as being remote from the POS device/terminal), the repository having a plurality of secure element representations (the complete user account and credit card information that is associated with various financial institutions and stored in each device as well as in the user's/buyer's financial institution portion of the repository that inherently contains a plurality of stored users' account information; see pgs. 9-10, para. 0102 and 0111) and [inherently] pair the mobile device with a specific secure element representation (in order to identify the proper accounts associated with a specified user that can be used for electronic transactions; see pgs. 9-10, para. 0102 and 0111); and wherein the mobile device is remote from the repository (see figs. 4 and 9; wherein the portion of the repository corresponding to the user's/buyer's financial institution 470 is disclosed/depicted as being remote from the POS device/terminal) and is configured to a) authenticate at the mobile device (see pgs. 5, 7 and 10; para. 0062-0063, 0084 and 0111); b) receive the POS command communication over the first communication channel (see figs. 4-5, 7 and 9-10 as well as pgs. 5 and 8-9, para. 0059 and 0100-0101), and c) send at least a portion of the digital credential data to the point-of-sale terminal as the device response communication over the first communication channel (see figs. 5 and 10 as well as pgs. 5 and 10, para. 0065-0067 and 0111-0113; wherein the credential data is interpreted to include portions of a user's financial account information that is necessary to complete the transaction as well as a confirmation signal that is received by the POS device).
But, Rosenberg does not specifically discuss the method comprising the following: the repository [the portion of the repository that corresponds to a user's/buyer's financial institution 470 of figs. 4 and 9] being configured to validate the mobile device; and the mobile device being configured to authenticate to the repository.

[cont. on next supplemental box]

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

[Regarding claim 36 -- cont.]
However, Yeager discloses a method and system for authorizing and implementing electronic transactions (see the Abstract as well as pg. 1, para. 0003, for example); wherein Yeager teaches the concept of authenticating and validating a mobile device at a repository (server 320 in combination with database 610; see figs. 3 and 6 as well as pg. 3, para. 0031).
It would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the system of Rosenberg comprise the repository being configured to validate the mobile device; and the mobile device being configured to authenticate to the repository, as shown by Yeager, for the purpose of preventing unauthorized transactions and payments.

Regarding Claim 37, Rosenberg in view of Yeager disclose all limitations of claim 36. Rosenberg further discloses the system further comprising a second communication channel (the communication connection/link between the device 110/900 and the user's/buyer's financial institution 470; see figs. 4 and 9) and wherein: the repository is configured to receive a request for the digital credential data from the mobile device using the second communication channel (in order to initiate transfer of funds from a user's account to a seller's account; see pgs. 5, 10, para. 0062-0064 and 0111, for example; wherein the command is sent to the portion of the repository that comprises the smartlink 100 of device 110/the portion of device 900 that securely contains the user's financial account information) and to send a response with at least a portion of the digital credential data to the mobile device using the second communication channel (portions of the user's financial account information that is needed in order to complete the transaction and purchase; see figs. 5 and 7 as well as pgs. 5, para. 0064-0067 and 0081-0085).

Regarding Claim 38, Rosenberg in view of Yeager disclose all limitations of claim 36. Rosenberg further inherently discloses the mobile device comprises a [inherent] cache memory configured to store at least a portion of the digital credential data as cached data (see figs. 5 and 7 as well as pgs. 5, 7 and 10, para. 0062-0064, 0061-0084 and 0111) and the mobile device is configured to send the cached data as at least a portion of the device response communication (see fig. 7 as well as pg. 7, para. 0084-0085 and 0111).

Regarding Claim 40, Rosenberg in view of Yeager disclose all limitations of claim 36. Rosenberg further discloses the mobile device being proximate to the point-of-sale terminal (see figs. 4 and 8).

Regarding Claim 41, Rosenberg in view of Yeager disclose all limitations of claim 36. Rosenberg further discloses the mobile device being remote from the repository (the portion of the repository associated with the user's/buyer's financial institution 470; see figs. 4 and 9).

Regarding Claim 42, Rosenberg in view of Yeager disclose all limitations of claim 36. Rosenberg further discloses the point-of-sale terminal being remote from the repository (the portion of the repository associated with the user's/buyer's financial institution 470; see figs. 4 and 9).

Regarding Claim 43, Rosenberg in view of Yeager disclose all limitations of claim 36. Rosenberg further discloses the mobile device being remote from the repository (the portion of the repository associated with the user's/buyer's financial institution 470; see figs. 4 and 9) and the point-of-sale terminal is remote from the repository (the portion of the repository associated with the user's/buyer's financial institution 470; see figs. 4 and 9) and the digital credential data comprises Track Data (data in the form of account numbers and information that is associated with a user's financial accounts; see pgs. 7 and 10, para. 0084 and 0111)..

Regarding Claim 44, Rosenberg in view of Yeager disclose all limitations of claim 36. Rosenberg further discloses the first communication channel comprises a near-field communication channel (see pgs. 2-3 and 5, para. 0036 and 0064-0065).

Regarding Claim 55, Rosenberg discloses a method (see figs. 4-5, 7 and 9-10 as well as pgs. 5-6 and 8-10, para. 0056-0072, 0074, 0097-0103 and 0105-0113) for acquiring digital credential data (a transaction confirmation signal in combination with the necessary portions of the complete user account and credit card information that is associated with the financial institutions of a user and used to complete a transaction; see pg. 10, para. 0111-0113, for example) by a point-of-sale terminal (POS device 420/520; see figs. 4 and 9) comprising: a mobile device (device 110/900 of figs. 4 and 9) in combination/connection with a repository (an inherent memory associated with the smartlink device 100 that is connected to device 110/an inherent memory associated with device 900 that has securely stored user financial account information in combination with a buyer's/user's financial institution 470; see figs. 4 and 9 as well as pgs. 5 and 10, para. 0062-0065 and 0111) having a plurality of secure element representations (the complete user account and credit card information that is associated with various financial institutions and stored in each device as well as in the user's/buyer's financial institution portion of the repository that inherently contains a plurality of stored users' account information; see pgs. 9-10, para. 0102 and 0111) wherein the mobile device is [inherently] paired with one of the secure element representations in the repository (in order to identify the proper accounts associated with a specified user that can be used for electronic transactions; see pgs. 9-10, para. 0102 and 0111); sending through a first communication channel a POS command communication from the point-of-sale terminal to the mobile device requesting the digital credential data (see figs. 4-5, 7 and 9-10 as well as pgs. 5 and 8-9, para. 0059 and 0100-0101); and sending through the first communication channel a device response communication from the mobile device to the point-of-sale terminal wherein the device response communication comprises at least a portion of the digital credential data (see figs. 5 and 10 as well as pgs. 5 and 10, para. 0065-0067 and 0111-0113; wherein the credential data is interpreted to include portions of a user's financial account information that is necessary to complete the transaction as well as a confirmation signal that is received by the POS device).
But, Rosenberg does not specifically discuss the method comprising: authenticating and validating a stationary device at the repository [the user's/buyer's financial institution].

[cont. on next supplemental box]

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

[Regarding claim 55 - cont.]
However, Rosenberg discloses the a step of authenticating and validating at the mobile device (see pgs. 5, 7 and 10; para. 0062-0063, 0084 and 0111)
Yeager discloses a method and system for authorizing and implementing electronic transactions (see the Abstract as well as pg. 1, para. 0003, for example); wherein Yeager teaches the concept of authenticating and validating a mobile device at a repository (server 320 in combination with database 610; see figs. 3 and 6 as well as pgs. 3-4, para. 0031 and 0035; wherein the stationary device is interpreted to be a personal computer).
It would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the method of Rosenberg comprise the step of authenticating and validating a stationary device at the repository, as shown by Yeager, for the purpose of preventing unauthorized transactions and payments.

Regarding Claim 56, Rosenberg in view of Yeager disclose all limitations of claim 55. Rosenberg further discloses a second communication channel (the communication connection/link between the device 110/900 and the user's/buyer's financial institution 470; see figs. 4 and 9) and wherein: the repository is configured to receive a request for the digital credential data from the stationary device using the second communication channel (in order to initiate transfer of funds from a user's account to a seller's account; see pgs. 5, 10, para. 0062-0064 and 0111, for example; wherein the command is sent to the portion of the repository that comprises the smartlink 100 of device 110/the portion of device 900 that securely contains the user's financial account information) and to send a response with at least a portion of the digital credential data to the stationary device using the second communication channel (portions of the user's financial account information that is needed in order to complete the transaction and purchase; see figs. 5 and 7 as well as pgs. 5, para. 0064-0067 and 0081-0085).

Claims 14-15, 21, 24-26, 28-34 & 47-52 lack an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Yeager and further in view of Bishop.

Regarding Claims 14 & 24, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose the POS command communication comprises a plurality of command communications conforming to IS07816-4 protocol, the device response communication comprises the plurality of the response communications conforming to IS07816-4 protocol, and the method further comprises: interpreting in the mobile device the POS command communications wherein, for at least one POS command communication the mobile device returns to the point-of-sale terminal as a portion of the device response communication a cached IS07816-4 protocol response communication from a cache located in the mobile device.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses the POS command communication comprises a plurality of command communications conforming to IS07816-4 protocol (ISO7816-4 is used since ISO7816 protocol is disclosed and the protocol is used to control communications between devices; Par. 0043), the device response communication comprises the plurality of the response communications conforming to IS07816-4 protocol, and the method further comprises: interpreting in the mobile device the POS command communications wherein, for at least one POS command communication the mobile device returns to the point-of-sale terminal as a portion of the device response communication a cached IS07816-4 protocol response communication from a cache located in the mobile device (the transaction device 102 is the mobile device, and the command communications originate from the database but are moved to cache upon execution by t he device's processor; Par. 0043).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's feature in to modified Rosenberg's system. The motivation would have been to allow for the use of an internationally accepted commercial communications standard (Bishop, Par. 0039).

Regarding Claim 15, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose sending through a second communication channel a device command communication from the mobile device to the repository; and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises the at least a portion of the digital credential data.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses sending through a second communication channel a device command communication from the mobile device to the repository (the Internet is the second communication channel; Par. 0024); and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises the at least a portion of the digital credential data (the response can also be sent through the Internet; Par. 0024).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's feature in to modified Rosenberg's system. The motivation would have been to take advantage of the Internet to complete commercial transactions (Bishop, Par. 0024).

Regarding Claim 21, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose the first communication channel comprises a near-field communication channel.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses the first communication channel comprises a near-field communication channel (the RFID system includes a near-field communication channel; Par. 0039).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's feature in to modified Rosenberg's system. The motivation would have been to facilitate point of sale transactions (Bishop, Par. 0006).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding Claims 25 & 29, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose sending through a second communication channel from the mobile device to the repository a device command communication conforming to any part of ISO 7816 part 1, 2, 3, or 4; and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises the at least a portion of the digital credential data.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses sending through a second communication channel from the mobile device to the repository (the Internet is the second communication channel; Par. 0024) a device command communication conforming to any part of ISO 7816 part 1, 2, 3, or 4 (ISO 7816 part 4 is used, since communications is controlled; Par. 0043); and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises the at least a portion of the digital credential data (the response is sent through the Internet; Par. 0024).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's feature in to modified Rosenberg's system. The motivation would have been to facilitate point of sale transactions (Bishop, Par. 0006).

Regarding Claim 26, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose the mobile device is remote from the repository and the method further comprises: sending through a second communication channel using TCP/UDP/IP protocol from the mobile device to the repository a device command communication; and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises the at least a portion of the digital credential data.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses the mobile device is remote from the repository and the method further comprises: sending through a second communication channel using TCP/UDP/IP protocol from the mobile device to the repository a device command communication (the Internet is the second communiation channel; Par. 0024); and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises the at least a portion of the digital credential data (the response can also travel through the Internet; Par. 0024).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's feature in to modified Rosenberg's system. The motivation would have been to facilitate point of sale transactions (Bishop, Par. 0006).

Regarding Claim 28, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose the POS command communication conforms to IS07816-4 protocol, the device response communication conforms to IS07816-4 protocol and the method further comprises: sending through a second communication channel from the mobile device to the repository a device command communication that conforms to IS07816-4 protocol; and sending through the second communication channel a repository response communication from the repository to the mobile device a repository response communication that conforms to IS07816-4 protocol.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses the POS command communication conforms to IS07816-4 protocol, the device response communication conforms to IS07816-4 protocol (ISO7816 protocol is used for communications between the devices, thus the ISO7816-4 is used; Par. 0043) and the method further comprises: sending through a second communication channel from the mobile device to the repository a device command communication that conforms to IS07816-4 protocol (the Internet is the second communication channel; Par. 0024); and sending through the second communication channel a repository response communication from the repository to the mobile device a repository response communication that conforms to IS07816-4 protocol (response conforms to ISO7816-4 since the response is a communication between devices; Par. 0043).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's feature in to modified Rosenberg's system. The motivation would have been to facilitate point of sale transactions (Bishop, Par. 0006).

Regarding claim 30, Rosenberg in view of Yeager disclose all limitations of claim 11, but lack explicitly teaching the method further comprises converting inside the mobile device at least a portion of the credential data into Track Data.
In the field of RF Transaction authentication, Bishop teaches the method further comprises converting inside the mobile device at least a portion of the credential data into Track Data (para [0031], [0036]-[0037] forwarded and encoding account related information in a portion of a data stream in track format).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of modified Rosenberg to include the method of communicating account related data of Bishop in order to secure customer related information (Bishop, para [0010]).

Regarding claim 31, Rosenberg in view of Yeager disclose all limitations of claim 11, but lack explicitly teaching the mobile device is remote from the point-of-safe terminal, and wherein the method further comprises: converting inside the mobile device at least a portion of the credential data into Track Data; and providing the Track Data formatted as digital credential data according to IS07813 as at least a portion of the device response communication.
In the field of RF Transaction authentication, Bishop teaches the mobile device is remote from the point-of-sale terminal (para [0027], input device may be a cellular phone interfacing with.. para [0028] POS device and host network interfaces to a remote network for authorization), and wherein the method further comprises: converting inside the mobile device at least a portion of the credential data into Track Data (para [0036]-[0037] forwarding and encoding account related information in a portion of a data stream in track format); and providing the Track Data formatted as digital credential data according to IS07813 as at least a portion of the device response communication (para [0031] account information is stored as track 1 and track 2 data as defined in ISO/IEC 7813; para [0036]-[0037] authentication data may be forwarded or encoded in all or a portion of a data stream, representing data encoded in track 2 or track 3 format; para [0031], wherein the stream of data may look like "0000 0000 00000000" which is a stream of keys).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of Rosenberg in view of Yeager to include the method of communicating account related data of Bishop in order to secure customer related information (Bishop, para [0010]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding claim 32, Rosenberg in view of Yeager disclose all limitations of claim 11, but lack explicitly teaching the mobile device is remote from the repository, the point-of-sale terminal is remote from the repository, the repository comprises a database of static Track Data, and the method further comprises: constructing in the repository cache data or at least a portion of a repository response communication using the database of static Track Data.
In the field of RF Transaction authentication, Bishop teaches the mobile device is remote from the repository, the point-of-sale terminal is remote from the repository (para [0027], input device may be a cellular phone interfacing with.. para [0028] POS device and host network interfaces to a remote network for authorization), the repository comprises a database of static Track Data (para [0032],[0041], host network utilizes a database containing account data; para [0031], wherein account data can be in Track 1 or Track 2 format), and the method further comprises: constructing in the repository cache data or at least a portion of a repository response communication using the database of static Track Data (para [0032] database may be configured to store account information; para [0031] wherein account information is stored as Track 1 or Track 2 data).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of Rosenberg in view of Yeager to include the method of communicating account related data of Bishop in order to secure customer related information (Bishop, para [0010]).

Regarding claim 33, Rosenberg in view of Yeager disclose all limitations of claim 11, but lack explicitly teaching the first communication channel comprises an NFC communication channel; the POS command communication comprises a select file command conforming to IS07816-4 protocol using a VISA AID starting with A000000003; and the device response communication comprises digital credential data that does not have a beginning PAN digit, as defined in IS07813, equal to a numeral "4".
In the field of RF Transaction authentication, Bishop teaches the first communication channel comprises an NFC communication channel (para [0027]-[0028] user communicates with network over a communications protocol; para [0032] wherein the communications protocol may be RFID [RFID is a type of NFC communications protocol]); the POS command communication comprises a select file command conforming to IS07816-4 protocol using a VISA AID starting with A000000003 (para [0043] storing transaction device information according to ISO 7816 file structure standards; para [0050] wherein such values can be in numeric units such as "0,1,2,3,..n," or similar); and the device response communication comprises digital credential data that does not have a beginning PAN digit, as defined in IS07813, equal to a numeral "4" (para [0033] device uses PIN but not PAN; para [0031] as defined by ISO/IEC 7813).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of Rosenberg in view of Yeager to include the method of communicating account related data of Bishop in order to secure customer related information (Bishop, para [0010]).

Regarding claim 34, Rosenberg in view of Yeager disclose all limitations of claim 11, but lack explicitly teaching the first communication channel comprises an NFC communication channel; the POS command communication comprises a select file command conforming to IS07816-4 protocol using a VISA AID starting with A000000003; the device response communication comprises digital credential data that does not have a beginning PAN digit, as defined in IS07813, equal to a numeral "4"; and the method further comprises formatting the digital credential data in the point-of-sale terminal into a digital credential that is identical to a static magnetic stripe card that conforms to IS07813.
In the field of RF Transaction authentication, Bishop teaches the first communication channel comprises an NFC communication channel (para [0027]-[0028] user communicates with network over a communications protocol; para [0032] wherein the communications protocol may be RFID [RFID is a type of NFC communications protocol]); the POS command communication comprises a select file command conforming to IS07816-4 protocol using a VISA AID starting with A000000003 (para [0043] storing transaction device information according to ISO 7816 file structure standards; para [0050] wherein such values can be in numeric units such as "0,1,2,3,..n," or similar); the device response communication comprises digital credential data that does not have a beginning PAN digit, as defined in IS07813, equal to a numeral "4"; and the method further comprises formatting the digital credential data in the point-of-sale terminal into a digital credential that is identical to a static magnetic stripe card that conforms to IS07813 (para [0033] device uses PIN but not PAN; para [0031] as defined by ISO/IEC 7813; para [0035]-[0036] account data is communicated by magnetic stripe format conforming to the aforementioned ISO standards).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of Rosenberg in view of Yeager to include the method of communicating account related data of Bishop in order to secure customer related information (Bishop, para [0010]).

Regarding claim 47, Rosenberg in view of Yeager disclose all limitations of claim 36, but lack explicitly teaching the repository comprises a digital database of a plurality of mobile device identifications and at least one secure element representation identifier associated with each mobile device and the repository is configured to validate the mobile device using the digital database.
In the field of RF Transaction authentication, Bishop teaches the repository comprises a digital database of a plurality of mobile device identifications and at least one secure element representation identifier associated with each mobile device and the repository is configured to validate the mobile device using the digital database (para [0031]-[0032] an account identifier may be used to validate the account using the database).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of modified Rosenberg to include the method of communicating account related data of Bishop in order to secure customer related information (Bishop, para [0010]).

Regarding claim 48, Rosenberg in view of Yeager disclose all limitations of claim 36, but lack explicitly teaching the mobile device comprises non-persistent memory for caching a cached portion of the digital credential data and the mobile device is configured to provide the cached portion to the point-of-sale terminal through the first communication channel.
In the field of RF Transaction authentication, Bishop teaches the mobile device comprises non-persistent memory for caching a cached portion of the digital credential data and the mobile device is configured to provide the cached portion to the point-of-sale terminal through the first communication channel (para [0023] information can be stored in memory elements such as look up tables and data structures [which are commonly non-persistent memory elements]; para [0036] wherein data stored in such memory elements may be account related information).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of modified Rosenberg to include the method of communicating account related data of Bishop in order to secure customer related information (Bishop, para [0010]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding claim 49, Rosenberg in view of Yeager disclose all limitations of claim 36, but lack explicitly teaching there is a plurality of command communications and a plurality of response communications over the first communication channel.
In the field of RF Transaction authentication, Bishop teaches there is a plurality of command communications and a plurality of response communications over the first communication channel (para [0027]-[0028] user communicates with network over a communications protocol; para [0032] wherein the communications protocol may be RFID [RFID is a type of NFC communications protocol]).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of Rosenberg in view of Yeager to include the method of communicating account related data of Bishop in order to secure customer related information (Bishop, para [0010]).

Regarding Claim 50, Rosenberg in view of Yeager disclose all limitations of claim 36, but do not disclose the request for the acquisition of the digital credential data and the device response communication comprise 7816-4 data.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses the request for the acquisition of the digital credential data and the device response communication comprise 7816-4 data (the communications between devices conform to the ISO 7816-4 protocol and thus comprise 7816-4 data; Par. 0043).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's feature in to modified Rosenberg's system. The motivation would have been to expedite point of sale transactions (Bishop, Par. 0006).

Regarding Claim 51, Rosenberg in view of Yeager disclose all limitations of claim 36, but do not disclose a second communication channel wherein, the repository is configured to receive a request for the digital credential data from the mobile device using the second communication channel and to send a response with at least a portion of the digital credential data to the mobile device using the second communication channel; and wherein the device command communication and the repository response communication comprise 7816-4 data.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses a second communication channel wherein, the repository is configured to receive a request for the digital credential data from the mobile device using the second communication channel (the Internet is the second communication channel; Par. 0024) and to send a response with at least a portion of the digital credential data to the mobile device using the second communication channel; and wherein the device command communication and the repository response communication comprise 7816-4 data (ISO7816 protocol is disclosed for controlling communications between the devices, thus ISO7816-4 is used; Par. 0043).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's feature in to modified Rosenberg's system. The motivation would have been to expedite point of sale transactions (Bishop, Par. 0006).

Regarding Claim 52, Rosenberg in view of Yeager disclose all limitations of claim 36, but do not disclose a second communication channel and wherein: the repository is configured to receive a request for the digital credential data from the mobile device using the second communication channel and to send a response with at least a portion of the digital credential data to the mobile device using the second communication channel; and wherein the first communication channel and the second communication channel comprise TCP/UDP/IP communication channels.
However, Bishop is in the field of expediting point of sale transactions (Par. 0006) and discloses a second communication channel and wherein: the repository is configured to receive a request for the digital credential data from the mobile device using the second communication channel and to send a response with at least a portion of the digital credential data to the mobile device using the second communication channel (the Internet is the second communication channel; Par. 0043); and wherein the first communication channel and the second communication channel comprise TCP/UDP/IP communication channels (TCP/UDP/IP is used over the Internet; Par. 0027).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Bishop's feature in to modified Rosenberg's system. The motivation would have been to expedite point of sale transactions (Bishop, Par. 0006).

Claims 16, 22, 39 & 45 lack an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Yeager and further in view of Hohle.

Regarding Claim 16, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose the repository uses ISO 7816 to extract at least a portion of the digital credential data from the paired secure element representation.
However, Hohle is in the field of facilitating commercial transactions over a network (Col. 1, lines 7-11) and discloses the repository uses ISO 7816 to extract at least a portion of the digital credential data from the paired secure element representation (card object database 116 is the repository; Col. 4, lines 13-24).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Hohle's feature in to modified Rosenberg's system. The motivation would have been to provide for the use of an internationally accepted standard (Hohle, Col. 4, lines 13-24).

Regarding Claim 22, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose the first communication channel comprises a TCP/UDP/IP communication channel.
However, Hohle is in the field of facilitating commercial transactions over a network (Col. 1, lines 7-11) and discloses the first communication channel comprises a TCP/UDP/IP communication channel (the TCP/IP connection is the communication channel; Col. 8, lines 51-63).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Hohle's feature in to modified Rosenberg's system. The motivation would have been to allow for usage of the Internet to facilitate commercial transactions (Hohle, Col. 8, lines 51-63).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding Claim 39, Rosenberg in view of Yeager disclose all limitations of claim 36, but does not disclose the repository uses IS07816 to extract the at least a portion of the digital credential data from the paired secure element representation.
However, Hohle is in the field of facilitating commercial transactions over a network (Col. 1, lines 7-11) and discloses a repository that uses IS07816 to extract at least a portion of the digital credential data from a paired secure element representation (card object database 116 is the repository; Col. 4, lines 13-24).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Hohle's feature in to modified Rosenberg's system. The motivation would have been to provide for the use of an internationally accepted standard (Hohle, Col. 4, lines 13-24).

Regarding Claim 45, Rosenberg in view of Yeager disclose all limitations of claim 36, but do not disclose the mobile device is remote from the point-of-sale terminal and the first communication channel comprises a TCP/UDP/IP communication channel.
However, Hohle is in the field of facilitating commercial transactions over a network (Col. 1, lines 7-11) and discloses the mobile device is remote from the point-of-sale terminal the first communication channel comprises a TCP/UDP/IP communication channel (the TCP/IP connection is the communication channel; Col. 8, lines 51-63).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Hohle's feature in to modified Rosenberg's system. The motivation would have been to allow for usage of the Internet to facilitate commercial transactions (Hohle, Col. 8, lines 51-63).

Claim 23 lacks an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Yeager and further in view of Tang.

Regarding Claim 23, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose the authenticating step comprises matching a gesture signal with a valid gesture signal.
However, Tang is in the field of detecting and eliminating fraud in a transaction (Abs.) and discloses the authenticating step comprises matching a gesture signal with a valid gesture signal (the secret gesture, is the gesture signal; Par. 0029).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Tang's feature in to modified Rosenberg's system. The motivation would have been to provide security for the user by preventing fraud (Tang, Par. 0029).

Claim 27 lacks an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Yeager and further in view of Garcia Ruano.

Regarding Claim 27, Rosenberg in view of Yeager disclose all limitations of claim 11, but does not disclose the mobile device is remote from the repository and the method further comprises: sending through a second communication channel using a Secure Socket Layer and TCP/UDP/IP protocol from the mobile device to the repository a device command communication; and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises the at least a portion of the digital credential data.
However, Garcia Ruano is in the field of using a mobile phone as a payment device (Abs.) and discloses the mobile device is remote from the repository and the method further comprises: sending through a second communication channel using a Secure Socket Layer and TCP/UDP/IP protocol from the mobile device to the repository a device command communication (the Internet is the second channel, and a secure connection using TCP/IP protocol is used; Par. 0155); and sending through the second communication channel a repository response communication from the repository to the mobile device wherein the repository response communication comprises the at least a portion of the digital credential data (the response is sent from the operations processor; Par. 0066).
It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Garcia Ruano's feature in to modified Rosenberg's system. The motivation would have been to allow for secure transactions over the Internet (Garcia Ruano, Par. 0155).

Claim 35 lacks an inventive step under PCT Article 33(3) as being obvious over Bishop in view of Pond.

Regarding claim 35, Bishop teaches a system for acquiring digital credential data using a mobile device comprising: a point-of-sale terminal having a NFC interface using IS07816-4 protocol to transmit a request for the digital credential data and to receive digital credential data (para [0043]-[0045] RFID transaction device [wherein RFID is an NFC interface] is used to store and communicate account and transaction-related information, and conforms to ISO7816 file structure standards); and a mobile device having a NFC interface using IS07816-4 protocol configured to (para [0027] input device being a cellular phone, para [0043] conforming to the ISO7816 standards) receive the request from the point-of-sale terminal for an acquisition of the digital credential data, interpret the request from the point-of-sale within an operating system of the mobile device and within an application running in that operating system (Fig. 2, items 210-218, send and receiving requests [pertaining to transactions] between POS and Acquirer; para [0043] wherein one of the communicating devices may be a cellular phone), but does not disclose sending the digital credential data to the point-of-sale terminal using IS08916-4 protocol generated from an application running in an operating system in the mobile device.
However, Pond is in the field mobile device payment methods, and Pond teaches sending the digital credential data to the point-of-sale terminal using IS08916-4 protocol generated from an application running in an operating system in the mobile device (col. 7, ln. 15-40, data can be communicated according to ISP 7816 standards).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the RF transaction system of Bishop to include the use of the ISO8916 protocol of Pond in order to use a structure that is based on a standard (Pond, col. 7, ln. 29-33).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/041670

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Claim 46 lacks an inventive step under PCT Article 33(3) as being obvious over Rosenberg in view of Yeager and further in view of Pond.

Regarding claim 46, Rosenberg in view of Yeager disclose all limitations of claim 36, but lack explicitly teaching the mobile device is configured for generating a gesture signal and to authenticate to the repository by matching the gesture signal with a valid gesture signal. In the field mobile device payment methods, Pond teaches the mobile device is configured for generating a gesture signal and to authenticate to the repository by matching the gesture signal with a valid gesture signal (col. 12, ln. 1-13, RFID transponder interrogator window may also be comprised of an array of interrogators and other sensors to allow for gestures to be used as input into the Commerce system. If a certain hand gesture, for example is valid, then the commerce system would authorize a transaction).
It would have been obvious to one having ordinary skill in the art at the time of the invention to modify the system of modified Rosenberg to include the use of specific gestures of Pond in order to provide more security for the user (Pond, col. 12, ln. 10-11).

Claims 53-54 lack novelty under PCT Article 33(2) as being anticipated by Bishop.

Regarding claim 53, Bishop teaches a repository for secure element representations (para [0044] database 116 may be in communication with a transaction device for communicating account related information) comprising: at least one secure element reader (para [0045] RFID transaction device 102 and RFID reader 104); a plurality of secure element representations disposed proximate to the secure element reader (para [0045] RFID transaction device 102 communicates with RFID reader 104; wherein each of these devices may be based on elements as per para [0023]); a server disposed proximate to the secure element reader, the server having a multitasking processor to communicate with the plurality of secure element representations through the secure element reader and conduct a plurality of command/response time-wise overlapping sessions with the plurality of secure element representations (para [0044) the RFID device and reader communicate secure account and transaction related information according to interrogation signaling methods [wherein RFID is a type of NFC protocol]); and an internet connection to the server wherein each of the secure element representations is addressable over the internet (para [0024]-[0025] transaction methods performed using internet).

Regarding claim 54, Bishop discloses all limitations of claim 53 and further discloses the plurality of secure element representations is selected from the group consisting of hardware representations, virtual hardware representations, and a combination thereof (para [0023] the elements representing the data can be any number of hardware and/or software components configured to perform to specified functions).

Claims 1-56 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 67979.W2	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2012/053129	International filing date *(day/month/year)* 30 August 2012 (30.08.2012)	Priority date *(day/month/year)* 30 August 2011 (30.08.2011)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant YEAGER, C., Douglas		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 11 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 04 March 2014 (04.03.2014)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Nora Lindner e-mail: pt05.pct@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: JAMES PALMER
LUEDEKA NEELY GROUP, P.C.
P.O. BOX 1871
KNOXVILLE, TN 37901-1871

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	16 NOV 2012
Applicant's or agent's file reference 67979.W2	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2012/053129	30 August 2012	30 August 2011

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - G06Q 20/00 (2012.01)
USPC - 705/64

Applicant YEAGER, C.

1. This opinion contains indications relating to the following items:

- [x] Box No. I Basis of the opinion
- [ ] Box No. II Priority
- [ ] Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- [ ] Box No. IV Lack of unity of invention
- [x] Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- [ ] Box No. VI Certain documents cited
- [ ] Box No. VII Certain defects in the international application
- [ ] Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	24 October 2012	Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (July 2011)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

   ☐ on paper

   ☐ in electronic form

   b. (time)

   ☐ in the international application as filed

   ☐ together with the international application in electronic form

   ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	2-29	YES
	Claims	1	NO
Inventive step (IS)	Claims	8-11, 15-16, 19-23, 28-29	YES
	Claims	1-7, 12-14, 17-18, 24-27	NO
Industrial applicability (IA)	Claims	1-29	YES
	Claims	None	NO

2. Citations and explanations:

Claim 1 lacks novelty under PCT Article 33(2) as being anticipated by Yeager (US 2007/0075133 A1).

Regarding claim 1, Yeager discloses a method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction (method, system and computer-readable medium for radio frequency identification device, title; the adapter is connected to a host device like a mobile phone to construct a mobile device capable of financial transactions, Fig. 3 and [0027]-[0029], in which the mobile device communicates with a terminal such as the Mastercard PayPass system, Fig. 5 and [0030]) comprising:
using a remote permanent cryptographic key to calculate an expected cryptogram that is expected to comprise at least a portion of the digital credential data (a secret key on a remote server, Fig. 6 and [0031]-[0032], which is a remote permanent cryptographic key, is used to calculate an expected cryptogram that comprises, and hence encrypts, digital credential data such as credit card information, [0022]), wherein the remote permanent cryptographic key is persistently stored at a remote source that is remote from the mobile device (the secret key is stored in a remote location that is remote from the mobile device/host, Fig. 6 and [0031]-[0032]) and wherein the mobile device does not access a duplicate local permanent cryptographic key persistently stored locally to the mobile device (the mobile device/host also shares the secret key, Fig. 6 and [0031]-[0032], and the mobile device/host does not access the secret key; only the server and the adapter have access to the secret key, because they're the only two entities that know the key, [0031]-[0032]);performing an interrogation between the point-of-sale terminal and the mobile device (the adapter is connected to a host device like a mobile phone to construct a mobile device capable of financial transactions, Fig. 3 and [0027]-[0029], in which the mobile device communicates with a terminal such as the Mastercard PayPass system, Fig. 5 and [0030]) comprising: sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device requesting the digital credential data (the digital credential data is credit card information, [0022], and is requested by the terminal to the mobile device in order to facilitate a transaction, Fig. 9 and [0036]); and
sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal comprising the expected cryptogram as the at least a portion of the digital credential data (credenttial data is sent to a server via the terminal, Fig. 9 and [0036], in which the credential data is encrypted using the encryption key for the purpose of communication between an adapter and server, [0031]-[0032], and hence the encrypted credential data is the expected cryptogram comprising at least a portion of the digital credential data); wherein the financial transaction is authorized (the transaction is determined to be successful or not, hence authorized, and then the user account may then be updated by deducting the transaction amount, Fig. 9 and [0036]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Claim 2 lacks an inventive step under PCT Article 33(3) as being obvious over Yeager (US 2007/0075133 A1) and further in view of Smets et al (US 2006/0022033 A1), hereinafter referred to as Smets.

Regarding claim 2 of claim 1, Yeager further discloses a further step that precedes the performing the interrogation step, the further step comprising:
sending the remote permanent cryptographic key to the mobile device from the remote source (the secret key is chosen by the server sent from a server to the mobile host, [0031]-[0032]); and transiently caching the remote permanent cryptographic key in the mobile device as a cached transient permanent cryptographic key (the server may change the secret key after each transaction, [0031]-[0032], and hence the secret key is actually a temporary session key or cached transient permanent cryptographic key, [0031]-[0032]), sending the expected cryptogram calculated, at least in part, from the cached transient cryptographic key (communications is encrypted with the session key, and hence results in an expected cryptogram, [0031]-[0032]).
Yeager does not adequately disclose:
the step of sending through the communication channel the at least one POS command communication comprises sending unpredictable data; the step of sending through the communication channel the at least one POS command communication comprises sending a request for an expected cryptogram that is expected to be calculated by the mobile device, at least in part, from the unpredictable data; and the step of sending through the communication channel the at least one device response communication from the mobile device to the point-of-sale terminal comprises sending the expected cryptogram calculated, at least in part, from the unpredictable data. However, Smets is also in the field of electronic payment systems (abstract) and further teaches:
the step of sending through the communication channel the at least one POS command communication comprises sending unpredictable data (an unpredicatable number UN, which is unpredictable data, is sent from the POS terminal, Fig. 5 and [0026]); the step of sending through the communication channel the at least one POS command communication comprises sending a request for an expected cryptogram that is expected to be calculated by the mobile device, at least in part, from the unpredictable data (using the unpredictable number, a mobile device, such as the card, calculates a CVC3 number based on a portion of the unpredictable number and transmits the result to the terminal, Fig. 5 and [0026]); and the step of sending through the communication channel the at least one device response communication from the mobile device to the point-of-sale terminal comprises sending the expected cryptogram calculated, at least in part, from the unpredictable data (the resulting cryptogram CVC3 is calculated in part from the unpredictable number and transmitted to the terminal, Fig. 5 and [0026]). Therefore, it would have been obvious to a person having ordinary skill in the art wherein: the step of sending through the communication channel the at least one POS command communication comprises sending unpredictable data; the step of sending through the communication channel the at least one POS command communication comprises sending a request for an expected cryptogram that is expected to be calculated by the mobile device, at least in part, from the unpredictable data; and the step of sending through the communication channel the at least one device response communication from the mobile device to the point-of-sale terminal comprises sending the expected cryptogram calculated, at least in part, from the unpredictable data, as taught by Smets, in which the mobile device may also comprise a mobile card device for an electronic payment system of Royyuru. This combination increase the security of the electronic payment system in the event that an unauthorized person obtains the CVC3 number for a particular transaction (Smets [0010]).

Claims 3-6, 24, 26 lack an inventive step under PCT Article 33(3) as being obvious over Royyuru et al (US 2010/0185545 A1), hereinafter referred to as Royyuru and further in view of Brown et al (US 2009/0006262 A1), hereinafter referred to as Brown.

Regarding claim 3, Royyuru discloses a method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction (dynamic primary account number and unique key per card, title; financial transaction authorization, abstract, Fig. 3) comprising:
performing an interrogation between the point-of-sale terminal and the mobile device (in NFC technology, a mobile device is in communication with a point-of-sale POS terminal, [0022]) comprising: sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device (commands and responses are communicated between a terminal and mobile device in order to perform a financial transaction, [0057]), the at least one POS command communication comprising (a) a request for the digital credential data that is expected to comprise an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data, and, at least in part, from a permanent cryptographic key (transaction requests comprise credit card numbers, which is digital credential data, and is calculated from a unpredictable number, which is unpredictable data, and the message is encrypted with a key, [0049]-[0051]) and (b) the unpredictable data (an unpredictable number UN, which is unpredictable data, is generated by the NFC terminal and transmitted to the device, [0057]); and sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal (commands and responses are communicated between a terminal and mobile device in order to perform a financial transaction, [0057]), the at least one device response communication comprising at least a portion of the digital credential data that comprises an unexpected cryptogram (encrypting the credit card numbers with an unpredictable number will result in a dynamic PAN, which is an unexpected cryptogram, [0049]-[0051]), wherein the financial transaction is authorized (the financial transaction may be authorized or denied, [0050]).
Royyuru may not adequately describe that an unexpected cryptogram is substituted in place of the expected cryptogram. However, Brown is also in the field of financial transactions (abstract) and further teaches cryptogram substitution of one cryptogram for another cryptogram ([0134]-[0141]; Once the data format is known, it is effectively a template, like an invoice sheet, in which there is a location where information like a price of an item is shown. This is similar to substituting one value for another value given that the data is of the same type, like price). Therefore, it would have been obvious to a person having ordinary skill in the art that: an unexpected cryptogram is substituted in place of the expected cryptogram, as taught by Brown, in a financial transaction system of Royyuru. This combination allows for a a less expensive microcontroller to be required (Brown [0134]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Regarding claim 4 of Claim 3, Royyuru further discloses wherein the unpredictable data comprises an unpredictable number (unpredictable number UN, [0049]-[0051] and [0057]).

Regarding claim 5 of Claim 3, Royyuru discloses that the unpredictable data may be any number, such as a random number, a time of day, or another number generated or received by the presentation instrument ([0051]). Royyuru does not specifically state wherein the unpredictable data comprises a transaction amount. However, it is notoriously well known that a transaction amount is a number. A transaction amount is also unpredictable in the sense that the number is not known as opposed to a credit card number which is already predetermined. Therefore, it would have been obvious to a person having ordinary skill in the art for the unpredictable data of Royyuru to comprise any number, such that the number may be a transaction amount, because a transaction amount is a number that is unpredictable and changes with each transaction.

Regarding claim 6 of Claim 3, Royyuru further discloses a mobile device preparation step that precedes the performing an interrogation step, the mobile device preparation step comprising sending critical data from a remote source to a mobile device, wherein the critical data comprises data used to formulate at least a portion of the digital credential data as a local portion of the digital credential data (before a financial transaction may occur, the mobile device needs to be programmed with a key and information regarding a primary account number PAN that can be mapped to a dynamic PAN, [0004]-[0006] and [0047]-[0048]).

Regarding claim 24 of Claim 3, Royyuru further discloses an authorizing step that follows the step of performing an interrogation, the authorizing step comprising sending the unpredictable data from the mobile device to a remote application system (the mobile device may send the unpredictable number to a remote system as Track-1 data, because the unpredictable number is contained in the Track-1 data format, [0049]-[0051]).

Regarding claim 26 of Claim 3, Royyuru further discloses wherein the communication channel comprises a near-field communication channel (communication via NFC technology is used, [0002]-[0003] and [0022]).

Claims 7, 17 lack an inventive step under PCT Article 33(3) as being obvious over Royyuru et al (US 2010/0185545 A1), hereinafter referred to as Royyuru and further in view of Brown et al (US 2009/0006262 A1), hereinafter referred to as Brown, and further in view of Smets et al (US 2006/0022033 A1), hereinafter referred to as Smets.

Regarding claim 7 of Claim 6, Royyuru may not specifically state: wherein the local portion of the digital credential data comprises a predetermined cryptogram, which is calculated without the use of the unpredictable data, as the unexpected cryptogram. However, Smets is also in the field of electronic payment systems (abstract) and further teaches: wherein the local portion of the digital credential data comprises a predetermined cryptogram (a bitmap is created which serves as a type of template that defines data that is used or unused/discretionary, [0013]-[0014], and hence the bitmap creates a cryptogram that is predetermined and as-of-yet unexpected), which is calculated without the use of the unpredictable data, as the unexpected cryptogram (the unpredictable number is not placed in the bitmap yet, because it is considered to be discretionary, [0026] and [0031]-[0033]). Therefore, it would have been obvious to a person having ordinary skill in the art: wherein the local portion of the digital credential data comprises a predetermined cryptogram, which is calculated without the use of the unpredictable data, as the unexpected cryptogram, as taught by Smets, in an electronic payment system of Royyuru. This combination allows for financial transaction data to be standardized (Smets [0013]-[0014]).

Regarding claim 17 of Claim 3, Royyuru may not specifically state: creating a predetermined cryptogram on the mobile device as the unexpected cryptogram; wherein the predetermined cryptogram is calculated without the use of the unpredictable data; and sending at least a portion of the predetermined cryptogram from the mobile device to a remote application system. However, Smets is also in the field of electronic payment systems (abstract) and further teaches: creating a predetermined cryptogram on the mobile device as the unexpected cryptogram (a bitmap is created which serves as a type of template that defines data that is used or unused/discretionary, [0013]-[0014], and hence the bitmap creates a cryptogram that is predetermined and as-of-yet unexpected); wherein the predetermined cryptogram is calculated without the use of the unpredictable data (the unpredictable number is not placed in the bitmap yet, because it is considered to be discretionary, [0026] and [0031]-[0033]); and sending at least a portion of the predetermined cryptogram from the mobile device to a remote application system (at least a portion of the cryptogram is sent from the mobile device to a remote system for authorization of the transaction, Fig. 5 and [0026]). Therefore, it would have been obvious to a person having ordinary skill in the art for: creating a predetermined cryptogram on the mobile device as the unexpected cryptogram; wherein the predetermined cryptogram is calculated without the use of the unpredictable data; and sending at least a portion of the predetermined cryptogram from the mobile device to a remote application system, as taught by Smets, in an electronic payment system of Royyuru. This combination allows for financial transaction data to be standardized (Smets [0013]-[0014]).

Claims 12-14, 18 lack an inventive step under PCT Article 33(3) as being obvious over Royyuru et al (US 2010/0185545 A1), hereinafter referred to as Royyuru and further in view of Brown et al (US 2009/0006262 A1), hereinafter referred to as Brown, and further in view of Fisher et al (US 2009/0124234 A1), hereinafter referred to as Fisher.

Regarding claim 12 of Claim 6, Royyuru may not adequately disclose: wherein the mobile device preparation step further comprises transiently storing at least a portion of the critical data on the mobile device, wherein the mobile device does not persistently store the at least a portion of critical data. However, Fisher is also in the field of payment transactions ([0011]) and further teaches: wherein the mobile device preparation step further comprises transiently storing at least a portion of the critical data on the mobile device (critical data like a cryptographic key, is transiently stored in the mobile device, because it is only valid for the duration the session, Fig. 4 and [[0016]]), wherein the mobile device does not persistently store the at least a portion of critical data (the cached key data may be flushed, and hence the mobile device does not persistently store the key, Fig.4 and [0017]-[0018]). Therefore, it would have been obvious to a person having ordinary skill in the art: wherein the mobile device preparation step further comprises transiently storing at least a portion of the critical data on the mobile device, wherein the mobile device does not persistently store the at least a portion of critical data, as taught by Fisher, in a payment transaction system of Royyuru. This combination allows for a financial transaction system that is more secure in the event that the mobile device is lost or stolen (Fisher [0013]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding claim 13 of Claim 6, Royyuru further discloses wherein the local portion of the digital credential data comprises an unpredictable cryptogram as the unexpected cryptogram (the Primary Account Number PAN, which is digital credential data, is not sent to the remote system; instead a dynamic PAN is generated and sent as the unpredictable, unexpected cryptogram, Fig. 4 and [0051]-[0055]).
Royyuru may not best disclose: wherein the unpredictable cryptogram is calculated, at least in part, using a temporary cryptographic key. However, Fisher is also in the field of payment transactions ([0011]) and further teaches: wherein the unpredictable cryptogram is calculated, at least in part, using a temporary cryptographic key (a session key, which is a temporary cryptographic key, is created for the mobile device, Fig. 3 and [0016], and the session key is used to encrypt data for the session, [0016]). Therefore, it would have been obvious to a person having ordinary skill in the art: wherein the unpredictable cryptogram is calculated, at least in part, using a temporary cryptographic key, as taught by Fisher, in a payment transaction system of Royyuru. This combination allows for a financial transaction system that is more secure in the event that the mobile device is lost or stolen (Fisher [0013]).

Regarding claim 14 of Claim 6, Royyuru further discloses wherein the mobile device preparation step further comprises:
Royyuru further discloses wherein the local portion of the digital credential data comprises an unpredictable cryptogram as the unexpected cryptogram (the Primary Account Number PAN, which is digital credential data, is not sent to the remote system; instead a dynamic PAN is generated and sent as the unpredictable, unexpected cryptogram, Fig. 4 and [0051]-[0055]).
Royyuru may not best disclose: creating a temporary cryptographic key in a remote application system wherein the remote application system is the remote source; sending at least a portion of the temporary cryptographic key from the remote application system to the mobile device as a portion of the critical data; and wherein the unpredictable cryptogram is calculated, at least in part, using the temporary cryptographic key. However, Fisher is also in the field of payment transactions ([0011]) and further teaches:
creating a temporary cryptographic key in a remote application system wherein the remote application system is the remote source (a session key, which is a temporary cryptographic key, is server-generated and created for the mobile device, Fig. 3 and [0016]); sending at least a portion of the temporary cryptographic key from the remote application system to the mobile device as a portion of the critical data (at least a portion of session key is sent from the server to the mobile device, because the session key is server generated, Fig. 3 and [0016]); and wherein the unpredictable cryptogram is calculated, at least in part, using the temporary cryptographic key (the session key is used to encrypt data for the session including cryptograms communicated during the session, [0016]). Therefore it would have been obvious to a person having ordinary skill in the art for: creating a temporary cryptographic key in a remote application system wherein the remote application system is the remote source; sending at least a portion of the temporary cryptographic key from the remote application system to the mobile device as a portion of the critical data; and wherein the unpredictable cryptogram is calculated, at least in part, using the temporary cryptographic key, as taught by Fisher, in a payment transaction system of Royyuru. This combination allows for a financial transaction system that is more secure in the event that the mobile device is lost or stolen (Fisher [0013]).

Regarding claim 18 of Claim 3, Royyuru may not adequately disclose: creating a temporary cryptographic key on the mobile device; wherein the temporary cryptographic key is used to calculate, at least in part, an unpredictable cryptogram as the unexpected cryptogram; sending at least a portion of the unpredictable cryptogram from the mobile device to a remote application system. However, Fisher is also in the field of payment transactions ([0011]) and further teaches: creating a temporary cryptographic key on the mobile device (a session key, which is a temporary cryptographic key, is created for the mobile device, Fig. 3 and [0016]); wherein the temporary cryptographic key is used to calculate, at least in part, an unpredictable cryptogram as the unexpected cryptogram (the session key is used to encrypt data for the session, [0016], and hence constitutes an unpredictable cryptogram calculated at least in part with a temporary session key); sending at least a portion of the unpredictable cryptogram from the mobile device to a remote application system (at least a portion of the cryptogram is sent to a remote server in order to conduct payment transactions, Fig. 1 and [0011]-[0013]). Therefore it would have been obvious to a person having ordinary skill in the art for: creating a temporary cryptographic key on the mobile device; wherein the temporary cryptographic key is used to calculate, at least in part, an unpredictable cryptogram as the unexpected cryptogram; sending at least a portion of the unpredictable cryptogram from the mobile device to a remote application system, as taught by Fisher, in a payment transaction system of Royyuru. This combination allows for a financial transaction system that is more secure in the event that the mobile device is lost or stolen (Fisher [0013]).

Claim 25 lacks an inventive step under PCT Article 33(3) as being obvious over Royyuru et al (US 2010/0185545 A1), hereinafter referred to as Royyuru and further in view of Brown et al (US 2009/0006262 A1), hereinafter referred to as Brown, and further in view of Buhot et al (US 2010/0207742 A1), hereinafter referred to as Buhot.

Regarding claim 25 of Claim 3, Royyuru further discloses that the POS command communication conforms to a data protocol and the device response communication conforms to a data protocol (in order to communicate, [0057] and [0037]). Royyuru lacks wherein the data protocol is the ISO 7816-4 protocol. However, Buhot is also in the field of near field communications (abstract) and further teaches the ISO 7816-4 data protocol ([0052] and [0085]). Therefore, it would have been obvious to a person having ordinary skill in the art to substitute a data protocol for the ISO 7816-4 protocol of Buhot wherein the POS command communication conforms to a data protocol and the device response communication conforms to a data protocol of Royyuru. This combination allows for an electronic payment system using NFC technology (Buhot [0018]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Claim 27 lacks an inventive step under PCT Article 33(3) as being obvious over Royyuru et al (US 2010/0185545 A1), hereinafter referred to as Royyuru and further in view of Brown et al (US 2009/0006262 A1), hereinafter referred to as Brown, and further in view of Yeager (US 2007/0075133 A1).

Regarding claim 27 of Claim 3, Royyuru does not specifically state: wherein the mobile device does not access a local persistently stored permanent cryptographic key that is expected to be used to calculate the expected cryptogram wherein the expected cryptogram is expected to be contained within the at least a portion of the digital credential. However, Yeager is also in the field of NFC devices ([0003]) and further teaches: wherein the mobile device does not access a local persistently stored permanent cryptographic key that is expected to be used to calculate the expected cryptogram wherein the expected cryptogram is expected to be contained within the at least a portion of the digital credential (a mobile device, like a mobile phone, [0027], does not actually access the keys, because the keys for encrypting the credential data are only shared between the server and adapter, Fig. 6 and [0031]-[0032]). Therefore, it would have been obvious to a person having ordinary skill in the art: wherein the mobile device does not access a local persistently stored permanent cryptographic key that is expected to be used to calculate the expected cryptogram wherein the expected cryptogram is expected to be contained within the at least a portion of the digital credential, as taught by Yeager, in a financial transaction system of Royyuru. This combination better ensures the confidentiality and security of the keys (Yeager [0031]).

Claims 8-11, 15-16, 19-23 meet the criteria set out in PCT Article 33(2)-(3), because the prior art does not teach or fairly suggest:

Regarding claim 8 creating remote unpredictable data in a remote application system wherein the remote application system is the remote source; sending the remote unpredictable data from application system to an HSM; calculating a predetermined cryptogram in the HSM; sending the predetermined cryptogram from the HSM to the remote application system; sending at least a portion of the predetermined cryptogram from the remote application system to the mobile device as a portion of the critical data; and wherein the local portion of the digital credential data comprises the predetermined cryptogram as the unexpected cryptogram.

Regarding claim 9 creating a predetermined cryptogram, which is calculated without the use of the unpredictable data, in a remote application system wherein the remote application system as the remote source; sending at least a portion the predetermined cryptogram from the remote application system to the mobile device as a portion of the critical data; and wherein the local portion of the digital credential data comprises the predetermined cryptogram as the unexpected cryptogram.

Regarding claim 10 wherein the critical data comprises a set of possible predetermined cryptograms; and the method further comprises a logical step of logically determining, in the mobile device, which of the possible predetermined cryptograms within the set of predetermined cryptograms to designate as the unexpected cryptogram; wherein the logical step is based, at least in part, on the unpredictable data; and wherein the local portion of the digital credential data comprises the designated predetermined cryptogram as the unexpected cryptogram.

Regarding claim 11: wherein the critical data comprises a set of possible predetermined cryptograms and card risk management data; and the method further comprises a logical step of logically determining, in the mobile device, which of the possible predetermined cryptograms within the set of possible predetermined cryptograms to designate as the unexpected cryptogram; wherein the logical step of is based, at least in part, on the unpredictable data or based, at least in part, on the card risk management data; and wherein the local portion of the digital credential data comprises the designated predetermined cryptogram as the unexpected cryptogram.

Regarding claim 15 wherein the critical data comprises a temporary cryptographic key; and the method further comprises a step of calculating at least one local unpredictable cryptogram that is calculated, in at least part, using the temporary cryptographic key, and, in at least part, using a calculation formula determined from a set of calculation formulas; and the method further comprises a logical step of logically determining, in the mobile device, which local unpredictable cryptogram to designate as the unpredictable cryptogram; wherein the step of logically determining a decision is made based, at least in part, on the unpredictable data; and wherein the local portion of the digital credential data comprises the designated local unpredictable cryptogram as the unexpected cryptogram.

Regarding claim 16 wherein the critical data comprises a temporary cryptographic key and card risk management data; and the method further comprises a step of calculating at least one local unpredictable cryptogram that is calculated, in at least part, using the temporary cryptographic key, and, in at least part, using a calculation formula determined from a set of calculation formulas; and the method further comprises a logical step of logically determining, in the mobile device, which local unpredictable cryptogram to designate as the unpredictable cryptogram;
wherein the logical step is made based, at least in part, on the unpredictable data or based, at least in part, on the card risk management data; and wherein the local portion of the digital credential data comprises the designated local unpredictable cryptogram as the unexpected cryptogram.

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Regarding claim 19: an authorizing step that follows the step of performing the interrogation, the authorizing step comprising: sending an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system, wherein the unexpected cryptogram comprises a predetermined cryptogram; verifying a correctness of the predetermined cryptogram by the application system
(a) by comparing the predetermined cryptogram with a previously stored reference predetermined cryptogram and
(b) without reference to the unpredictable data from the point-of-sale terminal; and sending an authorization response from the remote application system to the point-of-sale wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the predetermined cryptogram.

Regarding claim 20 an authorizing step that follows the step of performing the interrogation, the authorizing step comprising: sending an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system, wherein the unexpected cryptogram comprises an unpredictable cryptogram: verifying a correctness of the unpredictable cryptogram by the application system wherein the unpredictable cryptogram is compared with a result of an unpredictable cryptogram calculation; wherein the unpredictable cryptogram calculation is calculated using, at least in part, a temporary cryptographic key; and sending an authorization response from the remote application system to the point-of-sale wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable cryptogram.

Regarding claim 21 a corroborative authorizing step that follows the step of performing the interrogation, the corroborative authorizing step comprising: sending through a second communication channel an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system; sending through a third communication channel the unpredictable data from the mobile device to the remote application system; verifying a correctness of the unexpected cryptogram in the remote application system;
verifying a correctness of the unpredictable data in the remote application system by comparing the unpredictable data sent through the second communication channel with the unpredictable data sent through the third communication channel; sending through the second communication channel an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable data and, at least in part, by the verifying of the correctness of the unexpected cryptogram.

Regarding claim 22 a verifying a transaction amount step that follows the step of performing an interrogation and precedes the corroborative
authorizing step, the verifying a transaction amount step comprising: displaying transaction amount data to a display on the mobile device wherein the transaction amount data is at least a portion of the unpredictable data; requesting verification of the transaction amount data from a card holder by the mobile device display screen; sending the result of the requesting verification of the transaction amount data to a remote application system as input transaction amount data; and wherein the corroborative authorizing step comprises determining, at least in part, an accuracy of the result of the verification step by using the input of the transaction amount data.

Regarding claim 23 an authorizing step that follows the step of performing an interrogation, the authorizing step comprising: sending an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system, wherein the unexpected cryptogram comprises a predetermined cryptogram; verifying a correctness of the predetermined cryptogram wherein the unpredictable data from the point-of sale (a) is substituted by the application system with a previously created unpredictable data that was previously used to calculate the predetermined cryptogram; and subsequently (b) is sent with the predetermined cryptogram to the HSM for cryptogram correctness verification; and sending an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the predetermined cryptogram.

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding claim 28: A method for acquiring digital credential data by a point-of-sale terminal from a secure mobile device for authorization of a financial transaction comprising: performing an interrogation between the point-of-sale terminal and the secure mobile device comprising: sending through a communication channel at least one POS command communication from the point-of-sale terminal to the secure mobile device,
the at least one POS command communication comprising (a) a request for the digital credential data that is expected to comprise an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data, and, at least in part, from a permanent cryptographic key and (b) the unpredictable data; and sending through the communication channel at least one device response communication from the secure mobile device to the point-of-sale terminal, the at least one device response communication comprising at least a portion of the digital credential data that comprises the expected cryptogram; in a step that follows the step of performing an interrogation, a secure mobile device transmitting step comprising sending over a second communication channel the unpredictable data from the secure mobile device to a remote application system; in a step that follows the step of performing an interrogation, a point-of-sale terminal transmitting step comprising sending over a third communication channel an authorization request from the point of sale terminal to the remote application system, the authorization request comprising the expected cryptogram and the unpredictable data; in a step that follows the secure mobile device transmitting step and the point-of-sale terminal transmitting step, a corroborative authorizing step comprising: verifying a correctness of the expected cryptogram by the application system; verifying a correctness of the unpredictable data by the application system by comparing the unpredictable data sent over the second communication channel with the unpredictable data sent over the third communication channel; and sending through the third communication channel an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable data and at least in part by the verifying of the correctness of the expected cryptogram; wherein the financial transaction is authorized.

Claim 29 meets the criteria due to their dependence on novel claim 28.

The prior art, as shown below, details some of the aspects of the invention, however none of the prior art teaches all the missing limitations either alone or in combination as specified:

Royyuru et al (US 2010/0185545 A1), discloses a method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction (dynamic primary account number and unique key per card, title: financial transaction authorization, abstract, Fig. 3) comprising:
performing an interrogation between the point-of-sale terminal and the mobile device (in NFC technology, a mobile device is in communication with a point-of-sale POS terminal, [0022]) comprising: sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device (commands and responses are communicated between a terminal and mobile device in order to perform a financial transaction, [0057]), the at least one POS command communication comprising (a) a request for the digital credential data that is expected to comprise an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data, and, at least in part, from a permanent cryptographic key (transaction requests comprise credit card numbers, which is digital credential data, and is calculated from a unpredictable number, which is unpredictable data, and the message is encrypted with a key, [0049]-[0051]) and (b) the unpredictable data (an unpredictable number UN, which is unpredictable data, is generated by the NFC terminal and transmitted to the device, [0057]); and sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal (commands and responses are communicated between a terminal and mobile device in order to perform a financial transaction, [0057]), the at least one device response communication comprising at least a portion of the digital credential data that comprises an unexpected cryptogram (encrypting the credit card numbers with an unpredictable number will result in a dynamic PAN, which is an unexpected cryptogram, [0049]-[0051]), wherein the financial transaction is authorized (the financial transaction may be authorized or denied, [0050]).Royyuru may not adequately describe that an unexpected cryptogram is substituted in place of the expected cryptogram, or the verifying correctness features.

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Yeager discloses a method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction (method, system and computer-readable medium for radio frequency identification device, title; the adapter is connected to a host device like a mobile phone to construct a mobile device capable of financial transactions, Fig. 3 and [0027]-[0029], in which the mobile device communicates with a terminal such as the Mastercard PayPass system, Fig. 5 and [0030]) comprising: using a remote permanent cryptographic key to calculate an expected cryptogram that is expected to comprise at least a portion of the digital credential data (a secret key on a remote server, Fig. 6 and [0031]-[0032], which is a remote permanent cryptographic key, is used to calculate an expected cryptogram that comprises, and hence encrypts, digital credential data such as credit card information, [0022]). Yeager does not disclose the unpredictable data; and sending through the communication channel at least one device response communication from the secure mobile device to the point-of-sale terminal, the at least one device response communication comprising at least a portion of the digital credential data that comprises the expected cryptogram; in a step that follows the step of performing an interrogation, a secure mobile device transmitting step comprising sending over a second communication channel the unpredictable data from the secure mobile device to a remote application system; in a step that follows the step of performing an interrogation, a point-of-sale terminal transmitting step comprising sending over a third communication channel an authorization request from the point of sale terminal to the remote application system, the authorization request comprising the expected cryptogram and the unpredictable data; in a step that follows the secure mobile device transmitting step and the point-of-sale terminal transmitting step, a corroborative authorizing step comprising: verifying a correctness of the expected cryptogram by the application system; verifying a correctness of the unpredictable data by the application system by comparing the unpredictable data sent over the second communication channel with the unpredictable data sent over the third communication channel; and sending through the third communication channel an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable data and at least in part by the verifying of the correctness of the expected cryptogram; wherein the financial transaction is authorized.

Claims 1-29 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.

Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact

Boult Wade Tennant
Verulam Gardens
70 Gray's Inn Road
London WC1X 8BT
ROYAUME UNI

Date
06.05.15

Reference	Application No./Patent No.
PEH/P131279EP00	12827026.1 - 1955 / 2751754 PCT/US2012053129
Applicant/Proprietor	
Yeager, C., Douglas	

Communication

The extended European search report is enclosed.

The extended European search report includes, pursuant to Rule 62 EPC, the supplementary European search report (Art. 153(7) EPC) and the European search opinion.

Copies of documents cited in the European search report are attached.

☑ 0 additional set(s) of copies of such documents is (are) enclosed as well.

Refund of the search fee
If applicable under Article 9 Rules relating to fees, a separate communication from the Receiving Section on the refund of the search fee will be sent later.

Should you wish to further prosecute this application in the examination phase, your attention is drawn to the provisions of Rule 70a EPC. An invitation to respond to the extended European search report will be issued shortly (R. 70(2) EPC).

Europäisches Patentamt · European Patent Office · Office européen des brevets

The examination is being carried out on the **following application documents**

Description, Pages

1-4, 6-82	as published	
5, 5a-5k	filed in electronic form on	10-11-2014

Claims, Numbers

1-21	filed in electronic form on	10-11-2014

Drawings, Sheets

1/24-24/24	as published	

1 Cited Documents

1.1 Reference is made to the following documents; the numbering will be adhered to in the rest of the procedure.

D1 US 2011/099079 A1 (WHITE SPENCER NEIL [US])
28 April 2011 (2011-04-28)

D2 WO 01/08113 A1 (VISA INT SERVICE ASS [US]; DAVIS VIRGIL M [US]; CUTINO SUZANNE C [US];)
1 February 2001 (2001-02-01)

D3 US 2010/153721 A1 (MELLQVIST ANDERS [SE])
17 June 2010 (2010-06-17)

D4 WO 2009/017754 A1 (EBAY INC [US]; MURPHY TIMOTHY [US]) 5 February 2009 (2009-02-05)

D5 US 2002/026414 A1 (NAKAJIMA MITSURU [JP] ET AL)
28 February 2002 (2002-02-28)

Mastercard, Ex1002, p. 364

2 Amendments (Art. 123(2) EPC)

2.1 With the letter received on 10-11-2014, the applicant has filed amendments which do not appear to meet the requirements of Article 123(2), the reasons being as follows:

2.1.1 Claim 1 has been amended to include that "the at least one POS command communication conforms to a card specification". Nevertheless, the description [0116] describes that the interrogation is the one defined by a card specification and not the POS command communication. Thus, there is no basis for the POS command communication conforming to a card specification.

2.1.2 Claim 6 has been amended to include the fact that "the unexpected cryptogram comprises the predetermined cryptogram". Nevertheless, the paragraphs cited in the letter, i.e. [0116] and [0118], describe that the predetermined cryptogram refers to a type of unexpected cryptogram. Thus, there is no basis for one comprising the other.

2.1.3 Claim 11 has been amended to include the fact that "the unexpected cryptogram comprises the unpredictable cryptogram". Nevertheless, the paragraphs cited in the letter, i.e. [0116] and [0118], do not describe the unpredictable cryptogram and description [0117] describes that the unpredictable cryptogram refers to a type of unexpected cryptogram. Thus, there is no basis for one comprising the other.

2.1.4 The same reasoning applies mutatis mutandis to claims 12, 13 and 15.

2.1.5 Claims 12 and 13 also have been amended to include "calculating a plurality of unpredictable cryptograms". In the letter it is specified that there is a step of logically determining which unpredictable cryptogram to use and thus a plurality of these must be calculated using the temporary cryptographic key. Nevertheless, there are several possibilities about the origin of such cryptograms and not necessarily using the temporary cryptographic key, since there could be other unexpected cryptograms with other keys. Thus, there is no basis for such amendments.

2.1.6 Claim 14 introduces the following amendments with no apparent basis in the letter sent by the applicant: "... as a position of the critical data; wherein ... as the unexpected cryptogram".

2.1.7 Claim 15 introduces that the "unpredictable cryptogram is calculated at least in part from a temporary cryptographic key". The letter provides description [0150] as a basis, but no basis is found in that paragraph.

2.1.8 Claim 15 further introduces "sending at least a portion of the temporary cryptographic key to a remote application system". The letter provides description [0113] as a basis, but no basis is found in that paragraph.

2.1.9 Claim 15 also introduces that "the local portion of digital credential comprises an unpredictable cryptogram as the unexpected cryptogram". The letter provides as a basis the original claim 14. Nevertheless, the original claim 14 describes that "the location portion of the digital credential comprises the predetermined cryptogram as the unexpected cryptogram". Thus, there is no basis for such amendments.

2.2 All other amendments appear to meet the requirements of Article 123(2) EPC:

2.2.1 Description pages 5, 5a-5k are a copy of the original claims introduced as further aspects of the invention.

2.2.2 The rest of claim 1 has a basis on original claim 3, description [0116]-[0121] and [0132].

2.2.3 Claims 2 and 3 have a basis on original claims 4 and 5.

2.2.4 Claim 4 has a basis on original claim 6, description [0109], [0186] and [0202].

2.2.5 Claims 5 and 7 have a basis on original claims 7 and 9 and description [0116] and [0118].

2.2.6 Claims 8-10 have a basis on original claims 10-12 and description [0116].

2.2.7 Claim 16 has a basis on original claim 19 and description [0116].

2.2.8 Claim 17 has a basis on original claim 20 and description [0117].

2.2.9 Claims 18-21 have a basis on original claims 21-23 and 27 respectively.

3 Clarity and Conciseness (Art. 84 EPC)

3.1 The use of vague words, such as for instance in claim 1 "expected cryptogram" and "unexpected cryptogram", makes the reading of the claims unclear and, hence, does not meet the requirements of Article 84 EPC. These words should be amended to include the technical features which are disclosed in the description paragraphs [0116]-[0118] in order for such words to have a technical meaning.

3.2 Moreover, claims 6 and 20 contains the word HSM which is vague and unclear and thus should be amended. For the purpose of this report we will interpret it as in description [0040], being "Hardware Security Module".

3.3 It also seems that claim 19 introduces what appears to be, *prima facie*, an obvious error, i.e. "... a verifying a transaction ...", which should be corrected under Rule 139 EPC.

3.4 Independent claim 1 does not meet the requirement following from Article 84 EPC, taken in combination with Rule 43(1) and (3) EPC, that any independent claim must contain all the technical features essential to the definition of the invention because it is clear from the description on paragraphs [0007] and [0137]-[0139] that the feature of a remote application system is essential to the definition of the invention, since this is the third party which authorizes the financial transaction by verifying the correctness of the received data.

4 Novelty and Inventive Step (Art. 52(1), 54 and 56 EPC)

4.1 Taking into account the above objections and independent claim 1, the invention of the application (see [0007], [0105], [0137]-[0139] and claims 1, 18) can be summarized as:

A method for authorizing a financial transaction including a mobile device, a Point of Sale/POS and a remote application system comprising the steps of:

- Sending from the POS to the mobile device unpredictable data and a request for digital credential data;

- Sending from the mobile device to the POS a response with digital credential data, including a cryptogram;

- Sending from the mobile device to the remote application system the unpredictable data;

- Sending from the POS to the remote application system the digital credential data, including the unexpected cryptogram, and the unpredictable data;

- Sending from the remote application system to the POS an authorization to perform the financial transaction if the received data is correct.

4.2 Document D1 discloses:

A method for authorizing a financial transaction including a mobile device, a Point of Sale/POS and a remote application system ("... system for securing payment ... mobile communication device ... point of sale ... payment server ...", [0028], ref. 100, 120, 140 in figure 1; "... method for securing payment ...", [0032], ref. 400, 420, 440 in figure 4; [0038]) comprising the steps of:

Mastercard, Ex1002, p. 367

- Sending from the POS to the mobile device unpredictable data and a request for digital credential data ("... Point of sale device communicates amount to mobile communication device ...", [0028]);

Note: The request is regarded as implicit since there is a response to this communication.

- Sending from the mobile device to the POS a response with digital credential data, including a cryptogram ("... mobile communication device ... submit a payment to a POS, the payment including a payment number and an amount ...", [0032]; "... payment number is a combination of the one-time digital key and the random number ...", [0028]);

- Sending from the mobile device to the remote application system the unpredictable data ("... mobile communication ... communicates the amount ... to payment server ...", [0028]);

Note: The mobile communication only communicates the amount number to the payment server, since there is an embodiment where the payment number is routed through the POS to the payment server (see [0028]).

- Sending from the POS to the remote application system the digital credential data, including the unexpected cryptogram, and the unpredictable data ("... POS submits the payment instructions to payment server, including the payment number and the amount ...", [0032]);

- Sending from the remote application system to the POS an authorization to perform the financial transaction if the received data is correct ("... Payment server verifies the payment number and confirms the payment to POS ...", [0032]).

4.3 Thus, most of the subject-matter of claim 1 is disclosed in D1 (see [0028], [0032]) and the only difference is that the "POS command conforms to a card specification" which is a non-technical constraint that would be given beforehand to the person skilled in the art, being an engineer in the field of electronic payments (EPC Guidelines G-VII.5.4.1), which the person would use to implement it without using inventive skills.

4.3.1 Hence, the subject-matter of independent claim 1 is not inventive within the meaning of Article 56 EPC.

4.3.2 Moreover, even if the fact that the POS is expecting "an expected cryptogram" but receives an "unexpected cryptogram" is amended to provide more technical details regarding the vague wording "expected" and

Mastercard, Ex1002, p. 368

"unexpected" (see section 3.1 of this communication), this feature would still have no technical effect in the invention since the POS does not make any kind of check to the cryptogram received but rather just relays it to the remote application system to make the appropriate verification (see description [0137]), thus rendering the subject-matter of claim 1 still not inventive under Article 56 EPC.

4.4 The subject-matter of dependent claims 2-21 is not inventive under Article 56 EPC because the additional features of ...

4.4.1 claim 2 regarding the unpredictable data comprising an unpredictable number are normal design procedures to the person skilled in the art, being an engineer in the field of electronic payments;

4.4.2 claim 3 regarding the unpredictable data comprising a transaction amount are disclosed in D1 ("Point of sale device communicates amount to mobile communication device ...". [0028]);

4.4.3 claim 4 regarding a step previous to performing the interrogation are disclosed in D1 ("... payment server issues a one-time digital key to mobile communication device ...", [0032]);

4.4.4 claim 5 regarding a predetermined cryptogram not using the unpredictable data are already disclosed in D1 ("... payment number is a combination of the one-time digital key and the random number ...", [0028]), since the payment number is the unexpected cryptogram and the amount, which is not used to create the unexpected cryptogram, is the unpredictable data;

4.4.5 claims 6 and 20 regarding the use of an HSM or Hardware Security Module in the preparation step are well-known to the skilled person (e.g. see D2 abstract and D3 abstract);

4.4.6 claim 7 regarding the creation of the predetermined cryptogram in the remote system are disclosed in D1 ("... payment server issues a one-time digital key to mobile communication device ...", [0032]; "... payment server knows the one-time digital key in use ...", [0028]);

4.4.7 claims 8-9, 12-13 regarding a plurality of possible predetermined cryptograms are a normal design procedure to the skilled person;

4.4.8 claim 10 and 21 regarding storing transiently at least a portion of the critical data or not accessing a local persistently stored key is regarded as a normal design procedure especially taking into account the the one-time digital key

only has validity during the current transaction and once the current transaction has been completed the payment server issues a new one-time digital key to the mobile device ([0032]);

4.4.9 claim 11 regarding the use of a temporary cryptographic key is disclosed in D1 ("... payment server issues a one-time digital key to mobile communication device ...", [0032]; "... payment number is a combination of the one-time digital key and the random number ..." [0028]; "... the combining may include multiplying the number ...", [0028]);

4.4.10 claims 14-15 regarding generating the predetermined cryptogram or cryptographic key in the mobile device instead of the server are regarded as normal design procedure to the skilled person, since the having the one-time digital key generation algorithm in the server and sending it to the mobile device or having it in the mobile device and sending it to the server is one of several possibilities that the skilled person would use depending on the circumstances without using inventive skills;

4.4.11 claims 16-17 regarding an authorization step is disclosed in D1:

"... POS submits the payment instructions to payment server, including the payment number and the amount. Payment server verifies the payment number and confirms the payment to POS device ...", [0032];

"... payment number is a combination of the one-time digital key and the random number ...", [0028];

"... the combining may include multiplying the number ...", [0028];

taking into account that the payment number is the unexpected cryptogram and the amount, which is not used to create the unexpected cryptogram, is the unpredictable data;

4.4.12 claim 18 regarding a corroborative authorization step is disclosed in D1:

"... POS submits the payment instructions to payment server, including the payment number and the amount ..." [0032]; "... payment number is a combination of the one-time digital key and the random number ...", [0028];

"... mobile communication ... communicates the amount ... to payment server ...", [0028];

"... Payment server verifies the payment number and confirms the payment to POS device ...", [0032];

and the verification of the unpredictable data sent by the mobile device and the POS is considered a normal design procedure to the skilled person;

Mastercard, Ex1002, p. 370

4.4.13 claim 19 regarding displaying transaction amount on the mobile device is disclosed in D1 ([0033]);

5 Procedure

5.1 It is not at present apparent which part of the application could serve as a basis for a new, allowable claim. Should the applicant nevertheless regard some particular matter as patentable, an independent claim should be filed taking account of Rule 43(1) EPC. The applicant should also indicate how the subject-matter of the new claim differs from the state of the art and the significance thereof.

5.2 When filing amended claims the applicant should at the same time bring the description into conformity with the amended claims. Care should be taken during revision, especially of the introductory portion and of any statements of problem or advantage, not to add subject-matter which extends beyond the content of the application as originally filed (Article 123(2) EPC).

5.3 In order to comply with the requirements of Rule 137(4) EPC, the applicant should clearly identify the amendments made, irrespective of whether they concern amendments by addition, replacement or deletion, and indicate the passages of the application as filed on which these amendments are based (Guidelines H-III, 2.1).

5.4 According to the application of Rule 50(1) EPC in combination with Rule 49(8) EPC, no hand-written amendments by the applicant are accepted (Office Journal of the EPO 2013, 603-604).

5.5 The independent claim is not in the two-part form in accordance with Rule 43 (1) EPC, which in the present case would be appropriate, with those features known in combination from the prior art being placed in the preamble (Rule 43 (1)(a) EPC) and the remaining features being included in the characterising part (Rule 43(1)(b) EPC).

5.6 The features of the claims should be provided with reference signs placed in parentheses to increase the intelligibility of the claims (Rule 43(7) EPC). This applies to both the preamble and characterising portion (see Guidelines F-IV, 4.19).

Europäisches Patentamt
European Patent Office
Office européen des brevets

SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application Number
EP 12 82 7026

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 2011/099079 A1 (WHITE SPENCER NEIL [US]) 28 April 2011 (2011-04-28) * abstract * * figures 1,4 * * paragraph [0028] * * paragraphs [0032] - [0033] *	1-21	INV. G06Q20/00 G06Q20/02 G06Q20/20 G06Q20/32 G06Q20/38 G06Q20/40
A	WO 01/08113 A1 (VISA INT SERVICE ASS [US]; DAVIS VIRGIL M [US]; CUTINO SUZANNE C [US];) 1 February 2001 (2001-02-01) * the whole document *	1-21	H04L9/32
A	US 2010/153721 A1 (MELLQVIST ANDERS [SE]) 17 June 2010 (2010-06-17) * the whole document *	1-21	
A	WO 2009/017754 A1 (EBAY INC [US]; MURPHY TIMOTHY [US]) 5 February 2009 (2009-02-05) * the whole document *	1-21	
A	US 2002/026414 A1 (NAKAJIMA MITSURU [JP] ET AL) 28 February 2002 (2002-02-28) * abstract * * figure 12 * * paragraphs [0116] - [0123] *	1-21	TECHNICAL FIELDS SEARCHED (IPC) G06Q H04L G06F

The supplementary search report has been based on the last set of claims valid and available at the start of the search.

Place of search	Date of completion of the search	Examiner
The Hague	23 April 2015	Horat, David

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C04)

Mastercard, Ex1002, p. 372

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 12 82 7026

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on. The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

23-04-2015

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011099079 A1	28-04-2011	US 2011099079 A1	28-04-2011
		US 2013091062 A1	11-04-2013
		US 2014258133 A1	11-09-2014
WO 0108113 A1	01-02-2001	AU 6491800 A	13-02-2001
		US 7908216 B1	15-03-2011
		US 2011125638 A1	26-05-2011
		US 2012239565 A1	20-09-2012
		US 2014046746 A1	13-02-2014
		WO 0108113 A1	01-02-2001
US 2010153721 A1	17-06-2010	CN 102257507 A	23-11-2011
		EP 2359303 A1	24-08-2011
		JP 2012511761 A	24-05-2012
		KR 20110106839 A	29-09-2011
		US 2010153721 A1	17-06-2010
		WO 2010067211 A1	17-06-2010
WO 2009017754 A1	05-02-2009	US 2009037285 A1	05-02-2009
		US 2014006196 A1	02-01-2014
		WO 2009017754 A1	05-02-2009
US 2002026414 A1	28-02-2002	DE 60133701 T2	14-05-2009
		EP 1189184 A2	20-03-2002
		JP 2002074223 A	15-03-2002
		US 2002026414 A1	28-02-2002

Mastercard, Ex1002, p. 373

Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact

Boult Wade Tennant
Verulam Gardens
70 Gray's Inn Road
London WC1X 8BT
ROYAUME UNI

Date
30.04.14

Reference	Application No./Patent No.
PEH/P131279EP00	12827026.1 - 1955 PCT/US2012053129
Applicant/Proprietor	
Yeager, C., Douglas	

Communication pursuant to Rules 161(2) and 162 EPC

1. Amendment of the application (R. 161(2) EPC)

The above-mentioned international (Euro-PCT) application has entered the European phase.

Under Articles 28, 41 PCT and Rules 52, 78 PCT the application may be amended before a designated or elected Office.

In accordance with Rule 161(2) EPC, you may amend your application once within a **non-extendable period of six months** after notification of the present communication.

If filing amendments, you must identify them and indicate the basis for them in the application as filed. Failure to meet either requirement may lead to a communication from the Examining Division requesting that you correct this deficiency (R. 137(4) EPC).

The claims applicable on expiry of this period, i.e. those filed on entry into the European phase or in response to the present communication, will form the basis for the calculation of any claims fee to be paid (see page 2).

--2/

2 Claims fees under Rule 162 EPC

If the application documents on which the European grant procedure is to be based comprise more than fifteen claims, a claims fee shall be payable for the sixteenth and each subsequent claim within the period provided for in Rule 159(1) EPC.

☐ Based on the application documents currently on file, all necessary claims fees have already been paid (or the documents do not comprise more than 15 claims).

☐ All necessary fees will be/have been debited automatically according to the automatic debit order.

☑ The claims fees due for the claims 16 to 29 were not paid within the above-mentioned period.

Any outstanding claims fee, either based on the current set of claims or on any amended claims to be filed pursuant to Rule 161 EPC (see page 1), may still be validly paid within a **non-extendable period of six months** after notification of this communication (R. 162(2) EPC).

If a payment is made for only some of the claims, you must indicate for which claims it is intended. If a claims fee is not paid in due time, the claim concerned is deemed to be abandoned (R. 162(4) EPC).

If claims fees have already been paid, but on expiry of the above-mentioned period there is a new set of claims containing fewer fee-incurring claims than before, the claims fees in excess of those due under Rule 162(2), second sentence EPC will be refunded (R. 162(3) EPC).

You are reminded that the supplementary search carried out according to Article 153(7) EPC will relate only to the last set of claims applicable on expiry of the above period AND will be confined to those fee-incurring claims for which fees have been paid in due time.

The claims fee is currently

EUR 235 for the 16th and each subsequent claim up to the limit of 50
EUR 580 for the 51st and each subsequent claim

Note to users of the automatic debiting procedure
Unless the EPO receives prior instructions to the contrary, the fees for all claims incurring fees will be debited on the last day of the period for payment. For further details see the Arrangements for the automatic debiting procedure, Supplementary publication 4 - OJ EPO 2014.

Important information concerning fee amounts
Following any amendment to the Rules relating to Fees, the amount(s) mentioned in this communication may be different from the amount(s) **actually due on the date of payment**. The latest version of the Schedule of fees and expenses, published as a Supplement to the Official Journal of the EPO, is also available on the EPO website (**www.epo.org**) and can be found under **www.epo.org/schedule-of-fees**, which allows the viewing, downloading and searching for individual fee amounts, both current and previous.
Please note that procedural fees are usually adjusted every two years, on even years, with effect from 1 April.

Payments by cheque delivered or sent direct to the EPO are no longer accepted as from 1 April 2008 (see OJ EPO 2007, 626).

Mastercard, Ex1002, p. 375

Receiving Section



Mastercard, Ex1002, p. 376

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/491,922	06/08/2012	C. Douglas Yeager	Simpytapp0002US	1011

122870 7590 07/27/2015

Hanchuk Kheit LLP
258 Saint Nicholas Avenue, No. 8A
New York, NY 10027-5353

EXAMINER	
AGWUMEZIE, CHINEDU CHARLES	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
07/27/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@hanchukkheit.com

Office Action Summary	Application No. 13/491,922	Applicant(s) YEAGER, C. DOUGLAS	
	Examiner CHARLES C. AGWUMEZIE	Art Unit 3685	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *1/30/15*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-56* is/are pending in the application.

5a) Of the above claim(s) *1-35 and 53-56* is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *36-52* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *9/6/12; 11/27/12*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

4) ☐ Other: _____.

The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

Election/Restrictions

1. Claims 1-35 and 53-56 withdrawn from further consideration pursuant to 37 CFR 1.142(b), as being drawn to a nonelected Group, there being no allowable generic or linking claim. Applicant timely traversed the restriction (election) requirement in the reply filed on January 30, 2015. However Applicant's traverse is based on conclusory statement that there is no undue burden for the Examiner to conduct a substantive search of all the pending claims in the application. Examiner respectfully disagrees and reiterates that there will be serious and undue burden searching different classes/subclasses because the inventions are independent and distinct from one another and will present undue burden for examination of all claims. Accordingly the Electrion/Restriction is proper and should be maintained.

Claim Rejections - 35 USC § 103

2. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

3. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 36-52**, are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Toomer et al (hereinafter "Toomer") U.S. Patent Application Publication No. 2009/0210308 A1 in view of Loh et al (hereinafter "Loh") U.S. Patent Application Publication No. 2009/0143104 A1

5. As per **claim 36**, Toomer discloses a system for acquiring digital credential data comprising:

a mobile device (see fig. 3);

a first communication channel (see fig. 3 and associated text);

a point-of-sale terminal configured to generate a request for an acquisition of the digital credential data from the mobile device over the first communication channel as a POS command communication, and configured for receiving the digital credential data from the mobile device over the first communication channel as a device response communication ***(0056, which discloses that "The point of sale device 310 can be adapted to receive the credential 402 for the financial account from the mobile device 324 via the NFC transponder 406 and send a communication or request 403 related to the transaction that includes the credential and/or other information related to the financial account.");*** and

a repository that is remote from the point-of-sale terminal, the repository having a plurality of secure element representations and being configured to validate the mobile device and pair the mobile device with a specific secure element representation ***(0057, which discloses that "The acquirer system 312 can be adapted to maintain information 420 identifying one or more accounts 410 and 415. The information can identify one or more electronic devices authorized to use the electronic payment credential. That is, for a given account 410 and 415, the account information 420 can also include information identifying one or more devices 411-413 and 416-418 which are authorized to use the account.");*** and

wherein the mobile device is remote from the repository and is configured to

a) authenticate to the repository ***(see fig. 4; see fig. 7, which discloses device authorized? step 720);***

b) receive the POS command communication over the first communication channel ***(0056, which discloses that "The point of sale device 310 can be adapted to receive the credential 402 for the financial account from the mobile device 324 via the NFC transponder 406 and send a communication or request 403 related to the transaction that includes the credential and/or other information related to the financial account."),*** and

c) send at least a portion of the digital credential data to the point-of-sale terminal as the device response communication over the first communication channel ***(0056, which discloses that "The point of sale device 310 can be adapted to receive the credential 402 for the financial account from the mobile device 324 via the NFC transponder 406 and send a communication or request 403 related to the transaction that includes the credential and/or other information related to the financial account.").***

6. Alternatively Loh discloses a repository that is remote from the point-of-sale terminal, the repository having a plurality of secure element representations and being configured to validate the mobile device and pair the mobile device with a specific secure element representation ***(see figs. 5A and 5B; 0060, which discloses that "The wireless smart card 104 can allow pairing of other devices with the mobile communication device 108 through the Bluetooth or other personal area network by providing the key information in a secure manner."; 0065; 0067)***

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Toomer and incorporate a system comprising a repository that is remote from the point-of-sale terminal, the repository having a plurality of secure element representations and being configured to validate the mobile device and pair the mobile device with a specific secure element representation in view of the teachings of Loh in order to facilitate transaction.

7. As per **claim 37**, Toomer failed to explicitly disclose the system further comprising a second communication channel and wherein: the repository is configured to receive a request for the digital credential data from the mobile device using the second communication channel and to send a response with at least a portion of the digital credential data to the mobile device using the second communication channel.

Loh discloses the system further comprising a second communication channel and wherein: the repository is configured to receive a request for the digital credential data from the mobile device using the second communication channel and to send a

response with at least a portion of the digital credential data to the mobile device using the second communication channel (0010; 0011; 0012; 0075).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Toomer and incorporate a the system further comprising a second communication channel and wherein: the repository is configured to receive a request for the digital credential data from the mobile device using the second communication channel and to send a response with at least a portion of the digital credential data to the mobile device using the second communication channel in view of the teachings of Loh in order to facilitate transaction.

8. As per **claim 38,** Toomer further discloses the system wherein the mobile device comprises a cache memory configured to store at least a portion of the digital credential data as cached data and the mobile device is configured to send the cached data as at least a portion of the device response communication (0056)

9. As per **claim 39**, Toomer further discloses the system wherein the repository uses ISO7816 to extract the at least a portion of the digital credential data from the paired secure element representation (0049; 0054)

10. As per **claim 40**, Toomer further discloses the system wherein the mobile device is proximate to the point-of-sale terminal (see fig. 3 and associated text).

11. As per **claim 41**, Toomer further discloses the system wherein the mobile device is remote from the repository (see fig. 3 and associated text).

12. As per **claim 42**, Toomer further discloses the system wherein the point-of-sale terminal is remote from the repository (see fig. 3).

13. As per **claim 43**, Toomer further discloses the system wherein the mobile device is remote from the repository and the point-of-sale terminal is remote from the repository and the digital credential data comprises Track Data (see fig. 3 and associated text).

14. As per **claim 44**, Toomer further discloses the system wherein first communication channel comprises a near-field communication channel (see fig. 4 and associated text)

15. As per **claim 45**, Toomer further discloses the system wherein the mobile device is remote from the point-of-sale terminal and the first communication channel comprises a TCP/UDP/IP communication channel (0041; 0060).

16. As per **claim 46**, Toomer further discloses the system wherein the mobile device is configured for generating a gesture signal and to authenticate to the repository by matching the gesture signal with a valid gesture signal (0056).

17. As per **claim 47**, Toomer further discloses the system wherein the repository comprises a digital database of a plurality of mobile device identifications and at least one secure element representation identifier associated with each mobile device and the repository is configured to validate the mobile device using the digital database (see fig. 4 and associated text).

18. As per **claim 48**, Toomer further discloses the system wherein the mobile device comprises non-persistent memory for caching a cached portion of the digital credential data and the mobile device is configured to provide the cached portion to the point-of-sale terminal through the first communication channel (0056).

19. As per **claim 49**, Toomer further discloses the system wherein there is a plurality of command communications and a plurality of response communications over the first communication channel (0056).

20. As per **claim 50**, Toomer further discloses the system wherein the request for the acquisition of the digital credential data and the device response communication comprise 7816-4 data (0056).

21. As per **claim 51**, Toomer failed to explicitly disclose the system further comprising a second communication channel and wherein: the repository is configured to receive a request for the digital credential data from the mobile device using the

second communication channel and to send a response with at least a portion of the digital credential data to the mobile device using the second communication channel; and wherein the device command communication and the repository response communication comprise 7816-4 data.

Loh discloses the system further comprising a second communication channel and wherein: the repository is configured to receive a request for the digital credential data from the mobile device using the second communication channel and to send a response with at least a portion of the digital credential data to the mobile device using the second communication channel; and wherein the device command communication and the repository response communication comprise 7816-4 data (0010; 0011; 0012; 0075).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Toomer and incorporate a system further comprising a second communication channel and wherein: the repository is configured to receive a request for the digital credential data from the mobile device using the second communication channel and to send a response with at least a portion of the digital credential data to the mobile device using the second communication channel; and wherein the device command communication and the repository response communication comprise 7816-4 data in view of the teachings of Loh in order to facilitate transaction.

22. As per **claim 52**, Toomer failed to explicitly disclose the system further comprising a second communication channel and wherein: the repository is configured to receive a request for the digital credential data from the mobile device using the second communication channel and to send a response with at least a portion of the digital credential data to the mobile device using the second communication channel; and wherein the first communication channel and the second communication channel comprise TCP/UDP/IP communication channels

Loh discloses the system further comprising a second communication channel and wherein: the repository is configured to receive a request for the digital credential data from the mobile device using the second communication channel and to send a response with at least a portion of the digital credential data to the mobile device using the second communication channel; and wherein the first communication channel and the second communication channel comprise TCP/UDP/IP communication channels (0010; 0011; 0012; 0075)

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the system of Toomer and incorporate the system further comprising a second communication channel and wherein: the repository is configured to receive a request for the digital credential data from the mobile device using the second communication channel and to send a response with at least a portion of the digital credential data to the mobile device using the second communication channel; and wherein the first communication channel and the second communication

channel comprise TCP/UDP/IP communication channels in view of the teachings of Loh in order to facilitate transaction.

Conclusion

23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Charles C. Agwumezie whose number is **(571) 272-6838**. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin Hewitt can be reached on **(571) 272 – 6709**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/CHARLES C AGWUMEZIE/
Primary Examiner, Art Unit 3685
July 22, 2015

Notice of References Cited	Application/Control No. 13/491,922	Applicant(s)/Patent Under Reexamination YEAGER, C. DOUGLAS	
	Examiner CHARLES C. AGWUMEZIE	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2009/0210308 A1	08-2009	Toomer et al.	705/16
*	B	US-2007/0156436 A1	07-2007	Fisher et al.	705/1
*	C	US-2009/0075592 A1	03-2009	Nystrom et al.	455/41.1
*	D	US-2009/0143104 A1	06-2009	Loh et al.	455/558
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 February 2001 (01.02.2001)

PCT

(10) International Publication Number
WO 01/08113 A1

(51) International Patent Classification[7]: G07F 19/00

(21) International Application Number: PCT/US00/19984

(22) International Filing Date: 21 July 2000 (21.07.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/359,083 22 July 1999 (22.07.1999) US

(71) Applicant *(for all designated States except US)*: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; 900 Metro Center Boulevard, Foster City, CA 94404 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **DAVIS, Virgil, M.** [US/US]; 1121 Runnymead Drive, Los Altos, CA 94024 (US). **CUTINO, Suzanne, C.** [US/US]; 431 Arkansas Street, San Francisco, CA 94107 (US). **REID, Margaret** [GB/US]; 970 Chestnut Street, #11, San Francisco, CA 94109 (US). **HOFFMAN, Steve, R.** [US/US]; 293 Trenton Circle, Pleasanton, CA 94566 (US).

(74) Agent: **WEAVER, Jeffrey, K.**; Beyer Weaver & Thomas, LLP, P.O. Box 130, Mountain View, CA 94042-0130 (US).

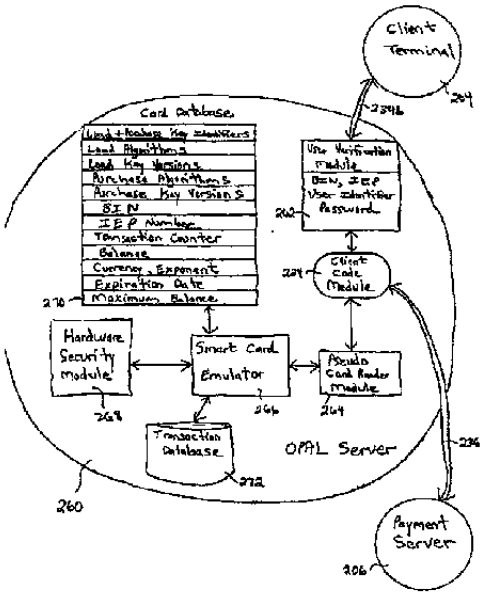
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

[Continued on next page]

(54) Title: INTERNET PAYMENT, AUTHENTICATION AND LOADING SYSTEM USING VIRTUAL SMART CARD



and replies to the bank server.

(57) Abstract: A system (250) loads, authenticates and uses a virtual smart card for payment of goods and/or services purchased on-line over the Internet. An online purchase and load (OPAL) server (260) includes a virtual smart card data base (270) that has a record of information for each smart card that it represents for a user at the behest of an issuer. The server includes a smart card emulator (266) that emulates a smart card by using the card data base and a hardware security module (268). The emulator interacts with a pseudo card reader module (264) in the server that imitates a physical card reader. The server (260) also includes a client code module (224) that interacts with the pseudo card reader and a remote payment (206) or load server (862). A pass-through client terminal (204) presents a user interface and passes information between the OPAL server and a merchant server (208), and between the OPAL server and a bank server (860). The Internet (202) provides the routing functionality between the client terminal and the various servers. A merchant advertises goods on a web site (208). A user uses the client terminal (204) to purchase goods and/or services from the remote merchant server (208). The payment server (206) processes, confirms and replies to the merchant server. The payment server is also used to authenticate (206') the holder of a virtual card who wishes to redeem loyalty points from a merchant. To load value, the client terminal requests a load from a user account at the bank server (860). The load server (862) processes, confirms

WO 01/08113 A1

— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNET PAYMENT, AUTHENTICATION AND LOADING SYSTEM USING VIRTUAL SMART CARD

FIELD OF THE INVENTION

The present invention relates generally to a payment and loading system using a computer network. More specifically, the present invention relates to a payment and loading system for a virtual smart card using an open network such as the Internet.

BACKGROUND OF THE INVENTION

With the explosive growth in the Internet over the past several years and the rapid increase in the number of consumers with access to the World Wide Web, there has been a great deal of interest in the development of electronic commerce on the Internet. Traditional financial transactions are being transformed. In particular, possibilities for the use of smart cards are expanding.

Also termed chip cards, integrated circuit cards, memory cards or processor cards, a smart card is typically a credit card-sized plastic card that includes one or more semiconductor integrated circuits. A smart card can interface with a point-of-sale terminal, an ATM, or with a card reader integrated with a computer, telephone, vending machine, or a variety of other devices. The smart card may be programmed with various types of functionality such as a stored-value application, a credit or debit application, a loyalty application, cardholder information, etc. Although a plastic card is currently the medium of choice for smart cards, it is contemplated that a smart card may also be implemented in a smaller form factor, for example, it may attach to a key chain or be as small as a chip module. A smart card may also be implemented as part of a personal digital assistant, telephone, or take a different form.

A smart card contains a hardware encryption module for performing a variety of encryption algorithms. Encryption may also be performed in software. *Applied Cryptography*, Bruce Schneier, John Wiley & Sons, Inc., 1996 discusses suitable encryption algorithms and is hereby incorporated by reference. Various mechanical

Mastercard, Ex1002, p. 393

and electrical characteristics of a smart card and aspects of its interaction with a card reader device are described in *Smart Card Handbook*, W. Rankl and W. Effing, John Wiley & Sons, Ltd., 1997, which is incorporated herein by reference.

One possible use of a smart card by a consumer is illustrated in FIG. 1. FIG. 1 illustrates an environment 100 useful for issuing smart cards and reconciling transactions performed with such a card. A terminal supplier 102 builds the equipment used by a service provider 104 to provide goods and/or services to consumers having a smart card at a service payment terminal 50. Card Supplier 106 contracts with an integrated circuit manufacturer and a card manufacturer for integrated circuits and plastic card bodies, then embeds the integrated circuits into the cards and initializes them with a serial number. It then delivers the cards to card issuer 108. In conjunction with clearing and administration system 110, card issuer 108 personalizes new cards and then transfers these cards to individuals (cardholders 112). The cardholder may then charge the card with value prior to use. Alternatively, the card may come with value already loaded. Cardholder 112 may then use the card at a service payment terminal 50 to purchase goods and/or services from service provider 104. Terminal 50 then debits the value from the card, thus creating a service payment. System 110 may be implemented using VisaNet, an existing global clearing and settlement system provided by Visa International Service Association of Foster City, California.

Periodically, all transactions are sent in a data file from terminal 50 via an acquirer 114 to clearing and administration system 110 along with accumulated service payment batches from other terminals. Based upon this collection data, clearing and administration system 110 then receives money from card issuer 108 that had originally come from cardholder 112. Clearing and administration system 110 then transfers a lump sum to acquirer 114 using a suitable settlement service (such as one provided by Visa International) to pay the various service providers having a relationship with acquirer 114. Based upon the previous collection data, acquirer 114 then transfers an appropriate amount of money to each service provider 104 reflecting the value of the goods and/or services that that service provider had provided that day to cardholders based upon deductions from their smart cards.

Mastercard, Ex1002, p. 394

A consumer typically uses such a service payment terminal 50 in a face-to-face environment in order to purchase goods in a store or directly from the terminal itself. Service payment terminal 50 can be an attended device or it can be integrated into a self-service device such as a vending machine or public telephone. For example, the service payment terminal may be incorporated into a soda machine in order to dispense sodas to a customer in which the customer pays by inserting the smart card. Or, the service payment terminal may be a point-of-sale terminal such as is found at a check-out counter where a consumer inserts his smart card in order to purchase goods.

Such a service payment terminal 50 allows a consumer to use a smart card for the payment of goods and/or services, generates a payment result from a transaction, and bundles individual payment results into a collection for transfer to a clearing and administration system, which then transfers funds that had been debited from a consumer's smart card to the merchant whose goods and/or services had been purchased from the terminal.

Thus as described above, a variety of goods or services may be purchased using a smart card from a merchant having a service payment terminal on the premises. In addition, a consumer with a smart card may purchase goods or services from a merchant over the Internet using a technique such as described in U.S. patent application No. 08/951,614 by Davis et al., filed October 16, 1997, entitled "Internet Payment Using Smart Card" which is incorporated by reference.

In order to purchase something, however, the card must be loaded with value first. Value can be loaded onto a stored-value card in a variety of ways. It may be inconvenient for a consumer to load value onto his or her smart card. A consumer must physically travel to a bank or other institution that has an automated teller machine (ATM) or other similar device in order to load value on to his or her smart card. The consumer can insert money into the machine and have a corresponding value put onto the smart card, the consumer can use a debit card to deduct value from the consumer's account at the bank for transfer to the card, or a credit card can be used as the source of funds to be transferred to the smart card. In either case, the consumer must travel to the bank to load value. Further creating difficulty is that not

Mastercard, Ex1002, p. 395

all banks or other financial institutions have such a machine for loading value onto a consumer's smart card.

A technique to allow a user to conveniently and easily load value onto a smart card over the Internet is described in U.S. patent application No. 09/070,488 by Davis et al., filed April 30, 1998, entitled "Internet Loading System Using Smart Card" which is incorporated by reference. It is desirable in some situations, however, to be able to use such payment and loading systems without having a physical smart card.

The successful development of such systems described above is somewhat dependent on the deployment of two hardware components new to the mass consumer market: smart cards and smart card readers (either stand alone or integrated with some form of personal electronic device such as a mobile telephone or computer keyboard). Both represent relatively new technology which raises the issues of reliability, cost, market acceptance and distribution. Although the above-described systems could technically be implemented, the lack of a large number of smart cards and card readers in public use raises certain infrastructure difficulties.

As mentioned above, the above-described systems have many benefits for electronic commerce. As cash may not be an option in many situations, the above systems offer a compelling solution for merchants selling products or services on-line that in the physical world might have low monetary value. The deployment of such systems, however, is hampered by lack of smart cards and smart card readers. This problem is further exasperated by the fact that the card reader market is not well developed from a standards perspective raising the potential for significant interoperability issues. Simply put, a practical problem exists in that without large numbers of smart cards and card readers in use, there is no great demand from consumers, and hence it is more difficult to convince merchants to use such systems.

Therefore, it would be desirable to have a technique that would quickly and easily allow consumers and merchants to use the above-described system, but without the need for physical smart cards and smart card readers to be distributed and installed. Such a technique would provide a fast, inexpensive alternative for users of the above-described systems to address the electronic market opportunity. Such a technique would also allow merchants and issuers to establish a market presence that

Mastercard, Ex1002, p. 396

would facilitate the acceptance of smart cards and card readers when those hardware components become more readily available.

SUMMARY OF THE INVENTION

To achieve the foregoing, and in accordance with the purpose of the present invention, an online purchase and load (OPAL) server is disclosed that implements virtual smart cards. The present invention complements the above-described Internet payment and loading systems by providing software emulation of smart cards and smart card readers. Advantageously, other components of the Internet payment and loading systems (such as the merchant server and payment server) and the techniques for processing payment and load transactions may remain the same. Use of the OPAL server will be transparent to merchants on the Internet. In one embodiment, a smart card and its associated card reader are emulated on a remotely-located OPAL server computer, thus obviating the need for physical smart cards and smart card readers. The existing client terminal acts as a pass-through device that is transparent to a user, a merchant server or a bank server.

This enhancement to Internet payment and loading systems provides many advantages. For example, the present invention accelerates the adoption of the systems in electronic markets by circumventing the cost and distribution issues associated with physical cards and card readers. When infrastructure to support physical smart cards and card readers is developed, the present invention can be replaced using the hardware approach and/or be used in conjunction with the actual hardware. The enhanced system of the present invention also provides a mechanism to address the low value (less then $10.00) electronic commerce market in a rapid manner using an infrastructure that is easily scaleable. By remaining integrated with the hardware-based approach, the present invention provided the means to accelerate development of the previously described Internet payment and loading systems and to create a base of consumers that may be converted to the hardware approach when the required hardware is more widely available.

Furthermore, the present invention is secure in that the cryptographic functions normally performed within a smart card are performed securely within the remote OPAL server that may be under the control of an issuing bank or a trusted

Mastercard, Ex1002, p. 397

third party. A further advantage of the present invention is that value may be credited to a consumer's account (i.e., the virtual smart card that is being emulated) quickly and easily by the OPAL server internally. A special load server is not necessarily required, but may be used.

In addition to the above advantages of an OPAL server, use of a virtual smart card is extremely advantageous for small dollar amount transactions. Often, consumers are reluctant to use, and merchants are reluctant to accept, credit card transactions for small dollar amounts. For the consumer and the merchant dealing with many of these small transactions can be a bookkeeping headache and may not be worth the expense. A merchant may also be unlikely to accept a credit card for a small dollar amount transaction because of the service fees per transaction. By permitting the use of a virtual card to make purchases over the Internet for small dollar amounts, a merchant may very well be able to begin charging for goods and/or services that he had been providing for free in the past. The invention works well with purchases of under about $10.00, although purchases of any amount may be made. A merchant is also provided a method to recover costs of services not previously charged for, and is provided immediate access to an existing, and rapidly growing, consumer base. Furthermore, the present invention integrates into an existing clearing and settlement system meaning that the merchant need not implement nor become familiar with new procedures for reconciliation of transactions.

Furthermore, a merchant need only make a minimal investment in time and money to take advantage of the present invention and to accept payments over the Internet. The merchant need not engage in the development of complex software or accounting procedures. Thus, smaller merchants will especially benefit from the present invention. By establishing a business relationship with an acquirer and incorporating standard merchant software, a merchant is ready to begin selling goods and/or services from his web site. Because a virtual smart card with a stored-value application is used, the payment server and the OPAL server perform the details of and provide security for the transaction and a merchant is relieved from having to control and keep track of a transaction. From a merchant's point of view, the merchant knows that a consumer desires to purchase an item and that a cost has been

Mastercard, Ex1002, p. 398

transmitted to the consumer, thus, when the merchant receives a confirmation message, the merchant may release the item to the consumer. The merchant need not be concerned about security nor be responsible for authenticating a card nor for determining a balance on the card.

In an authentication embodiment, a consumer may wish to access any of a variety of Web servers in order to redeem frequent flyer miles, award points, etc., that he or she has accumulated as part of a loyalty program. In this embodiment, a consumer has accumulated points through any of a variety of programs with airlines, restaurants, rental car companies, hotels, banks, credit or debit card issuers, telephone or other communication company, etc. Often the consumer wishes to redeem these points to receive free airline tickets, meals, car rental, overnight stays, prizes, awards, discounts, or other benefits. It is important to the airline (or other company) to be able to authenticate that the person trying to redeem points is the actual person who owns the points. By accessing a Web server associated with the particular program, this embodiment of the invention allows the consumer to use a virtual card in the OPAL server to authenticate that he or she is the true owner of the points and to receive benefits from the program.

In another embodiment of the present invention, a loading technique allows the consumer to conveniently load value on to his or her virtual card from any suitable device via an open network such as the Internet. A consumer is allowed to use any suitable computer at the home, office or elsewhere in order to connect to his bank or other financial institution. Using appropriate message integrity, value is transferred from the bank to the consumer's virtual card. At the same time, the corresponding value is transferred from the bank to the virtual card issuer through existing networks for later settlement with a merchant from whom the consumer purchases goods or services. Advantageously, this embodiment makes use of an existing clearing and settlement system for eventual settlement of the transaction between the merchant and the card issuer. Thus, a consumer may conveniently load value on to his or her virtual card while a high level of security is maintained.

From the consumer's perspective, this loading embodiment operates in a fashion similar to loading a physical card at an ATM machine, except that the consumer need not insert cash or an additional debit or credit card, nor need travel to

Mastercard, Ex1002, p. 399

a bank. The loading functionality is distributed across the Internet between the OPAL server, a bank server holding the consumer's account, and a load server with a security module. All of these entities may be physically remote from one another with router functionality being provided by the Internet.

To complement the above embodiments, an existing clearing and settlement system is used to reconcile the transaction and to pay the appropriate parties once the value has been spent. Advantageously, a new system and methodology for reconciling transactions need not be developed or implemented. The pre-existing clearing and settlement system is used which greatly simplifies implementation of the present invention. A participating bank need not implement or become familiar with new procedures for reconciliation of transactions.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention, together with further advantages thereof, may best be understood by reference to the following description taken in conjunction with the accompanying drawings in which:

FIG. 1 is a block diagram of a prior art clearing and administration system useful for reconciling financial transactions received from a service payment terminal.

FIG. 2 illustrates a system for payment over the Internet using a smart card.

FIG. 3 illustrates a system for payment over the Internet using a virtual smart card according to an embodiment of the invention.

FIG. 4 illustrates in greater detail the online purchase and load (OPAL) server of FIG. 3.

FIG. 5 illustrates in detail a payment embodiment of the present invention.

FIG. 6 illustrates another payment embodiment of the present invention in which the security card releases earlier.

Mastercard, Ex1002, p. 400

FIG. 7 illustrates yet another payment embodiment of the present invention having fewer round trip messages between the OPAL server and payment server.

FIG. 8 illustrates still another payment embodiment of the present invention in which the merchant server compares virtual card signatures.

FIG. 9 illustrates an added encryption layer useful for embodiments of the present invention.

FIG. 10 is a flowchart describing a user's perspective of a virtual card purchase transaction using the present invention.

FIGS. 11A-11D are a flowchart describing the processing of a user purchase using an embodiment of the present invention.

FIG. 12 is a flowchart describing the alternative embodiment of FIG. 6.

FIG. 13 is a flowchart describing the alternative embodiment of FIG. 7.

FIG. 14 is a flowchart describing the alternative embodiment of FIG. 8.

FIGS. 15A and 15B are a flowchart describing the added security layer of FIG. 9.

FIG. 16 illustrates a system for authentication using a virtual card according to another embodiment of the invention.

FIG. 17 illustrates a system for loading value onto a virtual card according to another embodiment of the invention.

FIGS. 18A-18D are a flowchart describing the loading of a user's virtual card using an embodiment of the invention.

FIGS. 19 and 20 illustrate a computer system 900 suitable for implementing embodiments of the invention.

Mastercard, Ex1002, p. 401

DETAILED DESCRIPTION OF THE INVENTION

FIG. 2 illustrates symbolically an internet payment system 200 using a smart card that is in accordance with U.S. patent application No. 08/951,614 referenced above; such a system serves as a background for an introduction to the present invention of FIG. 3.

TRANSACTION WITH PHYSICAL SMART CARD

Shown is Internet 202, a client terminal 204, a payment server 206 and a merchant server 208. Local cardholder functions including a consumer card interface, display and accept/cancel options are performed at client terminal 204. Payment functions including security card control, data store and use of a concentration point are performed by payment server 206. The presentation and eventual delivery of goods and/or services by a merchant are performed under control of merchant server 208. Internet 202 performs routing functions between each entity. It should be appreciated that Internet 202 may take the form of the Internet currently in use, or may also be any other open network implemented using any combination of computer, telephone, microwave, satellite, and/or cable networks.

Basically, client terminal 204 controls the interaction with a consumer and interfaces to card reader 210 which accepts a smart card having a stored-value application. Payment server 206 communicates directly with a terminal 214 or through a concentrator that handles any number of terminals each having a security card 218. Payment server 206 also communicates with concentration point 68 for transmission of transaction data to a clearing and settlement system. Database 223 stores all suitable information passing through payment server 206 for each transaction. Use of such a database allows any number of merchants (or merchant servers) to use payment server 206 for transactions. Payment server 206 controls payment functions such as handling the attached terminals, managing database 223 and collection functions. Merchant server 208 is a site that has contracted with an acquirer to accept smart card transactions as payments for goods and/or services purchased over the Internet.

Smart card 5 may take a variety of forms and is useful in many situations where it is desirable to store monetary value on a card that a consumer may use. In general,

Mastercard, Ex1002, p. 402

smart card 5 is any card or similar device able to store a value that is decremented when the card is used. The card may be purchased complete with a stored-value or value may later be added to the card by a consumer. Such cards may also have their value replenished.

Smart card 5 may also perform a variety of functions in addition to simply storing value. Such a card may serve debit, credit, prepayment, and other functions. Such a card typically includes information such as a bank identifier number, a sequence number, a purchase key, a load key, an update key, an expiration date, a transaction counter, etc., in addition to a running balance.

Smart card 5 may include an encryption module in order to provide a variety of security precautions. By way of example, security precautions may include simple PIN numbers, biometrics, simple algorithms, or sophisticated algorithms such as the Data Encryption Standard (DES) or Rivest, Shamir, Adelman (RSA) encryption. The card is thus able to use these precautions to verify consumers, card readers, etc., to validate security cards and/or to provide a unique signature. Preferably card 5 includes any number of keys known to the card issuer that are used during the course of a payment or load transaction to generate signatures for validation of the stored-value card, validation of the security card or module, and validation of the system itself.

Client terminal 204 is any suitable device for interacting with card 5 and for communicating over a network to a payment server and a merchant server. By way of example, client terminal 204 may be a mainframe computer, a work station, a personal computer, a set top box, a kiosk, or any type of service payment terminal that a consumer might use to purchase goods and/or services. Furthermore, client terminal 204 may also be embodied in any portable device such as a laptop computer, a cellular telephone (including GSM telephones), or any variety of a personal digital assistant (PDA). Card reader 210 is any suitable interface device that functions to transfer information and commands between client terminal 204 and card 5.

Client terminal 204 includes client code module 224 and card reader module 226. Reader module 226 may be implemented using any suitable software and libraries for communicating with card reader 210 and its actual implementation will

Mastercard, Ex1002, p. 403

depend upon the type of card reader used. Client module 224 controls communication between the client terminal, the card reader, the payment server and the merchant server. Client module 224 may be implemented using any suitable code. In one embodiment of the invention, client module 224 is implemented using a combination of "C" code and a Java applet. The applet is also supplemented with parameters from an HTML page sent from the merchant server. It is contemplated that Java code works well for implementing the modules on the client, payment and merchant servers because it is platform independent, and could even replace the "C" and "C++" code used.

Client module 224 is also responsible for controlling displays to the consumer and for the interaction between the card and the card reader. The module also builds the draw request message after receiving all of the start-up information from the card and the amount of the purchase from the merchant server.

Payment server 206 includes payment code module 228 and terminal interface 230. As with client terminal 204, payment server 206 may be implemented using any suitable computer. By way of example, a personal computer works well. There may be one payment server for each merchant server or a single payment server may service any number of merchant servers. Alternatively, there may be multiple payment servers for a single merchant. In addition, payment server 206 need not be remote from merchant server 208 but may be located at the same site and have a different Internet address, or the payment server and the merchant server may even be implemented on the same computer. Payment server 206 is designed to facilitate the communication between the consumer's smart card and a terminal's security card.

Payment module 228 may be implemented using any suitable code. By way of example, payment module 228 is implemented using a combination of "C" code, "C++" code and Java code. Payment module 228 is, in one specific embodiment, a multi-threaded process that can service multiple concurrent client applet transactions on demand. The module is responsible for controlling all interactions with terminal 214 including the transaction collection function. For individual transactions, payment module 228 controls the message flows and logs interim results. When an applet connects with payment server 206, it creates a transaction thread to support the transaction through its life cycle. Each thread, in turn, assigns a terminal for

Mastercard, Ex1002, p. 404

communication. Having a one-to-one correspondence between transaction threads and terminals has been found to provide desirable results.

Terminal interface 230 is any suitable set of software and libraries for communicating with a terminal 214 either directly or through a terminal concentrator. The actual implementation of terminal interface 230 will depend upon the type of terminal used. A terminal such as 214 may be any suitable terminal such as are known in the art. By way of example, an iq Delta 2010 terminal made by Schlumberger has been found to provide desirable results. Such a terminal supports a variety of commands originating from the terminal interface. These commands emulate the normal responses from a smart card to a security card should both be located in the same service payment terminal. The actual security card commands are held in the terminal while the terminal performs the tasks necessary to simulate the presence of a smart card. Alternatively, the emulation of the card commands can be done by the payment server using the terminal as a card reader, or may even be performed by client terminal 204.

Security card 218 is any suitable security card such as are known in the art (often referred to as a Purchase Secure Application Module--PSAM). In other embodiments, the functionality of security card 218 can be replaced by a hardware security module (HSM), could be implemented in hardware within the payment server, or could even be implemented in software.

By way of example, security card 218 is a removable credit card-sized smart card that is programmed to process and store data relating to financial transactions. Security card 218 contains a microchip embedded in the card that enables the card to authenticate and to validate the consumer's smart card. If a consumer's smart card is accepted by the security card, and the smart card contains sufficient value, the security card guarantees that the merchant providing goods and/or services will receive payment according to the amount deducted from the smart card. In a preferred embodiment, the security card also contains DES and public key purchase security keys and authenticates the smart card during a purchase transaction and secures the payment and collection totals. A security card also stores signature algorithms for all smart cards in use. A security card may also contain a transaction identifier for the current transaction, a financial sum of all transactions remaining to

Mastercard, Ex1002, p. 405

be settled, a session key, and master keys for all smart cards in use. Further, the security card may contain generations of keys, blocked card indicators, date of last update, multiple card programs, different currency rates and additional security.

Concentration point 68 is a staging computer that communicates with a payment server to collect batches of purchase transactions. The concentration point then sends these transaction batches to a clearing and settlement system for processing. Once processed, batch acknowledgments, along with other system updates, are sent back.

Merchant server 208 includes a merchant code module 232. Merchant server 208 may be implemented upon any suitable computer capable of communicating with and presenting information to consumers over the Internet. Merchant code module 232 may be implemented using any suitable code. By way of example, merchant module 232 may be implemented using a combination of Perl, HTML, and Java code. Merchant server 208 is typically a generic web server customized for the merchant's business. Merchant server 208 may include databases, CGI scripts and back-office programs that produce HTML pages for an Internet user.

A brief discussion of the flow of a transaction now follows. During a financial transaction, client terminal 204 and merchant server 208 exchange information 234 via Internet 202. Each transaction initiated by a consumer has a transaction identifier created at the merchant server; a merchant identifier unique to the payment server is also available from the merchant server. Client module 224 and the payment server also use this unique transaction identifier for tracking and logging information about the transaction. Merchant server 208 generates a unique identification of the transaction, completes other required parameters, encrypts as appropriate, and builds an HTML page and sends it to the client terminal. Client code module 224 interacts (235) with smart card 5 and builds a draw request message containing related card information, the purchase amount, and other information supplied by the merchant server.

Client terminal 204 then communicates (236) with payment server 206 by first forwarding the draw request to the payment server. Payment server 206 verifies the transaction to determine if it is a valid transaction from a known merchant. The

Mastercard, Ex1002, p. 406

transaction is logged into the payment server's transaction database 223. Upon completion of a transaction, payment server 206 builds a result message containing the identification of the transaction and signs it. The message is then routed to merchant server 208 via client terminal 204. Merchant server 208 then validates the result message. After determining that the transaction was successful, merchant server 208 creates an HTML page for the purchased information and sends it to client terminal 204. Alternatively, the merchant may also deliver purchased goods to the consumer at this point. It is also possible for the payment server and the merchant server to communicate information (238) directly between themselves. Preferably, as client terminal 204 has already established communication with the merchant server and the payment server, links 234 and 236 are used to exchange information between the payment server and the merchant server, rather than establishing a new link 238.

TRANSACTION WITH VIRTUAL SMART CARD

FIG. 3 illustrates an Internet payment and loading system 250 according to one embodiment of the present invention. Similar to FIG. 2, system 250 includes client terminal 204, payment server 206 and merchant server 208. System 250 dispenses with the need for card reader 210 and smart card 5; their functionality now being contained within on-line purchase and load (OPAL) server 260.

Client code module 224 is now functionally part of OPAL server 260 instead of being part of client terminal 204. Further, the functionality of card reader module 226 of FIG. 2 is now included within client code module 224 to allow communication with pseudo card reader module 264. Also, the user interface functionality of client code module 224 is transferred to a client terminal module 290 of client terminal 204. In this embodiment, pass-through client module 290 serves to "pass through" communications between merchant server 208 and OPAL server 260. As such, communications 234 of FIG. 2 are split into communications 234a and 234b.

OPAL server 260 effectively replaces the need for a physical smart card and physical card reader within system 250. To achieve this goal, OPAL server 260 implements a pseudo card reader module 264 and smart card emulator 266 in software (as described in more detail below in FIG. 4). A card database 270 stores information representing "virtual" smart cards in use within the system. Card

Mastercard, Ex1002, p. 407

emulator 266 interacts with card database 270 and a hardware security module (HSM) 268 to effectively replace the physical smart card and reader. Thus, client code module 224 may be implemented as before and be unaware that it is interacting with a software emulation of a smart card rather then with a physical smart card.

OPAL server 260 stores the same data used in the physical cards in its database and handles incoming commands from load or payment servers to increment or decrement a "card" balance as appropriate. Important data is stored in encrypted form and all functions that require a change to important data or the generation or checking of signatures is performed in HSM 268. Preferably, OPAL server 260 resides at an issuer's site or at its designated processor. It is contemplated that one such server may support multiple issuers provided appropriate safeguards are in place to partition data.

In an alternative embodiment, client terminal 204 does also include a card reader 210 and a smart card 5. In this embodiment, included in client terminal 204 is also client code module 224 in addition to pass-through client module 270. In this alternative embodiment, system 250 may operate in either of two modes. According to the present invention, the system may operate without using a physical smart card by using the emulation contained within OPAL server 260. Concurrently, or at a later date when smart cards and readers are more common, system 250 is then easily upgradeable to make use of the physical card and reader attached to client terminal 204.

FIG. 4 illustrates OPAL server 260 of Figure 3 in greater detail. OPAL server 260 communicates with client terminal 204 through user verification module 262 and with payment server 206 over link 236. OPAL server 260 emulates a physical smart card through the use of pseudo card reader module 264, smart card emulator 266, hardware security module (HSM) 268 and card data base 270.

Card database 270 is a database implemented in any suitable format and contains a record of information for each virtual smart card in use within the system. Preferably, card database 270 includes the information shown for each virtual smart card in use and thus helps to simulate a physical smart card. Preferably, an identifier such as a user name, password or some combination is used as an index into database

Mastercard, Ex1002, p. 408

270 in order to identify the appropriate virtual card for loading, debiting or authentication. Also, it is preferable that the information contained in the database is stored in an encrypted form for security. In one embodiment, the database is implemented in Sybase.

Each record in database 270 stores a variety of information for a virtual smart card: load and purchase keys identifiers, card and issuer certificates, load algorithms, load key versions, purchase algorithms, purchase key versions, a bank identification number (BIN), an IEP number, a transaction counter, a balance, a currency and exponent, an expiration date and a maximum balance. Load and purchase key identifiers indicate which keys should be used. Although all keys may be stored within HSM 268, in one embodiment the keys are stored within database 270 as well, with the exception of the HSM master key which is stored in HSM 268.

Load algorithms are identifiers that identify which cryptographic algorithm of HSM 268 is to be used for the verification and generation of signatures S1, S2, and S3 during a load. Load key version is an identifier identifying which version of a key shall be used for the generation or verification of a particular load signature. Purchase algorithms and purchase key versions perform a similar function during a purchase.

A six-digit BIN in combination with the ten-digit IEP forms a sixteen-digit identification number that uniquely identifies a particular virtual smart card. This identification number is also known as an OPAL card identifier. Preferably, each BIN, or card range, has a single maximum balance and currency for all of its virtual cards. A transaction counter counts all the transactions for a particular smart card. The balance keeps track of the value for the particular card; currency and exponent information provide further details on the balance. Expiration date provides an expiration date for the card. The maximum balance provides a maximum for the virtual card, or could also indicate a maximum balance for all virtual cards associated with a BIN.

Hardware security module (HSM) 268 is used to facilitate cryptographic processing. HSM 268 typically stores secret keys and encryption algorithms, performs cryptographic functions on secret data and generates signatures. As is

Mastercard, Ex1002, p. 409

known in the art, HSM 268 is generally a tamper-proof device which uses some level of physical security measures to protect the sensitive information inside. HSM 268 may be any security module used in the industry, such as a RACAL HSM Model RG7000, or similar to the security box attached to automatic teller machines. In alternative embodiments, HSM 268 may be implemented on a smart card within a card reader, on a series of smart cards, may be implemented on any suitably secure computer, or may be implemented in software.

HSM 268 performs the role of an encryption module of a physical smart card in addition to other tasks. In a physical smart card, various data elements such as balance and currency are contained securely within the smart card. In the embodiment shown, however, such data elements are not stored within HSM 268 but are stored on server 260 in card data base 270. For such important information, preferably these data elements are stored in an encrypted form in database 270. Thus, HSM 268 performs the additional task of receiving encrypted card data (such as transaction counter, balance, etc.) from data base 270 via emulator 266, decrypting the card data, performing any cryptographic functions upon the data, and then encrypting the data and sending it back out to be stored in card data base 270. For example, if the card balance is to be reduced, the encrypted balance is sent from data base 270 to HSM 268 where is decrypted, reduced, and then finally encrypted again before it is returned to data base 270.

HSM 268 also performs cryptograph functions related to signatures used within the system, such as signatures S1, S2 and S3. Signature S1 is used during a load operation and typically is generated by the smart card. Signature S2 is used during a load or purchase operation and is generated by the issuer or a payment server. Signature S3 is generated by the smart card on occurrence of a load or debit and is the final signature after the card has either loaded value onto, or debited value from, itself. In the present invention, HSM 268 performs these functions that are normally handled by a smart card because no physical smart card is present. HSM 268 is used to generate signatures S1 and S3 and verify signature S2 for a load operation, and is used to verify signature S2 and generate S3 for a purchase operation. HSM 268 may also perform other cryptographic functions that would normally be performed by a physical smart card.

Mastercard, Ex1002, p. 410

Transaction database 272 records information regarding transactions that occur such as a debit or a load, and may be implemented in a similar fashion as database 223. Also known as a history database, database 272 includes a purchase table (log full transactions and timestamps) and a load table (log full transactions, funding request/response and timestamps).

Pseudo card reader module 264 is a software module that performs the functionality of a physical card reader so that emulation of a smart card is transparent to client code module 224. Card reader module 264 accepts actual card reader commands from client code module 224 and, instead of using them to drive a physical card reader, places them into a format to communicate with smart card emulator 266 that is emulating a smart card. Thus, an existing application programming interface (API) used by client code module 224 to communicate with a smart card may continue to be used. In an alternative embodiment, card reader module 264 and emulator 266 may be collapsed into a single function block although this may require modification of the commands issued by client code module 224.

User verification module 262 allows OPAL server 260 to identify which user is logged on to the system and is desiring to access a virtual card in card database 270. Preferably, module 262 provides a login procedure that requires a secret user identifier and password from each user. A combination of this user identifier and password is then used as an index into card database 270 to identify the record that represents the virtual smart card for that user. User verification module 262 may also include the OPAL card identifier (BIN and IEP number) for the user, the funding account and its expiration date, and address information for address verification during the funding portion of the load transaction. An address verification system may compare billing information from an authorization to that on file to assure that the real cardholder is making the transaction.

Smart card emulator 266 emulates a physical smart card by accepting and passing incoming card commands from card reader module 264 and determining actions to perform. In the course of performing these actions, emulator 266 handles the interface to HSM 268, fetches data from, and stores data to, card database 270. For example, upon receiving a command to debit a card, emulator 266 fetches the balance from the appropriate record in database 270 and transfers the encrypted

Mastercard, Ex1002, p. 411

balance to HSM 268 to be decrypted and decremented. Once the new balance is encrypted by HSM 268, emulator 266 receives the new balance and stores it back in the appropriate record in database 270.

Once an action has been performed, emulator 266 generates a simulated smart card response that is then relayed via card reader module 264 and client code module 224 to payment server 206. Preferably, emulator 266 generates card commands that appear as if they have been generated by a physical smart card, thus making emulation of the smart card transparent to the rest of the system. Emulator 266 also updates transaction database 272 at appropriate steps in the processing of a debit or a load.

In addition to debiting or loading a virtual card in card database 270, OPAL server 260 is able to credit a virtual card if the card was debited by mistake. In other words, once a card has been debited to make a payment, OPAL server 260 is able to recover that value and credit the virtual card in the card database if necessary. For example, if a transaction fails and value has been taken off the card, but no value has been credited to a particular payment server, the system is able to credit the virtual card in the card database to replace the lost value. Such an operation is different from a formal load command in that a user's card is being credited for a value that had earlier been taken off the card.

USER PERSPECTIVE OF AN INTERNET TRANSACTION

FIG. 10 is a flowchart describing an embodiment of the present invention from a user's perspective such as may occur with the embodiment of the invention shown in FIG. 3. In step 502, a user sets up his or her virtual card within the system. In one embodiment, a physical card in the possession of the user is used to provide some of the information requested by the OPAL server. The user accesses OPAL server 260 over the Internet using an OPAL sign-on URL to access user verification module 262. A screen is presented to the user which requests that the user enter his or her user identifier, a funding account number, the CVV2 (card verification value), expiration date of that account, billing address, electronic mail address, and a chosen password. (The card verification value is a 3-digit value on the signature panel of a card used internationally for fraud deterrence.) Preferably, the first time the user

Mastercard, Ex1002, p. 412

identifier is entered it is in the clear, however, when the identifier is entered by the user subsequently for a transaction it appears masked on the screen so as to be kept secret. User verification module 262 then presents a screen to the user indicating that a confirmation will be sent to the user's electronic mail address. The user then logs out.

Later, an electronic mail confirmation is sent that contains a one-time logon password. The user receives the electronic mail and begins the setup process by logging on to the URL of OPAL server 260 and entering his or her user identifier and one-time password for checking by user verification module 262. Once these are verified, the user is prompted to change the one-time password to a new user-selected password. User verification module 262 then assigns a unique identification number ("OPAL card identifier") to the user.

During this session or at a later time, the user loads value onto the virtual card in step 504. Loading may be accomplished in many different manners. In preferred embodiments, loading is performed by either the loading embodiment discussed in FIGS. 17 and 18A-D, or by the alternative loading embodiment. In another alternative embodiment, a virtual card may come pre-loaded with a certain amount when an account is set up, i.e., the balance in database 270 is positive for a particular record. Other techniques for loading may also be used.

In step 506 the user accesses the merchant server web site via communication link 234a over the Internet. This access of a web site may be performed in any suitable fashion such as by using any commercially available web browser. Once at the merchant web site, the user is prompted to choose payment via either a physical smart card or via the virtual smart card of the present invention. If the user chooses payment via a physical smart card, purchase may proceed as described in U.S. patent application No. 08/951,614, which is hereby incorporated by reference. If the user chooses the virtual card, the user is prompted for his or her user identifier (which preferably is masked on screen) and password which is verified by OPAL server 260.

Next, in step 508 the user browses the merchant web site and selects goods and/or services for purchase from the merchant using the web site interface that the merchant has provided. The user then selects an appropriate button on the merchant

Mastercard, Ex1002, p. 413

web site to indicate what the user wishes to purchase. Next, in step 510 the user receives a total sale amount from merchant server 208, a current balance from OPAL server 260 and is directed to actuate a button on the web site indicating that the user wishes to proceed with the purchase using the virtual card.

In step 512 an embodiment of system 250 (such as is shown in FIG. 5, for example) processes the user order by way of payment server 206, OPAL server 260, terminal 214 and security card 218. In step 514 the user's virtual smart card is debited by the total sale amount and the user receives a "debited" message at the user's terminal. This message is optional if the system is designed so as to not inform the user of this debit. In step 516 the user receives a confirmation message from the merchant server indicating that the transaction has been completed. The user may now download the purchased information and/or receive a receipt for goods and/or services to be rendered or delivered from the merchant at a later date. In step 518 the merchant, via a clearing and settlement system, receives payment to its bank account for the goods and/or services rendered by way of information collected from the payment server. In one embodiment of the invention, an existing clearing and settlement system is used, as well as an existing methodology for transferring information from a security card for later reconciliation. This use of an existing "back end" allows the present invention to be implemented more quickly and less expensively.

DETAILED PAYMENT TRANSACTION FLOW

FIG. 5 illustrates a detailed embodiment of Internet payment and loading system 250 having client terminal 204, payment server 206, merchant server 208 and online purchase and load (OPAL) server 260. A security card 218 inside terminal 214 is in communication with payment server 206. Not shown for simplicity in this figure are other elements of the system shown in FIGS. 3 and 4. One embodiment of a technique by which a financial transaction may be completed over the Internet using a virtual smart card will now be described using the flowchart of FIGS. 11A through 11D with reference to FIG. 5. It should be appreciated that a wide variety of terminology may be used to describe message flow throughout system 250 in lieu of the terms "Draw request", "Debit IEP", "Debit response", and "Debit result" used below.

Mastercard, Ex1002, p. 414

Initially, a suitable web browser of client terminal 204 is used by the user to access a merchant server web site as indicated at 302. In step 602, the user selects goods and/or services from the merchant site and indicates to the site that the user wishes to purchase these items using a virtual smart card as indicated at 304. In step 604 the merchant server receives this request for a virtual card transaction.

In step 606 the merchant server builds an HTML page that includes the following parameters: the total cost of the transaction as determined by the merchant server; the type of currency being used; the port and IP address of the payment server; a unique transaction identifier used by both the payment server and the merchant server to track a transaction; and a unique merchant identifier assigned to the merchant by the acquirer and known to the payment server. Other information may also be included such as the currency's exponent, a status URL address of the merchant server used for communication from the client terminal, and a merchant server generated key and other security information to ensure the identity of the merchant server and the integrity of the message. Other process related information such as software release level, encryption methodology and keys may also be conveyed. Once this page has been built, the page is sent 306 to the requesting client browser and triggers the loading of a client terminal module (in this example a Java applet) in the client terminal.

Some browsers may not allow an applet to invoke a dynamic link library (DLL) due to security reasons. In an embodiment of the present invention, the client terminal applet along with any DLLs needed are preloaded on the client terminal. Then, the merchant server is allowed to invoke the client terminal applet and DLLs dynamically to circumvent this security precaution. In an alternative embodiment, the client applet is signed to ensure its authenticity and integrity.

The client terminal module 290 then displays a screen containing the amount provided by the merchant and requests that the user authorize the amount by entering their user identifier (which preferably is masked on screen) and password. Once entered, client terminal module 290 routes the purchase request 307 (including purchase parameters from the merchant server, user identifier and password) to OPAL server 260. OPAL server 260 then validates the user identifier and password with user verification module 262.

Mastercard, Ex1002, p. 415

In step 608 client code module 224 of OPAL server 260 then interacts with pseudo card reader module 264 to build a draw request message for later transmission 310 to payment server 206. It should be noted that at this point two types of emulation are occurring. Unlike a prior art payment service terminal that would include both a smart card and a security card in close physical proximity, OPAL server 260 neither includes a physical smart card nor a security card. The physical card is represented as a virtual card in a record of card data base 270, while security card 218 is attached to a remote payment server. Thus, as previously described in FIG. 2, client code module 224 will emulate commands that a security card would issue to build the draw request, while pseudo card reader module 264, smart card emulator 266 and data base 270 emulate a physical smart card.

In one embodiment of the invention, client code module 224 loads a local DLL, makes an API call to that library, which in turn makes a call to another DLL that finally makes a call to pseudo card reader 264. Preferably, the "Initiate IEP for Purchase" command is created and forwarded to emulator 266 via card reader module 264. The command is modified in any suitable fashion to identify which record in data base 270 will be debited (i.e., which virtual card); for example, the user identifier or password may be included. Next, emulator 266 parses the incoming command and does a database fetch to obtain the virtual card record from data base 270. In other embodiments, the fetch may be optimized to only retrieve certain information. Emulator 266 then sends the record to HSM 268 for decryption of the card data found in the record.

Once responses to "Initiate IEP" from reader 264 are received, client module 224 combines these responses into a byte stream suitable for transmission over a network to a payment server. Also at this point, the currency type and expiration date of the virtual card in data base 270 are checked, and the total cost of the ordered merchandise is checked against the card balance to ensure that the value on the card is great enough to cover the transaction. If the checks are not successful, a message to that effect is delivered to the user and this transaction terminates.

Because security card 218 is remotely located it would not be advantageous to engage in numerous commands and responses between the security card and client code module 224 over an open network such as the Internet. In the interest of speed

Mastercard, Ex1002, p. 416

and reliability, it is advantageous to have fewer messages exchanged. Accordingly, client module 224 emulates a variety of security card commands in order to receive responses to these commands from pseudo card reader 264. To operate securely and reliably in this environment, in one embodiment of the present invention, client module 224 emulates a security card and gathers all the responses for transmission in one draw request message. These commands and responses between client code module 224 and pseudo card reader 264 occur as if there were an actual card reader with a physical smart card inside; in other words, client code module need not be aware that a virtual card is being used.

The draw request message may include a variety of information including a draw request token, state information, the merchant identifier, the transaction identifier, security information, a purse provider identifier, an intersector electronic purse (IEP) identifier, an algorithm used by the card, an expiry date, the balance of the card, a currency code, a currency exponent, the authentication mode of the IEP, the transaction number of the IEP, a key version and the purchase amount. As all of this information is prepackaged into a single draw request message, the number of messages over the Internet between OPAL server 260 and payment server 206 is greatly reduced.

In this embodiment, the draw request message is built by packaging the virtual card's response to the "Reset" and "Initiate IEP for Purchase" commands, any public key certificates, the total cost, and the currency of the transaction received from the HTML page. For public key cards, the card and issuer certificates are obtained from read commands and may also be included in the draw request. By packaging all of this information together into one draw request message, it is possible to cut down on the number of messages exchanged between OPAL server 260 and payment server 206 and reliability and speed is improved.

Next, in step 610 OPAL server 260 accesses payment server 206 using the IP address received from the merchant server. In step 612 OPAL server 260 sends the draw request message to payment server 206 as indicated at 310. OPAL server 260 also creates a log of this message being sent.

Mastercard, Ex1002, p. 417

In step 614 payment server 206 sends to terminal 214 draw request 312 and processes the draw request in conjunction with an associated security card 218 as will be explained in greater detail below with reference to FIG. 11D. In one embodiment of the invention, the payment server creates a transaction thread for each connected client module 224 to service it through the life cycle of the transaction. After step 614, payment server 206 has received a "Debit IEP" command and a security card signature (S2) 314 from security card 218.

The security card signature (S2) is a value that uniquely identifies and validates security card 218 to prove to OPAL server 260 that the incoming debit command is a valid command from a real security card. This validation ensures that when the virtual card is debited the financial totals in the security card are updated. Thus, the user of the virtual card is guaranteed that a valid debit of the card has occurred. In a preferred embodiment of the invention, the security card signature is an encrypted value ensuring that no other entity can forge an identity of a security card.

In step 616 the payment server sends the debit command along with the security card signature 316 to OPAL server 260 to allow the virtual card to debit itself. At this time, payment server 206 also logs the debit command into its database. Upon receiving the debit command from the payment server, client module 224 replaces the amount in the debit command with the original amount (from the merchant server) to ensure that the amount has not been tampered with while traveling over the network. At this time, client module 224 may also create a log of the debit command.

In step 618 client module 224 forwards the debit command and security card signature to emulator 266 which again retrieves the appropriate virtual card record from data base 270 for processing. Because HSM 268 does not store data, the card record is retrieved each time the HSM is used. Alternatively, the card record is retained in memory while a transaction is occurring. The card record, debit command and signature are sent to HSM 268 where the security card signature (S2) is verified and a virtual card signature (S3) is generated. The card record is updated in HSM 268 with revised parameters (including balance and transaction counter) to reflect the purchase transaction and returned to the card data base. Client module 224 receives the HSM response and generates a "Debit Response" message along with the card

Mastercard, Ex1002, p. 418

signature (S3). If the virtual card does not have enough value to satisfy the purchase amount, then the "Debit Response" message indicates as such. Card signature S3 is a unique value identifying a valid virtual card in card data base 270. In a preferred embodiment of the invention, the signature is in encrypted form to prevent tampering.

In step 620, emulator 266 sends the response message along with the card signature back to client module 224. At this point, the purchase amount has been deducted from the balance on the virtual card (assuming a successful transaction). Next, in step 622, client module 224 packages the response message 322 along with the card signature and sends them back to payment server 206. Client module 224 also logs the result of this virtual card debit.

In step 624 payment server 206 receives incoming message 322 and creates a log and updates the transaction status in its database for future error recovery. Payment server 206 then directs this received message 324 to security card 218 in terminal 214. Next, in step 626 the security card processes this response from the OPAL server and verifies the received virtual card signature.

As security card 214 contains the keys and algorithms necessary to compute card signatures, the security card is able to validate that a received virtual card signature is in fact a valid one by comparing this card signature with a generated expected value. A successful comparison indicates that a response message 324 received from the virtual card is in fact a valid message and that the virtual card has been debited. An error result code or a comparison that is not successful potentially indicates that the virtual card has not been debited. This comparison of card signatures by the security card ensures that a virtual card is in fact debited before the merchant server is directed to release the purchased merchandise to the user. This comparison of the virtual card signature to an expected value is performed by the security card for the highest level of security. As will be described in the embodiments of FIG. 6, 7, and 8, this comparison of virtual card signatures may also take place in payment server 206, in OPAL server 260, in client terminal 204 or in merchant server 208 with a variety of other advantages. Assuming that the transaction is so far valid, in step 628 the security card sends a response indicating the result of the signature verification. The payment server uses this response to build the

Mastercard, Ex1002, p. 419

"Debit Result" message. If the transaction were invalid or the verification failed, an exception would be returned.

In step 630 terminal 214 updates its data store with the virtual card number, a transaction count, the total sale amount, the response from the security card, and transaction numbers from the virtual card and from the security card. The payment server also logs the response received from the terminal along with the merchant identifier, etc., as indicated in step 632. Next, in step 634, the payment server packages the result message including the transaction identifiers and sends this message 328 to OPAL server 260 in encrypted form. Server 260 passes the result to emulator 266 for appropriate database updates such as balance and counter. The transaction is also logged in the history file.

The result message is then forwarded 329 to client terminal 204. At this point, the transaction thread of the payment server that was used for the current transaction may release the terminal, thus allowing the terminal to be used by other transactions. This transaction thread then exits at this time.

By sending this result message in encrypted form, the confirmation included in the message may be passed to the merchant server by way of the client terminal without fear of tampering. As the result message is encrypted, it would be extremely difficult for the client terminal or another entity to forge a confirmation and trick the merchant server into thinking that a transaction had taken place. In another embodiment of the invention, if the client terminal is a trusted agent, then the result message need not be encrypted. In yet another embodiment, payment server 206 may send two confirmation messages, one not encrypted for the client terminal to process, and one encrypted for the merchant server, or both messages encrypted under different keys. FIGS. 15A and 15B present an embodiment in which payment server 206 sends two messages back to client terminal 204.

In step 636 the client terminal then passes the result message 330 on to merchant server 208 at the URL address previously received from the merchant server. The client may also post a message to the user informing that the debit has been completed. The client may also log confirmation of the payment. In step 638 the merchant server registers the confirmation included in the message and checks for

Mastercard, Ex1002, p. 420

success. The merchant server calls a validate routine within the merchant code module to validate the result message received via the client terminal. The validate routine decrypts the transaction identifier along with the encrypted result message. If the decrypted result message is acceptable, the merchant server then determines that a successful transaction has occurred. Next, in step 640 the merchant server generates a message with the purchased information and delivers this information to the client terminal. Alternatively, the merchant server may generate a purchase receipt to deliver to the client terminal indicating goods and/or services to be rendered. At this point, the client terminal may log the merchant server's response. Completion of these steps indicates a successful financial transaction over the Internet using a virtual smart card.

Returning now to a more detailed discussion of step 614, FIG. 11D describes one technique for processing a draw request message in conjunction with a security card 218. Once this draw request message has been received by payment server 206 and passed along to terminal 214, the terminal parses the message back into individual responses and passes these responses sequentially to the security card as will be explained below. In an alternative embodiment, a dumb terminal is used and the draw request is parsed into its components and otherwise processed by the payment server, which then sends the responses to the security card itself.

In step 680 payment code module 228 of payment server 206 edits the draw request for syntactic correctness and logs the draw request message as being received. In step 682 the draw request is passed to terminal interface 230 of the payment server. In one specific embodiment, the terminal interface then requests a terminal from the payment server's terminal pool. The payment server may have a pool of terminals connected to a terminal concentrator that is established at start-up. At start-up, the payment server receives a list of all valid terminal identifiers. The payment server uses these identifiers, and its knowledge of transactions in progress to determine an appropriate terminal to process the transaction. Once a terminal is determined, the terminal interface builds a terminal specific message based upon the draw request and the type of terminal.

In step 686 the terminal specific draw request 312 is sent to chosen terminal 214 over a local area network. A concentrator may act as a router between a

Mastercard, Ex1002, p. 421

transaction thread in the payment server and a corresponding terminal if many terminals are attached to the payment server. The concentrator looks at a header on the draw request to determine to which terminal the transaction should be routed. In one embodiment of the invention, concentrator 212 is not necessary and payment server 206 communicates directly with terminal 214.

In step 688 terminal 214 parses the draw request message into its various components and processes each component in turn to emulate a card interacting with the security card in a physical terminal. Prepackaging of a variety of information into the draw request message results in fewer exchanges over the Internet between OPAL server 260 and payment server 206. By now simulating an interaction, security card 218 behaves as if it were in a physical terminal along with an actual smart card. A variety of responses from a smart card may be emulated. In this embodiment, the terminal sends each of the two commands "Answer to Reset" and "Initialize IEP for Purchase" down to the security card individually and waits for a return message, "Debit IEP," before sending the next response. For a public key transaction, the certificates read by the client are also included as individual responses. In this fashion, even though all of the smart card information (the draw request) originating from OPAL server 260 has been sent at once in prepackaged form over the Internet, the traditional interaction between a smart card and the security card in a physical terminal is simulated at terminal 214 in a remote location.

In step 690 terminal 214 reaches a "draw amount" state, indicating that security card 218 is able to generate a debit command. In step 692, the security card generates its security card signature and the command "Debit IEP". This signature and debit command 314 are sent to terminal 214. The debit command issued by the security card may contain a wide variety of information including the security card identifier, the transaction identifier, the amount to be debited, the currency and currency exponent for the amount, the security card signature, the date, time, and location. The terminal in turn, sends the signature, command, and the terminal identifier to the payment server as indicated in step 694 and shown as 314. At this point, step 614 ends and control returns to step 616.

Mastercard, Ex1002, p. 422

FIRST ALTERNATIVE PAYMENT EMBODIMENT

FIG. 6 illustrates an alternative embodiment 250a in which security card 218 is able to be released sooner than the security card of FIG. 5; this embodiment also requires fewer exchanges between terminal 214 and payment server 206. A security card in a terminal is dedicated to a particular transaction from the moment when the terminal interface selects that terminal until the security card finally issues a "Debit Result" message and is released by the terminal interface. In some circumstances it is desirable to release the security card earlier. By releasing a security card earlier, the card is tied up for a shorter time per transaction and may move on to the next transaction sooner. Also, the less time that a terminal is dedicated to a particular transaction, and the fewer messages exchanged between the two, the less likely chance there is of a communication error that might interrupt and halt the transaction.

Embodiment 250a includes client terminal 204, OPAL server 260, payment server 206, merchant server 208, and terminal 214 having security card 218. Communication between the servers may take place in a similar fashion as in FIG. 5 as indicated by communication links 234a, 234b and 236. Instead of two round trips of information between the terminal and payment server, however, there is only one round trip in this embodiment.

FIG. 12 is a flowchart that describes a technique for implementing this embodiment with reference to FIG. 6. Step 702 indicates that communication between the various entities takes place in a similar fashion as in FIG. 5 up until terminal 214 reaches the "draw amount" state. At this point, draw request 312 has been received and processed by security card 218. Next, in step 704 the security card generates not only the security card signature S2 and the Debit IEP command, but also the expected virtual card signature S3 from emulator 266 and HSM 268. This expected virtual card signature is a value expected by the security card from the virtual card to validate the virtual card's Debit Response message. This validation will ensure that the virtual card has been debited in card data base 270.

In step 706 the security card signature S2, the Debit IEP command and the expected virtual card signature S3 are sent to the payment code module in the payment server as indicated at 314a. Also, the terminal updates its data store in a

Mastercard, Ex1002, p. 423

similar fashion as in step 630. Next, step 708 indicates that the transaction occurs as before with reference to step 616-622. These steps indicate that emulator 266 receives the Debit IEP command, debits the virtual card in data base 270, and returns the Debit Response message and the virtual card signature S3 to the payment server.

Next, in step 710 the payment server code module processes this response from emulator 266 by comparing 346 the received virtual card signature S3 with the expected virtual card signature received earlier from the security card. This comparison of the two signatures by the payment module of the payment server obviates the need for another round trip between the payment server and the security card. Because the security card has already delivered the expected card signature S3 to the payment server, the security card may be released as soon as message 314a is received.

Assuming that the comparison is successful, the payment module is then able to generate its own Debit Result message instead of waiting for a message from the security card. Next, step 712 indicates that the processing continues in a similar fashion as in steps 632-640. The Debit Result message is passed on to the merchant server by way of the client terminal and the merchant server may then deliver the purchased merchandise to the user.

SECOND ALTERNATIVE PAYMENT EMBODIMENT

In another embodiment 250b of the present invention as illustrated in FIG. 7, not only is security card 218 allowed to release earlier, but the number of messages exchanged between OPAL server 260 and payment server 206 are reduced. Instead of comparing virtual card signatures in the payment server, the expected virtual card signature from the security card is transmitted to OPAL server 260 where a trusted agent 356 performs the comparison of the expected virtual card signature with the actual signature S3 received from emulator 266. Thus, message exchange between OPAL server 260 and payment server 206 is reduced to one round trip. This is advantageous because the time for a transaction is reduced, the security card is released earlier and fewer messages are exchanged, leading to more reliability over the Internet.

Mastercard, Ex1002, p. 424

Embodiment 250b includes client terminal 204, OPAL server 260, payment server 206, merchant server 208 and terminal 214 having security card 218. Communication between the OPAL server, the client terminal and the merchant server may take place in a similar fashion as in FIG. 5 as indicated by communication links 234a and 234b.

FIG. 13 is a flowchart that describes a technique for implementing this embodiment with reference to FIG. 7. Step 722 indicates that communication between the various entities takes place in a similar fashion as in FIG. 5 up until terminal 214 reaches the "draw amount" state. At this point, draw request 312 has been received and processed by security card 218. Next, in step 724 the security card generates not only the security card signature S2 and the Debit IEP command, but also an expected virtual card signature S3.

In step 726 the security card signature, the Debit IEP command and the expected virtual card signature are sent to payment code module 228 in payment server 206 as indicated in 314a. Also, the terminal updates its data store in a similar fashion as in step 630. Next, in step 728 the payment server code module sends the Debit IEP command, security card signature and expected virtual card signature to OPAL server 260.

Next, step 730 indicates that the transaction occurs as before with reference to steps 618 and 620. The steps indicate that emulator 266 receives the Debit IEP command and debits the virtual card in data base 270. In step 732, client code module 224 itself compares the actual card signature S3 from emulator 266 with the expected signature from the security card. This comparison of the two signatures by client module 224 of the OPAL server obviates the need for another round trip between the payment server and the OPAL server. Also, because the security card has already delivered the expected card signature to the payment server, the security card may be released as soon as message 314a is received.

Assuming that the comparison is successful, OPAL server 260 is then able to generate its own Debit Result message in step 734 instead of waiting for the message from the payment server. Next, step 736 indicates that the processing continues in a similar fashion as in steps 636-640. The Debit Result message is passed on to the

Mastercard, Ex1002, p. 425

merchant server via client terminal 204 and the merchant server may then deliver the purchased merchandise to the user.

In a variation on this embodiment, the expected signature and the generated virtual card signature S3 can be passed on to client terminal 204 which performs the comparison and generates the Debit Result message.

THIRD ALTERNATIVE PAYMENT EMBODIMENT

FIG. 8 illustrates another embodiment 250c of the invention in which merchant server 208 performs the comparison of the virtual card signature S3 with the expected signature. Embodiment 250c includes client terminal 204, payment server 206, OPAL server 260, merchant server 208 and terminal 214 having security card 218. This embodiment has all of the advantages of the previous embodiment in which the security card is released earlier, and there are also fewer messages passed between the entities. In this embodiment, if OPAL server 260 or client terminal 204 is not to be trusted to compare the virtual card signatures, then an encrypted expected signature is passed to the merchant server via the OPAL server and the client terminal. OPAL server 260 also passes the raw, unencrypted signature S3 from the virtual card to the merchant server. A routine 366 in the merchant server then compares the two signatures.

FIG. 14 is a flowchart that describes a technique for implementing this embodiment with reference to FIG. 8. Step 742 indicates that communication between the various entities takes place in a similar fashion as in FIG. 5 up until the terminal reaches the "draw amount" state. At this point, draw request 312 has been received and processed by security card 218. Next, in step 744 the security card generates not only the security card signature S2 and the Debit IEP command, but also an expected virtual card signature S3.

In step 746 the security card signature, the Debit IEP command and the expected virtual card signature are sent to payment code module 228 in the payment server as indicated in 314a. Also, the terminal updates its data store in a similar fashion as in step 630. Next, in step 748 the payment server code module encrypts the expected virtual card signature and sends the Debit IEP command, security card signature and an encrypted expected virtual card signature to OPAL server 260. The

Mastercard, Ex1002, p. 426

expected virtual card signature is encrypted to prevent tampering by client terminal 204, OPAL server 260 or other outside entity.

Next, step 750 indicates that the transaction occurs as before with reference to steps 618 and 620. The steps indicate that emulator 266 receives the Debit IEP command, debits the virtual card in data base 270 and generates Debit Response and the raw virtual card signature S3. In step 752, client code module 224 sends the Debit Response message, the raw virtual card signature and the encrypted signature on to merchant server 208 via client terminal 204. In step 754 the merchant server processes the Debit Response message, decrypts the encrypted signature, and compares the two signatures. This comparison of the two signatures by the merchant server obviates the need for another round trip between the payment server and the OPAL server. Also, because the security card has already delivered the expected card signature to the payment server, the security card may be released as soon as message 314a is received.

Assuming that the comparison is successful, the merchant server is then able to generate its own Debit Result message in step 756 instead of waiting for the message from the security card. Next, step 758 indicates that the processing continues in a similar fashion as in steps 638 and 640. The merchant server may then deliver the purchased merchandise to the user.

ENCRYPTION LAYER EMBODIMENT

FIG. 9 illustrates an embodiment 250d of the present invention in which an encryption layer has been added. Although the present invention may be practiced without this added encryption layer, in a preferred embodiment of the invention this encryption layer is used. FIG. 9 includes client terminal 204, payment server 206, OPAL server 260 and merchant server 208. Other elements of the system have been omitted in this figure for simplicity. This extra encryption layer is used not only to protect the contents of messages being transmitted over the Internet, but also to prevent a client terminal, server or other entity from receiving or producing a message that would trick another entity into thinking that a valid transaction had occurred. This encryption also prevents messages from being accidentally or deliberately altered or misdirected. In addition, it should be appreciated that encryption may be

Mastercard, Ex1002, p. 427

present in any embodiment on all parts of any message sent for security. Preferably, any signature sent over a network is encrypted.

FIGS. 15A and 15B are a flowchart describing this embodiment of the invention with reference to FIG. 9. In step 802 payment server 206 and merchant server 208 share a unique encryption key 402. Through a prior business arrangement, both of the servers have arranged to share this unique key to add security to the transaction. The shared key may be of any suitable encryption standard and of any length. The key may be a Data Encryption Standard (DES) key having a length of 128 bits including parity. Although this shared key could be used directly, in a preferred embodiment of the invention there is a derived unique key for each transaction between the merchant server and the payment server. Alternatively, another encryption standard such as RSA may be used. Preferably, loading of value is performed under DES, while a purchase may be performed under either DES or public key technology.

In step 804 client terminal 204 and merchant server 208 engage in a protected Secure Sockets Layer (SSL) session 404 in which a connection is made, a user browses and makes a purchase selection. The SSL session protects the information transmitted over the Internet (such as card information, commands, and encryption keys) from being discovered by an unauthorized party. Other techniques for protecting a session may also be used.

In step 806 the merchant server derives a key from DES key 402 using information unique to the transaction such as the merchant identifier, the transaction identifier, or other information such as a random number. Because the payment server shares DES key 402 with the merchant server and also has access to this unique information about the transaction, the payment server will also be able to derive this same key from shared DES key 402. In this step the merchant server also creates a transaction session key (TSK) for use by the client terminal and payment server to encrypt information.

In step 808 merchant server 208 downloads an HTML page of information 406 to client terminal 204 that includes the TSK and the TSK encrypted with the derived key (ETSK). The TSK encrypted with the derived key will be used by the

Mastercard, Ex1002, p. 428

payment server to return an encrypted (unreadable by others) result message to the merchant server. Only the merchant server will be able to decrypt this result message and will thus be guaranteed that a successful transaction has occurred and that merchandise may be released to the user. Client terminal 204 then passes purchase request 307a including the TSK and ETSK to OPAL server 260. The purchase request may be formed as previously described in FIG. 5. Preferably purchase request 307a is also protected under an SSL session or similar.

In step 810 OPAL server 260 prepares the draw request in conjunction with emulator 266 and sends the draw request 408 encrypted with the TSK to payment server 206 along with the ETSK. In step 812 the payment server uses shared DES key 402 and the prearranged information unique to the transaction to derive the same key that the merchant server has used. Thus, the derived key can be used to decrypt the ETSK in order to produce the TSK. Once the payment server had produced the TSK, it decrypts the draw request and processes the draw request in any suitable fashion with the security card. Once the payment server has received the Debit IEP command from security card 218, it encrypts the command with the TSK. The ability to correctly derive keys and encrypt the messages authenticates the payment server as the appropriate one for the merchant server, thereby preventing value decrement by an unauthorized party.

In step 814 the payment server sends the encrypted Debit IEP command 410 to the OPAL server 260. In step 816 the OPAL server decrypts the Debit IEP command with the TSK it had received earlier from the merchant server and processes the Debit IEP command in a suitable fashion with emulator 266. Once client code module 224 has received the Debit Response message from the emulator, it encrypts this message with the TSK and sends the Debit Response message 412 to the payment server. In step 820, the payment server decrypts the Debit Response message with the TSK and processes the Debit Response message in a suitable fashion with the security card.

Once the payment server has received a Debit Result message from the security card, the payment server encrypts the Debit Result message with the TSK to form a Debit Result C message for client terminal 204. The Debit Result C message will be used by the client terminal to inform the user of a successful transaction. The

Mastercard, Ex1002, p. 429

payment server also generates its own confirmation message and encrypts the message with the derived key to form a Debit Result M message. The Debit Result M message will be used to inform the merchant server of a successful transaction. The payment server then sends 414 Debit Result C and Debit Result M to the OPAL server.

In step 822 the OPAL server decrypts and processes the Debit Result C message and passes the Debit Result M message 416 on to the merchant server by way of client terminal 204. Because the Debit Result M message is encrypted with ETSK, the client terminal or other entity (including the OPAL server) is not able to tamper with it. The unencrypted Debit Result C message may also be passed to the client terminal to inform the user of a successful transaction. Alternatively, the encrypted Debit Result C message may be decrypted directly by the client terminal.

In step 824 the merchant server is able to decrypt the Debit Result M message because it had originally produced the derived key from the DES key. Once the merchant server has determined that a valid Debit Result M message has been received, it confirms that a valid transaction has taken place and may release merchandise to the user. The ability to correctly derive keys and encrypt the messages authenticates the payment server as the appropriate one for the merchant server, thereby preventing value decrement by an unauthorized party.

This security embodiment of FIG. 9 may be used with any of the previously described embodiments of the invention. By way of example, this security embodiment may be used with the embodiments of FIGS. 7 and 8 in which there is only one round trip between the OPAL server and the payment server. In particular, the expected virtual card signature received from the security card may be encrypted with the derived key so that it is unreadable by the client terminal, yet the merchant server will be able to compare the received card signature with the expected card signature to validate the transaction.

Other security may also be added to a transaction. Preferably, the OPAL server resides behind a firewall and sensitive data is triple-DES encrypted. Parameter changes and signature generation is preferably handled within a hardware security module. Also, any user access is controlled through use of user identifiers and

Mastercard, Ex1002, p. 430

passwords. To protect against denial of service attacks, SSL is used to protect messages from the merchant or bank server to the client terminal. DES session keys protect the integrity of transactions passing between the client terminal, OPAL server and payment or load server.

AUTHENTICATION AND LOYALTY EMBODIMENT

FIG. 16 illustrates a system 250' for implementing an authentication application or a loyalty application over internet 202. These applications may reside within smart card emulator 266 of OPAL server 260 along with standard accounts, stored-value, or other types of card applications. In this embodiment, OPAL server may also be termed a loyalty server.

In the authentication embodiment, a consumer may wish to access any of a variety of Web servers in order to redeem frequent flyer miles, award points, etc., that he or she has accumulated as part of a loyalty program. In this embodiment, a consumer has accumulated points through any of a variety of programs with airlines, restaurants, rental car companies, hotels, banks, credit or debit card issuers, telephone or other communication company, etc. These points are often stored with the entity that has granted them in a database indexed by a consumer name or number. For example, prior art frequent flyer cards have a number printed thereon that is used to index the number of miles accumulated by an individual in the airline's database.

Often the consumer wishes to redeem these points to receive free airline tickets, meals, car rental, overnight stays, prizes, awards, discounts, or other benefits. It is important to the airline (or other company) to be able to authenticate that the person trying to redeem points is the actual person who owns the points. By accessing a Web server associated with the particular program, this embodiment of the invention allows the consumer to use a virtual card in OPAL server 260 to authenticate that he or she is the true owner of the points and to receive benefits from the program. A consumer is typically assigned a card number (or loyalty number) that is associated with the consumer's name in a points database on the Web server. This embodiment of the invention represents the consumer's card number in a virtual card in OPAL server 260. This card number is transmitted to the Web server as part of the virtual

Mastercard, Ex1002, p. 431

card signature, or in a similar fashion. Thus, a consumer is authenticated to a Web server.

For example, a consumer with 30,000 frequent flyer miles on one airline may use this embodiment of the present invention to access a Web server associated with the airline. The consumer is requesting a free round-trip ticket in exchange for 20,000 miles. The present invention then operates to authenticate the consumer and delivers a confirmation of authentication message to the Web server for the airline. The Web server then deducts 20,000 miles from the consumer's account (leaving 10,000 miles) and delivers the free ticket to the consumer.

In one specific embodiment, the Web server associated with the airline (or the airline itself) keeps track of the consumer's total mileage and deducts mileage. In this instance, an authentication application in smart card emulator 266 is used to validate the presence of the consumer's virtual card in card data base 270 and to authenticate that the card number stored therein is from the true consumer. The authentication application may also be used to obtain access to the Web server site, thus authenticating the individual to whom access is given. In another specific embodiment, emulator 266 includes a loyalty application (such as on a physical smart card) and the consumer's virtual card in data base 270 stores the consumer's accumulated frequent flyer mileage; the mileage from the virtual card is then debited and confirmed to the Web server in a similar fashion as described in various of the embodiments by which a cash value is stored on and debited from a virtual card.

System 250' may be implemented in a similar fashion as system 250 of FIG. 5. The elements shown in system 250' having counterparts in system 200 are described above and have similar functionality. System 250' includes a web server 208' that may be any suitable computer server capable of presenting award information (hereinafter "benefits") to a consumer over an open network such as the Internet. Web server 208' may be the same as merchant server 208 of FIG. 5 or a separate computer. Preferably, web server 208' is implemented in a similar fashion as described above for merchant server 208. Web server 208' includes server module 232' that is preferably implemented in a similar fashion as merchant module 232. Additionally, server module 232' includes functionality to store and present benefits

Mastercard, Ex1002, p. 432

that are available for particular consumers. For example, benefits available such as airline tickets, prizes, etc. may be presented.

Points (such as frequent flyer miles, for example) that a consumer accumulates to achieve benefits may be linked to a particular consumer by an account number, password, or other identifier. The amount of points accumulated for each consumer may be stored on web server 208' using server module 232', or may be located in another database of the organization providing the benefits. In an alternative embodiment, these points for each program that a consumer is enrolled in are stored in a record (the consumer's virtual card) of card data base 270 and are manipulated using a loyalty application resident within emulator 266. For example, a consumer may have a virtual card that in addition to storing monetary value, also stores a quantity of frequent flyer miles accumulated for a particular airline (or a number of airlines), points accumulated for using a particular credit card, points for hotel stays at particular hotels, etc. For points stored on the consumer's virtual card in OPAL server 260, these points may be verified and debited in much the same way that monetary value on the consumer's virtual card is debited as described herein.

One embodiment by which a consumer has his or her virtual card authenticated in order to redeem points for benefits will now be explained. In one specific embodiment, a technique similar to that described in the flowchart of FIGS. 11A-11D for debiting monetary value may be used. Initially, consumer operating client terminal 204 accesses web server 208' over link 234', views benefits presented for a particular program (such as an airline's frequent flyer program), selects benefits from that program, and requests the authentication application to authenticate that his or her virtual card does in fact permit access to the services. Web server 208' receives and processes this request. The above steps may be performed in a similar fashion as steps 602 and 604.

Next, similar to step 606, web server 208' sends a page of information to client terminal 204. When claiming benefits, the total cost field is zero and the currency field is a specially assigned value. Keeping total cost field equal to zero causes the system to perform authentication but not to create a payment record. Alternatively, for those consumer's whose virtual card holds the amount of their points, additional fields may be sent from server 208' to terminal 204 indicating which account to debit

Mastercard, Ex1002, p. 433

and by how many points. The total cost and currency fields may be readily adapted for this purpose. The page of information is then sent to OPAL server 260 in a similar fashion as previously described.

Next, in a similar fashion to steps 608-612, a draw request message is built by OPAL server 260, and the draw request is sent to authentication server 206' over link 236'. Similar to step 614, the authentication server now processes the draw request in conjunction with security card 218 and sends back a Debit IEP command and a security card signature S2 to authentication server 206'. As total cost is zero, the draw amount state reached by security card 218 is also zero. In the alternative embodiment in which a virtual card in data base 270 stores points for a particular loyalty program, total cost may be a numerical value and a draw amount state may be reached indicating a number of points to be deducted from the virtual card.

Next, similar to steps 616-618, authentication server 206' sends the Debit IEP command and security card signature to OPAL server 260 and this information is processed. Even though a monetary value may not be debited, processing such as incrementing a counter indicating number of transactions and generating a virtual card signature S3 may still occur. In the alternative embodiment in which points are stored in card data base 270, the points needed to redeem the benefit chosen by the consumer from web server 208' may be debited from the appropriate account in this step.

Steps 620 through 638 are performed in a similar manner as in FIGS. 11B and 11C, except that in this case a monetary transaction is not being verified, but rather the virtual card is being authenticated to allow the consumer to complete his access to services or benefits. In step 626 in particular, the signature S3 of the virtual card is verified by security card 218. In this embodiment, security card 218 would send an Authentication Result message rather than the Debit Result message of step 628. Web server 208' then debits the appropriate number of points from the consumer's account or allows access to a privileged service for the benefit requested. In the alternative embodiment in which points are stored in card data base 270, the Authentication Result message serves not only as an authentication of the consumer, but also confirmation that the correct number of points have been debited from the virtual card for the appropriate program. Next, similar to step 640, web server 208'

Mastercard, Ex1002, p. 434

releases the benefit requested by the consumer (such as airline tickets, prizes, discounts, etc.) and the benefit is arranged to be delivered to the consumer.

It should be appreciated that this technique of redeeming points for benefits may also be practiced using any of the alternative embodiments of FIGS. 6, 7 or 8, thereby obtaining the advantages associated with those embodiments. Furthermore, this technique may take advantage of the encryption layer embodiment of FIG. 9. Additionally, as described below, the present invention may also be used to load more points onto a virtual card in much the same way that monetary value is added.

LOADING EMBODIMENT

FIG. 17 illustrates a system 850 for loading value onto a virtual card according to one embodiment of the present invention. An alternative loading embodiment is discussed after the discussion of system 850. System 850 includes client terminal 204, bank server 860, OPAL server 260 and load server 862. Client terminal 204, bank server 860, load server 862 and OPAL server 260 communicate with one another over any suitable open network such as internet 202.

Preferably, each of client terminal 204, bank server 860, OPAL server 260 and load server 862 implement a code module (similar in operation to the code modules described above) in the Java programming language that provides the functionality described below. For simplicity of explanation, reference will be made below to "client terminal," "bank server," "OPAL server" and "load server" even though the resident code is performing the functions. Card issuer 108 has been described previously in FIG. 3. Card issuer 108 may be a separate financial institution from the bank that includes bank server 860, or card issuer 108 may be the same bank that includes bank server 860.

Bank server 860 is any suitable computer within a bank or other financial institution. By way of example, bank server 860 is any suitable personal computer, a workstation or a mainframe computer. In one embodiment, bank server 860 runs a "servlet" program (a Java applet running on server) for communication with client terminal 204.

Mastercard, Ex1002, p. 435

Load server 862 is also any suitable computer and may be located at a third party location (such as at an issuer's site or its processor) or may be located within the same bank as bank server 860. Load server 862 also runs a servlet program for communication with OPAL server 260 and hardware security module 864. In an alternative embodiment, load server 862 and bank server 860 are the same computer which runs two different applications representing the functionality of each server.

Hardware security module (HSM) 864 is a device known in the art that may be embodied in a hardware "black box" or on any suitable computer. The hardware security module can be implemented in a hardware module outside of load server 862, can be implemented within load server 862, can be implemented in software, can be implemented as a security card described above or similar to HSM 268 above. HSM 864 contains the encryption keys used for generating signatures (for example S1, S2 and S3) that provide security for the transaction. These signatures are used by HSM 268 and HSM 864 to insure that the virtual card is not expired or counterfeit (i.e., is a valid card), to insure that module 864 is authentic, to insure that system 850 is authentic and, in general, to provide for a valid transaction and to prevent fraud. HSM 268 also includes encryption keys for the generation of a virtual card signature. In an alternative embodiment, HSM 864 could be replaced by a standard terminal that includes a security card such as is shown in the previous embodiments. In this situation, the encryption keys would be stored in the security card.

Briefly, system 850 operates as follows. A consumer accesses bank server 860 using client terminal 204. Assuming that the consumer's virtual card in OPAL server is not overloaded and that the consumer's account with the bank has sufficient funds, the consumer is able to download value from bank server 860 onto his virtual card. OPAL server 260 communicates with load server 862 to receive authorization for the load and for higher security. The virtual card may then be used to make purchases over the Internet as described above. Once the bank has downloaded value to the virtual card, a corresponding amount of funds is transferred from the bank to card issuer 108. Additionally, the same consumer account at the bank can be used to fund multiple OPAL accounts. For instance, a parent can set up their bank account to fund their child's OPAL account.

Mastercard, Ex1002, p. 436

Card issuer 108 places these funds in a holding pool. Once the virtual card is used to make a purchase from a merchant, the transaction is captured and settled through a clearing and settlement service, such as system 110 described above. The issuer bank decrements the funds pool for the amount of the purchase, which is then paid to the merchant bank. The merchant bank pays the merchant for the transaction. Settlement may occur in any suitable fashion such as is known in the art and, in particular, may be implemented as previously described in FIG. 1.

LOADING EMBODIMENT DETAILED TRANSACTION FLOW

One embodiment of a technique by which a virtual card is loaded over the Internet will now be described using the flowchart of FIGS. 18A through 18D with reference to FIG. 17. Various of the steps below may occur in a different order; the following description is for illustration purposes. Interaction between client terminal 204 and bank server 860, and between OPAL server 260 and load server 862, is preferably implemented in a similar fashion as between client terminal 204 and merchant server 208, and between OPAL server 260 and payment server 206 as described above, respectively. Certain implementation details mentioned above with respect to payment are equally applicable to loading a virtual card. Furthermore, the exemplary flow shown in the figures illustrates a successful transaction although a negative result may also occur.

Initially, a suitable web browser of client terminal 204 is used by the user to access a bank server Internet site. In step 871 the user selects an option to load value onto his or her virtual card in OPAL server 260. Preferably, at this point the user connects to OPAL server 260 and signs in with his user identifier (which preferably is masked on screen) and password. In step 872 the bank server sends a request for card information (including current card balance and maximum card balance). This request is passed on to OPAL server 260. OPAL server 260 via card emulator 266 reads the current virtual card balance, currency, and other card information from card data base 270 and returns the balance to bank server 860 via client terminal 204. In step 873 the bank server determines the maximum load value and verifies that enough funds are in the user's account to accommodate a load request. Preferably, maximum load value is equal to the maximum balance minus the current value of the card.

Mastercard, Ex1002, p. 437

At this point a load amount screen is presented to the user. The funding account number, expiration date, the virtual card number, maximum load amount and current balance of the virtual card are displayed and the user is directed to enter the value to be loaded onto the card. The user enters the value to be loaded and confirms the amount on an acceptance screen which displays the last four digits of the funding account number and its expiration date.

Assuming that the user's account balance is adequate, the bank server requests the user's account be debited in step 874 by the load value. Advantageously, this debit request from the bank server can use the existing ATM and accounting systems of the bank to debit the user's account. From the bank's point of view, value is being transferred from the user's account much in the same way that value would be transferred to a user in the form of cash at an ATM. In this situation, though, the value is not being dispensed as cash at an ATM, but is being sent over the Internet to a virtual card.

In step 875 bank server 860 builds an HTML page that includes the following client applet parameters: the load value; the type of currency being used; the port and IP address of load server 862; a unique transaction identifier used by both the load server and the bank server to track a transaction; a unique bank identifier assigned to the bank and known to the load server; and a session key. Other information may also be included such as the currency's exponent, a status URL address of the bank server used for communication from the client terminal, and other security information to ensure the identity of the bank server and the integrity of the message. Other process-related information such as software release level, encryption methodology and keys may also be conveyed. Once this page has been built, the page is sent to the requesting client browser which passes the page on to OPAL server 260 in step 875a. Receipt of the page triggers the activation of client code module 224 (in this example a Java applet) in OPAL server 260.

In step 876 OPAL server 260 interacts with card emulator 266 to obtain card information in order to build a Load Request message for later transmission to load server 862. Once responses from the emulator are received, the OPAL server combines these responses into a byte stream suitable for transmission over a network to a load server.

Mastercard, Ex1002, p. 438

Client code module 224 terminal emulates a variety of hardware security module 864 commands in order to receive responses from card emulator 266. In this embodiment, the virtual card (and the emulator) and the hardware security module are physically separated from one another; communication takes place over the Internet. In the interest of speed and reliability, it is advantageous to have only the minimum number of messages exchanged.

To operate securely and reliably in this environment client code module 224 emulates a security module and gathers all the responses for transmission into one Load Request message. The Load Request message may include a variety of information and preferably includes a virtual card signature (signature S1), a virtual card number, an expiry date, and a load amount. Other information such as the security algorithm, transaction counter, current card balance, and bank server time stamp are also preferably provided. As all of this information is prepackaged into a single Load Request message, the number of messages exchanged between OPAL server 260 and load server 862 over the Internet is minimized.

Next, in step 877 the OPAL server accesses the load server using the IP address received from the bank server. (Alternatively, if the OPAL server is also serving as the load server, then control skips this step and moves to step 879.) In step 878 the OPAL server sends the Load Request message to the load server. In step 879 the load server processes the Load Request in conjunction with an associated hardware security module (HSM) 864 as will be explained in greater detail below with reference to FIG. 18D. After step 879, the load server has received a security module signature (signature S2) as part of a Load command (also known as "Credit IEP" command) from HSM 864. The security module signature is a value that uniquely identifies and validates the HSM to prove to OPAL server 260 that the incoming Load command is a valid command from a real issuer's security module. Thus, the user of the virtual card and other interested parties are guaranteed that a valid load of the card has occurred. In a preferred embodiment of the invention, the security module signature is an encrypted value ensuring that no other entity can forge an identity of a security module.

In step 880 the load server sends the Load command including the security module signature to OPAL server 260 for loading of the virtual card. In step 881,

Mastercard, Ex1002, p. 439

upon receiving the Load command, client code module 224 passes the Load command to card emulator 266. Emulator 266 then processes the command in a similar fashion as it would process a Debit command described above. Emulator 266 retrieves a virtual card record from data base 270, verifies the signature using HSM 268, increases the virtual card balance by the load value, builds the transaction log, and returns the record to the data base. Emulator 266 also generates a Load Response message, a virtual card signature (signature S3), and a result code indicating success or failure of the load. In a preferred embodiment of the invention, this signature is in encrypted form to prevent tampering.

In step 882, the emulator sends the Load Response message containing the card signature (S3) and result code back to client code module 224. Next, in step 883 client code module 224 packages the Load Response message along with the card signature and sends them back to load server 862. In step 884 the load server receives the incoming message. The load server then processes the message into its components and directs the components to HSM 864. Next, in step 885 HSM 864 processes this response and verifies the received virtual card signature (S3).

As the hardware security module contains the keys and algorithms necessary to compute virtual card signatures, the security module is able to validate that a received card signature is in fact a valid one by comparing the received card signature with a generated expected value. A successful comparison indicates that a Load Response message received from the virtual card includes a valid success message and that the virtual card has been loaded. Assuming that the transaction is so far valid, in step 886 the security module sends a Load Result message (containing a confirmation) back to the load server.

It is possible that the virtual card has not been loaded by the proper amount, that the card is invalid, a user is unscrupulous or another discrepancy has occurred. For example, it is possible that OPAL server 260 has been tampered with to make it appear that a load has not occurred, when in fact a load has occurred. In this situation, processing in step 882 and on would be slightly different. For example, instead of generating a success code in the Load Response message, emulator 266 may generate a negative result code, potentially indicating that the virtual card has not been loaded. Processing of this situation would then occur as follows.

Mastercard, Ex1002, p. 440

In step 882, emulator 266 sends a Load Response containing the result code and virtual card signature S3 back to client code module 224. Code module 224 recognizes a negative result code, and invokes negative result handling. Module 224 then interacts with emulator 266 to generate a new Load Request for a zero value load using elements from the original request, along with a new card signature S1.

The negative result code, along with the signatures S3 and new S1, and the zero value Load Request are passed to load server 862 for analysis. The load server determines if the transaction counter in the zero value load equals the transaction counter in the previous request, along with verifying other pertinent information such as date and time, virtual card number, and currency code and exponent. If the counters are equal, the load server will hold the original S3 and will generate a new Load Request for security module 864 using data element values that would have been expected if the original transaction had failed. The new Load Request containing the new S1 is sent to the security module. If S1 is valid, then the original negative result is true and the security module generates a response to confirm to the load server that the signature was valid (thus, the load did not take place). The original negative result from the virtual card is then released to the security module to complete the original transaction. Processing would continue, but a user account would not be debited, and no settlement need occur because the virtual card was, in fact, not loaded. If S1 is not valid, the negative response is not true and then the result code in the original request is changed to reflect a successful load and passed to the security module. Processing then continues reflecting that a load has occurred.

Returning now to further processing, in step 887 load server 862 logs the response received from HSM 864 and updates its database with the transaction identifier, the bank identifier, the load value, etc. In general, any of the plethora of information passing through the load server may be added to its database. Next, in step 890 the load server creates a Load Result message including the transaction identifier and sends this message to OPAL server 260 in encrypted form. By sending this message in encrypted form, the message may be forwarded to the bank server by way of client terminal 204 without fear of tampering. As the Load Result message is encrypted, it would be difficult for the client terminal or another entity to forge such a message and trick the bank server into thinking that a valid load had taken place.

Mastercard, Ex1002, p. 441

In step 891 OPAL server 260 forwards the Load Result message via client terminal 204 to the bank server at the URL address previously received from the bank server. The client terminal may also post a message to the user informing that the load has been completed. In step 892 the bank server registers the Load Result message. The bank server calls a routine to decrypt the Load Result message. If the decrypted message is acceptable, the bank server determines a successful load has occurred. The Load Result message provides assurance to the bank that the user' card was in fact loaded with a particular value and thus prevents fraud. For example, a fraudulent user who tries to claim that his bank account was decremented and his card not loaded (and should thus receive more money from the bank) would be thwarted because the Load Result message proves that the user's card was in fact loaded. Alternatively, the Load Result message may indicate that a load did not occur, in which case the account would not be debited, and no settlement would occur.

At this point a successful load of the user's card has occurred (assuming all is well). For example, if the user had requested $100, that amount has been decremented from the user's account at the bank, and $100 has been loaded onto the user's virtual card. Preferably, at this point the amount loaded (in this example $100) is transferred from the bank to the virtual card issuer preferably through an existing network. The $100 is transferred so that the card issuer may manage the float on these unspent funds until the user spends the $100. Once the $100 (or a smaller portion) has been spent with a merchant, the card issuer is then able to settle the transaction with the merchant using any suitable clearing and settlement system. In an alternative embodiment, the bank may retain the $100 and settle directly with the merchant. In another embodiment, the bank and the card issuer are the same financial institution, and the $100 may be shifted between parts of the organization or remain in place.

Returning now to a more detailed discussion of step 879, FIG. 11D describes a technique for processing a Load Request message in conjunction with a security module. Once the Load Request message is received by the load server, the load server parses it into the appropriate elements and passes a request to the security module as will be explained below. Alternatively, the load server can build a network

Mastercard, Ex1002, p. 442

message and switch the request to a remote authentication server. Or, a smart terminal could parse the message and pass responses to the security module.

In step 895 the load server edits the Load Request for syntactic correctness and logs the request as received. In step 896 the load server constructs a Load Request message. In step 897 the load server passes the Load Request to the security module to emulate a card interacting with the security module. The load server behaves as if a physical card were actually interacting in an ATM (for example) through a network to a host with a security module. In this fashion, the Load Request originating from OPAL server 260 has been sent in prepackaged form over the Internet, thus emulating a traditional interaction between a physical card and a security module.

In step 898, the security module verifies the received virtual card signature S1 to prevent fraud. The security module generates its security module signature S2 and the Load command. The signature S2 will confirm to OPAL server 260 that the security module is authentic and belongs to the issuer of the virtual card. Additionally, S2 protects against a user trying to perform a fake load, keys out of synchronization, a counterfeit card, an expired card, etc. The security module then sends the signature and Load command to the load server as indicated in step 899. At this point, step 879 ends and control returns to step 880.

ALTERNATIVE LOADING EMBODIMENT

In an alternative embodiment, the load server functionality is incorporated into OPAL server 260. This embodiment allows an issuer to use the OPAL server as his authentication center. In this embodiment, the functionality of HSM 864 of load server 862 is incorporated into HSM 268 so that only one HSM is needed. Alternatively, two HSM's may be used. When the two servers are resident in the same hardware, message encryption is preferably deactivated to further increase throughput.

In a first step, the user accesses the bank server web site. The web site displays an option to load value onto his or her virtual smart card. The user chooses this option and is prompted to log in by entering his user identifier (which preferably is masked on screen) and password. This information is sent to OPAL server 260 (preferably in an SSL encryption session) which verifies the user data. OPAL server

Mastercard, Ex1002, p. 443

260 then sends back to the bank server the user's current virtual card balance (including currency type and exponent), maximum balance and maximum load amount. Bank server 860 then displays to the user a menu of load amounts or allows the user to enter an amount. The user selects a load amount and submits the request. In a preferred embodiment, the user is prompted locally by client terminal module 290 resident on client terminal 204 to confirm the amount to load. A display screen displays the last four digits of the funding account number and expiration date. Once the user approves, client terminal module 290 sends the load amount to OPAL server 260.

Next, OPAL server 260 routes a funds authorization request to a payment gateway which routes the request to the issuer of the virtual card via a network. A payment gateway may be implemented as an existing network endpoint that switches messages between networks (like those networks of Visa and American Express)--it performs message reformatting and protocol conversion as necessary. In a preferred embodiment, the request is routed over VisaNet, an existing global clearing and settlement system. Once approved, the payment gateway routes the approval response back to OPAL server 260.

Next, OPAL server 260 processes the load authentication internally, generating and verifying signatures S1, S2 and S3 in a similar fashion as described above. For example, if two HSMs are in use, HSM 268 represents the virtual smart card and HSM 864 represents the issuer. Smart card emulator 266 would then pass signatures generated by HSM 268 to HSM 864 and vice-versa. Should only one HSM be in use, HSM 268 would include not only cryptographic keys normally held within OPAL server, but also the issuer keys normally held within HSM 864. (Alternatively, HSM 268 may hold only a master key, while all other keys are passed from an encrypted database.) In this scenario, smart card emulator 266 would receive signature S1 (for example) from HSM 268, and then turn around and send signature S1 back to HSM 268 for verification (HSM 268 then acting as if it were HSM 864). Generations and verification of signatures S2 and S3 may be performed in a similar fashion.

Once successful, OPAL server 260 sends a confirmation message to client terminal 204 advising the user of the new amount loaded onto his virtual card. OPAL server 260 then may send a clearing request message to the issuer via the payment

Mastercard, Ex1002, p. 444

gateway. The payment gateway processes and responds. Finally, OPAL server 260 sends a load advise message to clearing and settlement system via the Payment Gateway.

COMPUTER SYSTEM EMBODIMENT

FIGS. 19 and 20 illustrate a computer system 900 suitable for implementing embodiments of the present invention. FIG. 19 shows one possible physical form of the computer system. Of course, the computer system may have many physical forms ranging from an integrated circuit, a printed circuit board and a small handheld device up to a huge super computer. Computer system 900 includes a monitor 902, a display 904, a housing 906, a disk drive 908, a keyboard 910 and a mouse 912. Disk 914 is a computer-readable medium used to transfer data to and from computer system 900.

FIG. 20 is an example of a block diagram for computer system 900. Attached to system bus 920 are a wide variety of subsystems. Processor(s) 922 (also referred to as central processing units, or CPUs) are coupled to storage devices including memory 924. Memory 924 includes random access memory (RAM) and read-only memory (ROM). As is well known in the art, ROM acts to transfer data and instructions uni-directionally to the CPU and RAM is used typically to transfer data and instructions in a bi-directional manner. Both of these types of memories may include any suitable of the computer-readable media described below. A fixed disk 926 is also coupled bi-directionally to CPU 922; it provides additional data storage capacity and may also include any of the computer-readable media described below. Fixed disk 926 may be used to store programs, data and the like and is typically a secondary storage medium (such as a hard disk) that is slower than primary storage. It will be appreciated that the information retained within fixed disk 926, may, in appropriate cases, be incorporated in standard fashion as virtual memory in memory 924. Removable disk 914 may take the form of any of the computer-readable media described below.

CPU 922 is also coupled to a variety of input/output devices such as display 904, keyboard 910, mouse 912 and speakers 930. In general, an input/output device may be any of: video displays, track balls, mice, keyboards, microphones, touch-sensitive displays, transducer card readers, magnetic or paper tape readers, tablets,

Mastercard, Ex1002, p. 445

styluses, voice or handwriting recognizers, biometrics readers, or other computers. CPU 922 optionally may be coupled to another computer or telecommunications network using network interface 940. With such a network interface, it is contemplated that the CPU might receive information from the network, or might output information to the network in the course of performing the above-described method steps. Furthermore, method embodiments of the present invention may execute solely upon CPU 922 or may execute over a network such as the Internet in conjunction with a remote CPU that shares a portion of the processing.

In addition, embodiments of the present invention further relate to computer storage products with a computer-readable medium that have computer code thereon for performing various computer-implemented operations. The media and computer code may be those specially designed and constructed for the purposes of the present invention, or they may be of the kind well known and available to those having skill in the computer software arts. Examples of computer-readable media include, but are not limited to: magnetic media such as hard disks, floppy disks, and magnetic tape; optical media such as CD-ROMs and holographic devices; magneto-optical media such as floptical disks; and hardware devices that are specially configured to store and execute program code, such as application-specific integrated circuits (ASICs), programmable logic devices (PLDs) and ROM and RAM devices. Examples of computer code include machine code, such as produced by a compiler, and files containing higher level code that are executed by a computer using an interpreter.

Although the foregoing invention has been described in some detail for purposes of clarity of understanding, it will be apparent that certain changes and modifications may be practiced within the scope of the appended claims. For instance, multiple issuers or multiple currencies may be represented on a single OPAL server. Also, the user identifier may be routed to the issuing bank for verification, instead of by the OPAL server. The virtual card database may be resident within the OPAL server or on separate hardware. The SET protocol may also be used at a future time.

In addition, other arrangements or databases for representing a virtual card that are capable of loading, storing and decrementing value on command may be used. Also, any network capable of performing routing functionality between a client

Mastercard, Ex1002, p. 446

terminal, an OPAL server, a load and a bank server may be used. Furthermore, the security module may be a physically separate module, a card located in a terminal attached to a load server, or its functionality may be incorporated directly into a load server in hardware or software. And although the client terminal may be used to route messages between the bank server and load server, both of these servers may also communicate directly between themselves, and may even be the same computer. The specific messages shown passing between the computers are exemplary, and other types of messages may be used. A specified Load Request is shown, but other information may also be loaded onto a virtual card using a security module emulation and then sent packaged as one message to the security module over a network. In addition to monetary value, other types of value such as electronic cash, checks, awards, loyalty points, benefits, etc., may be loaded onto a card, and the term "value" is intended to broadly cover all of these various types. Any suitable type of encryption may be used to encrypt messages passing between the computers.

Therefore, the described embodiments should be taken as illustrative and not restrictive, and the invention should not be limited to the details given herein but should be defined by the following claims and their full scope of equivalents.

Mastercard, Ex1002, p. 447

CLAIMS

1. An on-line purchase and load (OPAL) server for performing a transaction over a network using a virtual smart card, said OPAL server comprising:

a virtual smart card database having a plurality of records, each record including a virtual card identifier and a balance corresponding to a single virtual smart card;

a hardware security module;

a smart card emulator that receives smart card commands and processes said commands in conjunction with said virtual smart card database and said hardware security module; and

a pseudo card reader module that receives said smart card commands and relays said commands to said smart card emulator, whereby said OPAL server performs a transaction over said network using one of said records in said virtual smart card database.

2. An OPAL server as recited in claim 1 wherein said virtual card database further includes purchase algorithm identifiers, and wherein said hardware security module includes a plurality of purchase algorithms that are identified for use by one of said purchase algorithm identifiers, whereby said hardware security module may be used to perform cryptographic functions associated with a purchase.

3. An OPAL server as recited in claim 1 further comprising:

a user verification module that verifies a user accessing said OPAL server and generates a user identifier, said user identifier being suitable to identify one of said virtual smart card records in said card database.

4. An OPAL server as recited in claim 1 wherein said smart card emulator and said pseudo card reader module are implemented as a single software module.

Mastercard, Ex1002, p. 448

5. An OPAL server as recited in claim 1 wherein said network is an internet over which said OPAL server communicates with a merchant server and a payment server to transact a purchase.

6. An OPAL server as recited in claim 1 wherein said network is an internet over which said OPAL server communicates with a bank server and a load server to load value onto said virtual smart card.

7. An OPAL server as recited in claim 1 wherein said network is an internet over which said OPAL server communicates with a web server and an authentication server to authenticate a user.

8. An OPAL server as recited in claim 1 wherein said OPAL server communicates over said network with a payment gateway for funding account authorization and clearing.

9. A network payment system for transacting a sale of merchandise over a network using a virtual smart card, said network payment system comprising:

a router for routing communication between entities attached to said network;

a merchant server in communication with said network, said merchant server having at least a first item of merchandise for sale;

a client terminal in communication with said network, said client terminal including an output device for reviewing said first item for sale and an input device for initiating a purchase transaction to purchase said first item for sale;

an on-line purchase server having a record in a database representing a virtual smart card; and

a payment server in communication with said network, said payment server including an interface for communicating with a security card and being arranged to receive a purchase message from said on-line purchase server and to transmit a confirmation message to said merchant server over said network, whereby said merchant server is authorized to release said item of merchandise to a user associated with said virtual smart card.

Mastercard, Ex1002, p. 449

10. A network payment system as recited in claim 9 wherein said network is an internet and said merchant server includes a merchant web site for advertising said first item for sale over said internet.

11. A network payment system as recited in claim 9 wherein said on-line purchase server further includes

a hardware security module;

a smart card emulator that receives smart card commands and processes said commands in conjunction with said virtual smart card record of said database and said hardware security module, whereby said on-line purchase server implements a secure purchase over said network.

12. A computer-implemented method of transacting a sale of an item over a network using an on-line purchase server having a record in a database representing a virtual smart card, said method comprising:

receiving a cost of said item to be purchased by a user, said cost originating from a merchant server over said network;

formulating a draw request message using information in said virtual smart card record;

sending said draw request message to a payment server connected to said network so that said draw request may be processed by a security card associated with said payment server;

receiving a debit command from said payment server;

debiting a balance amount in said virtual smart card record by said cost; and

sending a debit response message to said payment server, whereby said merchant server may be informed that said sale of said item is a success and said merchant server may release said item to a user associated with said virtual smart card record.

Mastercard, Ex1002, p. 450

13. A method as recited in claim 12 wherein said network is an internet and said merchant server includes a merchant web site for advertising said item over said internet.

14. A method as recited in claim 12 wherein said on-line purchase server includes a smart card emulator and said method further comprises:

sending smart card commands to said smart card emulator that processes said commands in conjunction with said virtual smart card record of said database to assist in formulating said draw request message.

15. A method as recited in claim 14 wherein said on-line purchase server includes a hardware security module and said method further comprises:

generating cryptographic signatures for use in transacting said sale using said hardware security module, whereby said on-line purchase server implements a secure transaction over said network.

16. A network loading system for loading value over a network onto a virtual smart card, said network loading system comprising:

a router for routing communication between entities attached to said network;

a bank server in communication with said network, said bank server arranged to debit a user account by an indicated value;

a client terminal in communication with said network, said client terminal including an input device for indicating a value to debited from said user account;

an on-line load server having a record in a database representing a virtual smart card; and

an issuer load server in communication with said network, said issuer load server including an interface for communicating with a hardware security module and being arranged to receive a load request including a virtual smart card signature and being further arranged to transmit a confirmation message to said bank server over said network, thereby confirming that said virtual smart card has been loaded by said indicated value.

Mastercard, Ex1002, p. 451

17. A network loading system as recited in claim 16 wherein said network is an internet and said bank server includes a bank web site for accepting a load request.

18. A network loading system as recited in claim 16 wherein said on-line load server further includes

a hardware security module;

a smart card emulator that receives smart card commands and processes said commands in conjunction with said virtual smart card record of said database and said hardware security module, whereby said on-line load server implements a secure load over said network.

19. A network loading system as recited in claim 16 wherein said on-line load server and said issuer load server are the same computer.

20. A computer-implemented method of loading a virtual smart card over a network, said virtual smart card being represented as a record in a database of an on-line load server, said method comprising:

receiving from a bank server a request to load value onto said virtual smart card;

formulating a load request message using information in said virtual smart card record;

sending said load request message to an issuer load server connected to said network;

receiving a load command from said issuer load server;

loading said virtual smart card by said load value; and

sending confirmation information to said bank server, whereby said bank server is assured that said loading is a success.

21. A method as recited in claim 20 wherein said network is an internet and said bank server includes a bank web site for accepting a load request.

Mastercard, Ex1002, p. 452

22. A method as recited in claim 20 wherein said on-line load server includes a smart card emulator and said method further comprises:

sending smart card commands to said smart card emulator that processes said commands in conjunction with said virtual smart card record of said database to assist in formulating said load request message.

23. A method as recited in claim 22 wherein said on-line load server includes a hardware security module and said method further comprises:

generating cryptographic signatures for use in transacting said load using said hardware security module, whereby said on-line load server implements a secure load over said network.

24. A method as recited in claim 20 wherein said on-line load server and said issuer load server are the same computer.

25. A network authentication system for authenticating a user over a network using a virtual smart card, said network payment system comprising:

a router for routing communication between entities attached to said network;

a web server in communication with said network, said web server allowing a user to redeem loyalty points in exchange for benefits;

a client terminal in communication with said network, said client terminal including an output device for reviewing said benefits and an input device for initiating a redemption of said loyalty points;

an on-line loyalty server having a record in a database representing a virtual smart card; and

an authentication server in communication with said network, said authentication server including an interface for communicating with a security card and being arranged to receive a debit message from said on-line loyalty server and to transmit a confirmation message to said merchant server over said network, whereby said merchant server is authorized to release said benefits to a user associated with said virtual smart card.

Mastercard, Ex1002, p. 453

26. A network authentication system as recited in claim 25 wherein said network is an internet and said web server includes a web site for displaying said benefits over said internet.

27. A network authentication system as recited in claim 25 wherein said on-line loyalty server further includes

a hardware security module;

a smart card emulator that receives smart card commands and processes said commands in conjunction with said virtual smart card record of said database and said hardware security module, whereby said on-line loyalty server implements a secure authentication over said network.

28. A network authentication system as recited in claim 25 wherein said on-line loyalty server and said authentication server are the same computer.

29. A network authentication system as recited in claim 25 wherein said virtual smart card record in said database stores said loyalty points belonging to said user, and wherein said on-line loyalty server is further arranged to debit said loyalty points.

30. A computer-implemented method of redeeming loyalty points over a network using an on-line loyalty server having a record in a database representing a virtual smart card, said method comprising:

receiving an amount of loyalty points to be redeemed by a user for benefits, said amount originating from a web server over said network;

formulating a draw request message using information in said virtual smart card record;

sending said draw request message to an authentication server connected to said network so that said draw request may be processed by a security card associated with said authentication server;

receiving a debit command from said authentication server;

Mastercard, Ex1002, p. 454

debiting a balance of said loyalty points in said virtual smart card record by said amount; and

sending a debit response message to said authentication server, whereby said web server may be informed that said redemption of said loyalty points is a success and said web server may release said benefits to a user associated with said virtual smart card record.

31. A method as recited in claim 30 wherein said network is an internet and said web server includes a web site for displaying said benefits over said internet.

32. A method as recited in claim 30 wherein said on-line loyalty server includes a smart card emulator and said method further comprises:

sending smart card commands to said smart card emulator that processes said commands in conjunction with said virtual smart card record of said database to assist in formulating said draw request message.

33. A method as recited in claim 32 wherein said on-line loyalty server includes a hardware security module and said method further comprises:

generating cryptographic signatures for use in transacting said redemption using said hardware security module, whereby said on-line loyalty server implements a secure transaction over said network.

Mastercard, Ex1002, p. 455

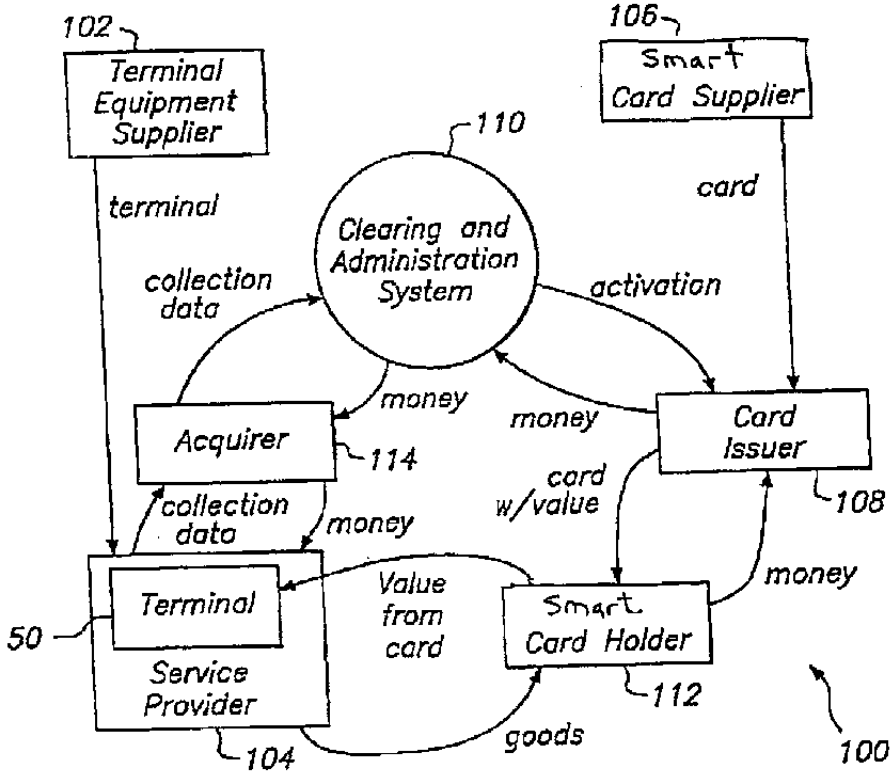


FIG. 1 PRIOR ART

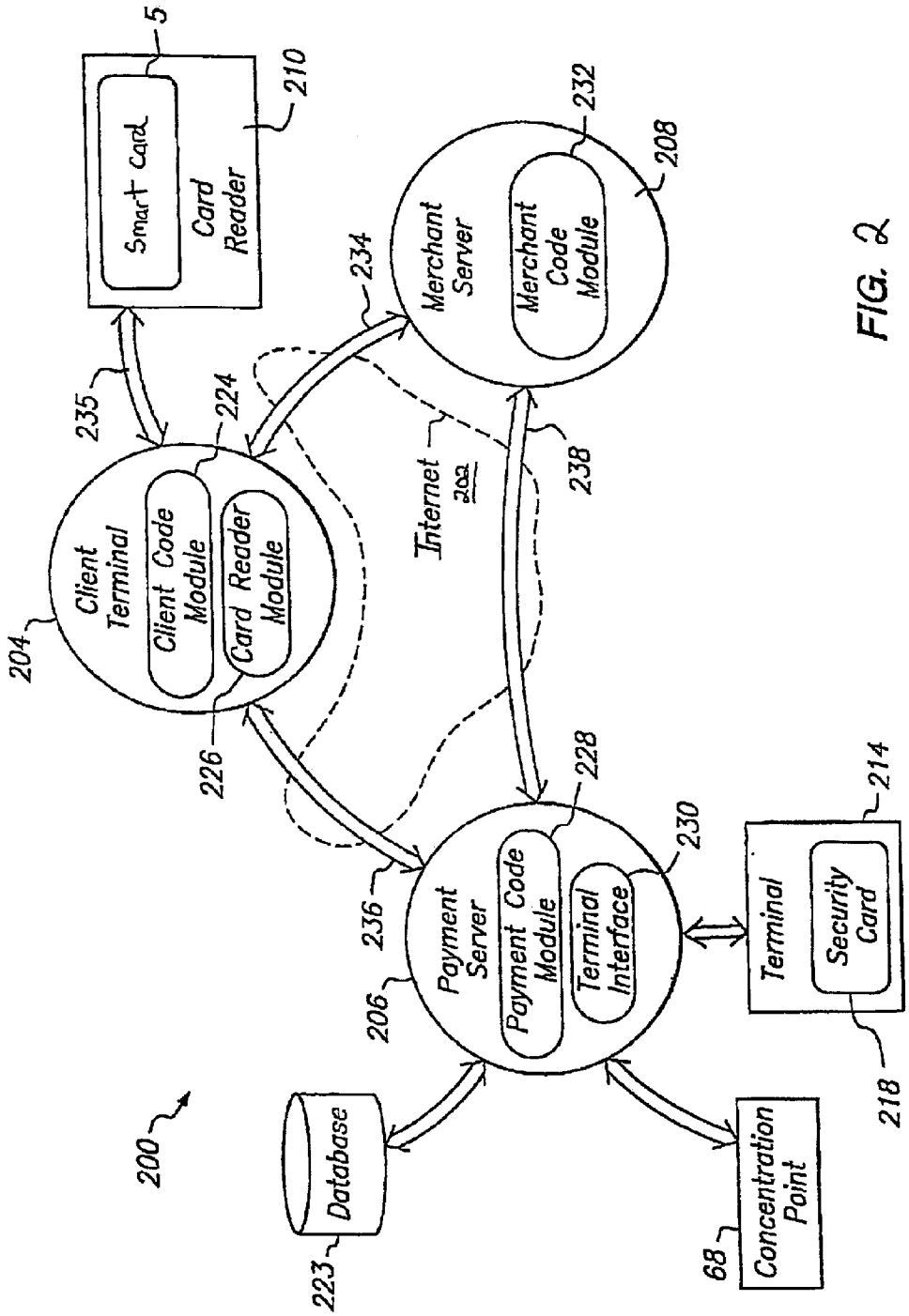

200
Client Terminal
204
Client Code Module
Card Reader Module
224
226
235
Smart Card
5
Card Reader
210
Internet
202
Merchant Server
208
Merchant Code Module
232
234
238
Payment Server
206
Payment Code Module
228
Terminal Interface
230
236
Terminal
214
Security Card
218
Database
223
Concentration Point
68

FIG. 2

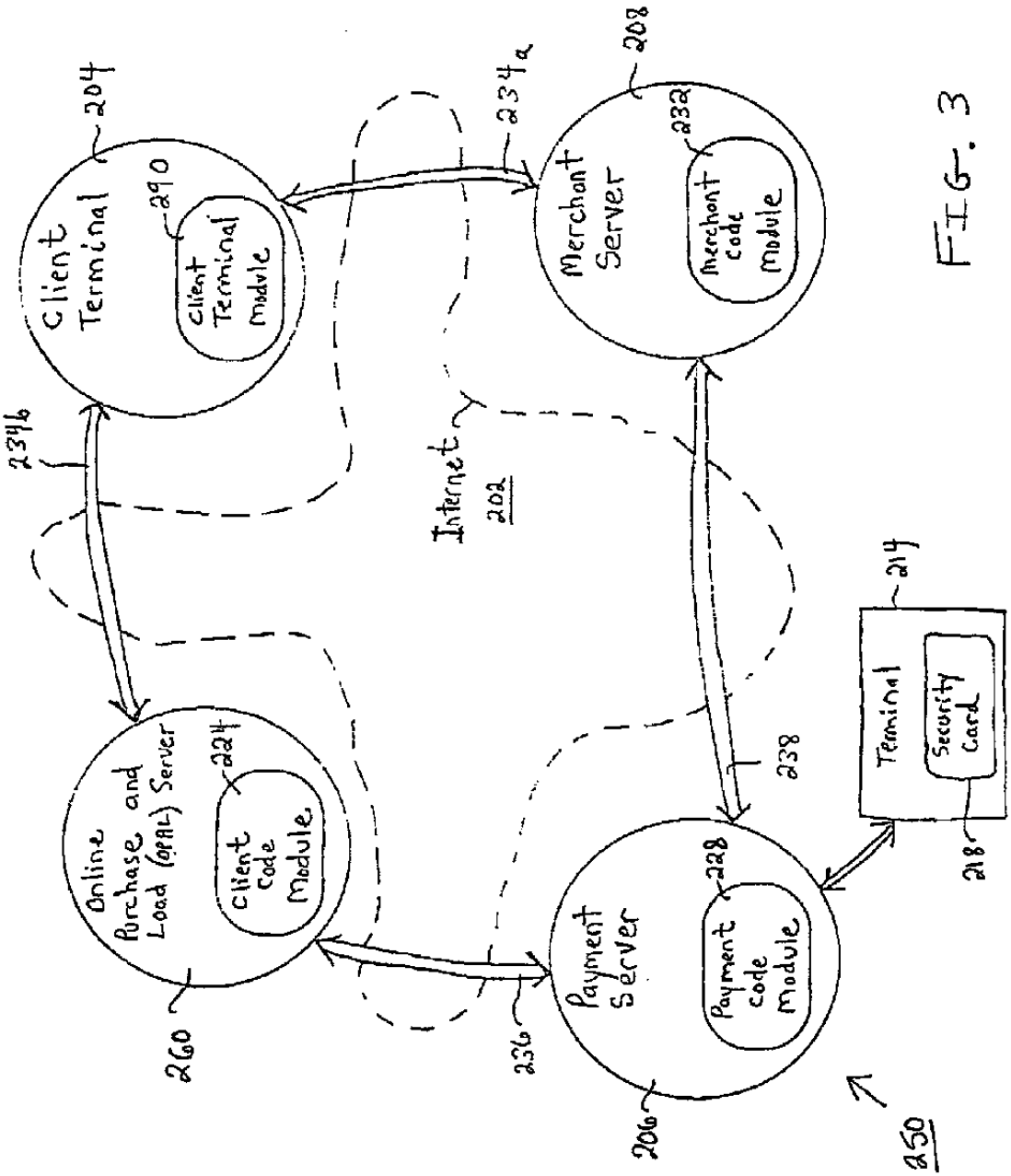
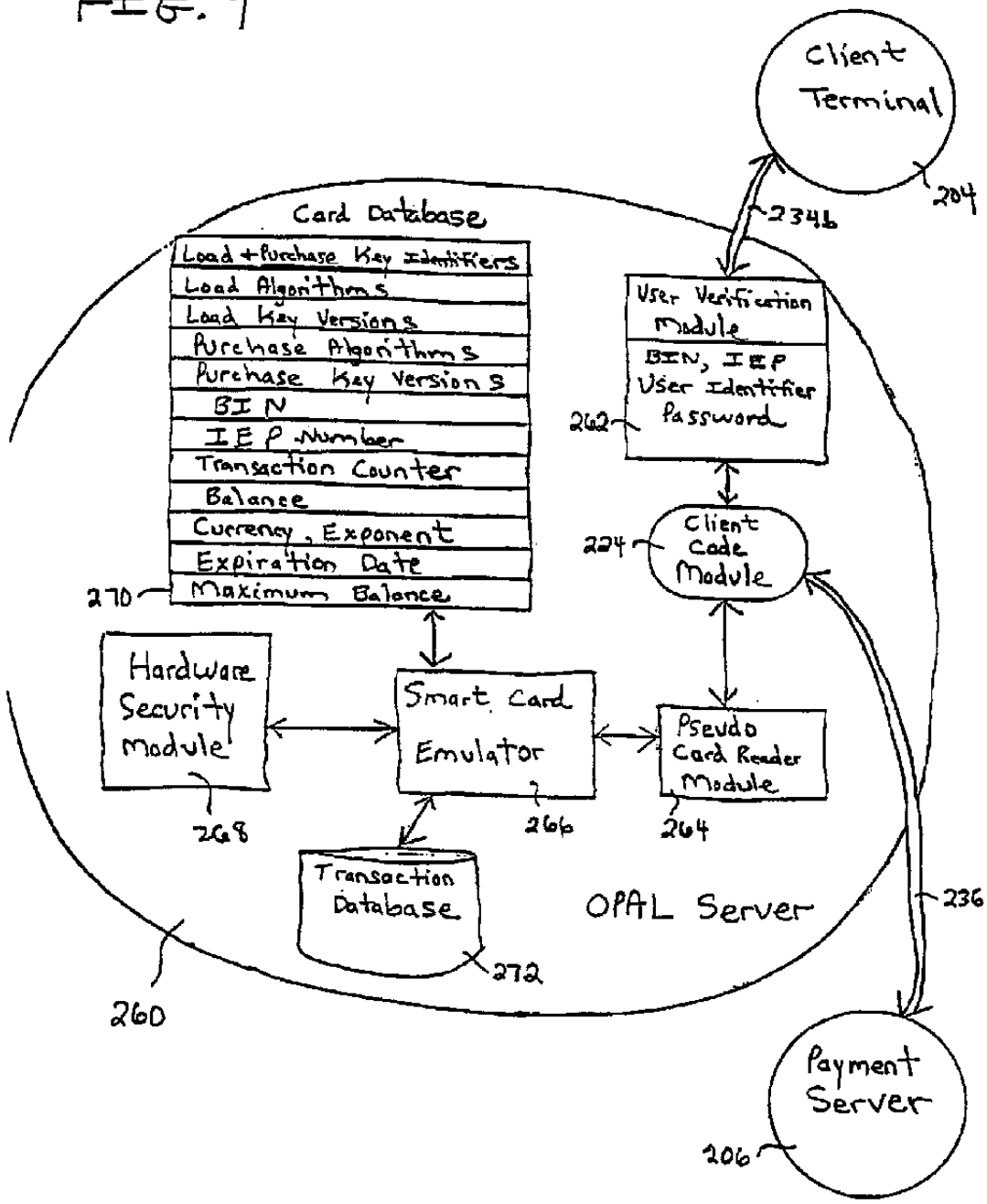

Client Terminal
204
290
Client Terminal Module
Merchant Server
208
232
Merchant Code Module
234a
Internet
202
234b
Online Purchase and Load (OPAL) Server
224
Client Code Module
260
Payment Server
206
228
Payment Code Module
236
238
Terminal
214
Security Card
218
250

FIG. 3

FIG. 4



Mastercard, Ex1002, p. 459

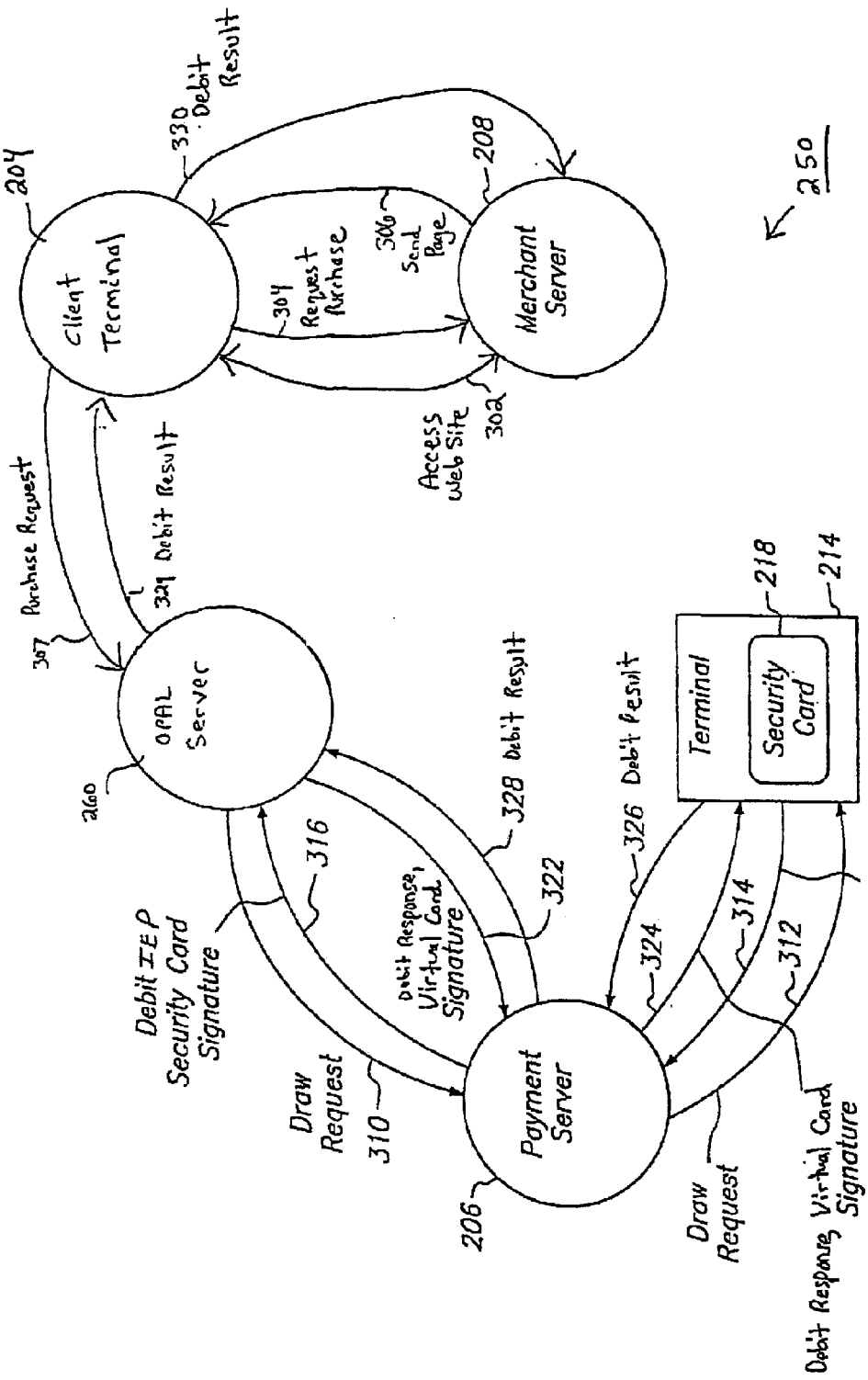


FIG. 5

Mastercard, Ex1002, p. 460

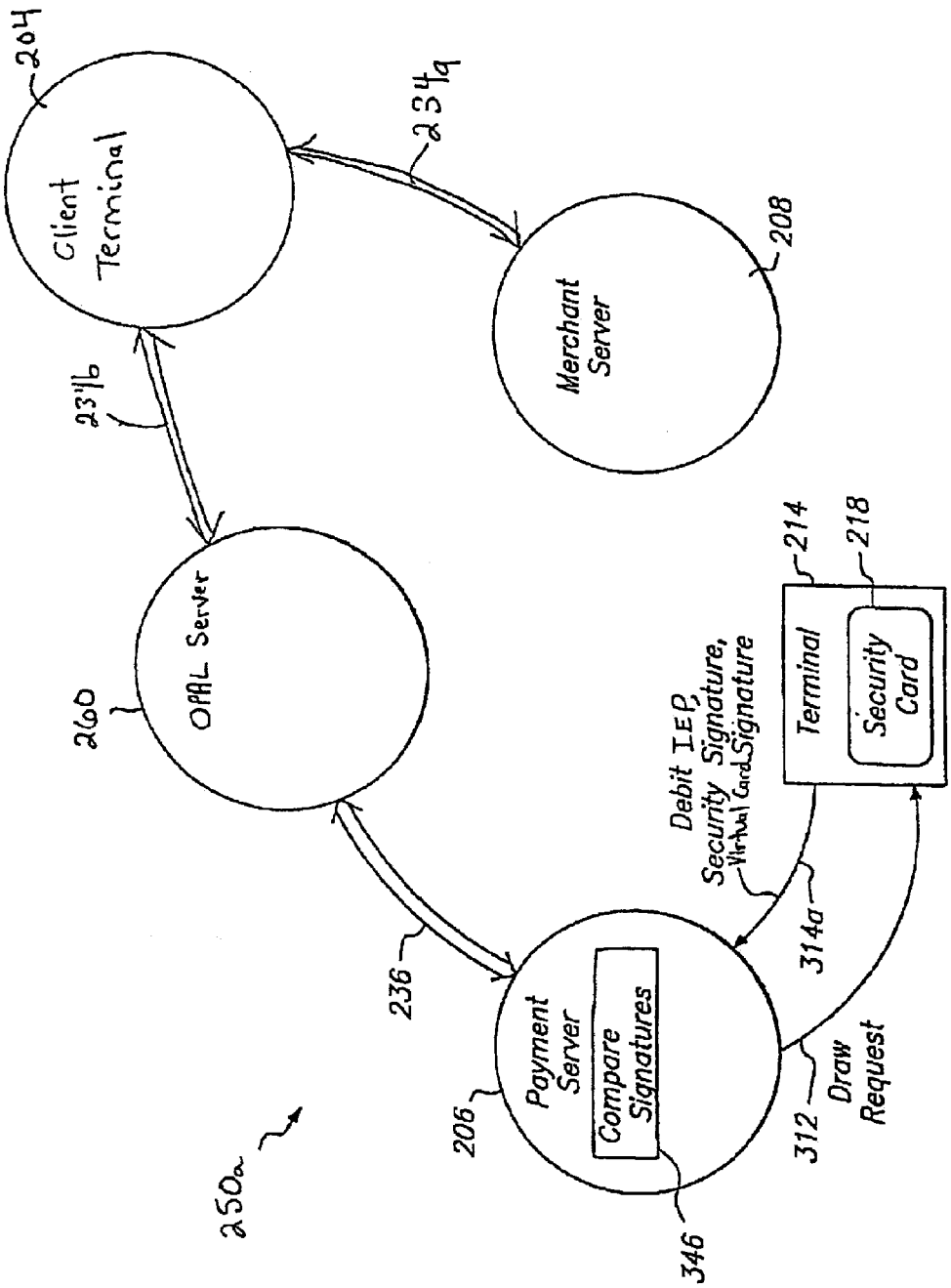

204
Client Terminal
234a
208
Merchant Server
232b
260
OAL Server
214
218
Terminal
Security Card
Debit IEP, Security Signature, Terminal Card Signature
314a
236
206
Payment Server
Compare Signatures
312
Draw Request
346
250a

FIG. 6

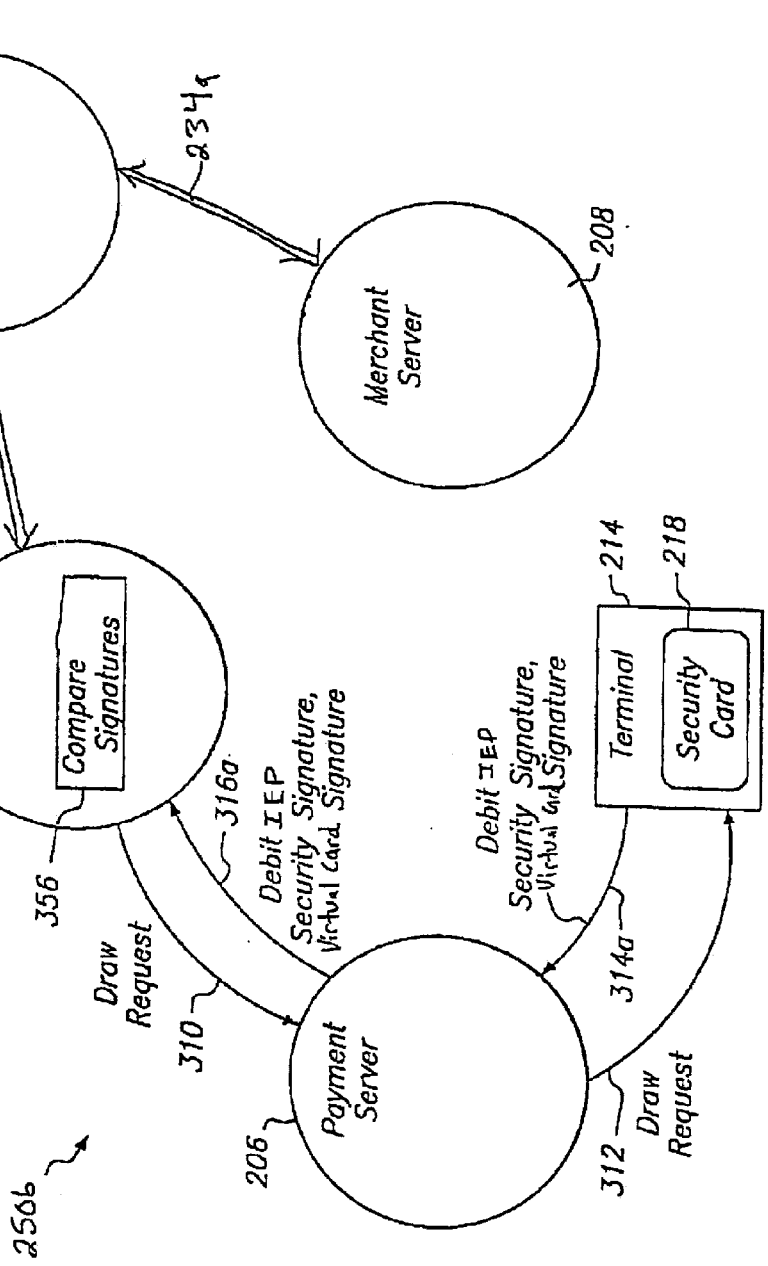

2566
204
Client Terminal
234q
208
Merchant Server
234b
260
OFAL Server
Compare Signatures
356
316a
Debit IEP
Security Signature,
Virtual Card Signature
Draw Request
310
206
Payment Server
Debit IEP
Security Signature,
Virtual Card Signature
314a
214
Terminal
218
Security Card
312
Draw Request

FIG. 7

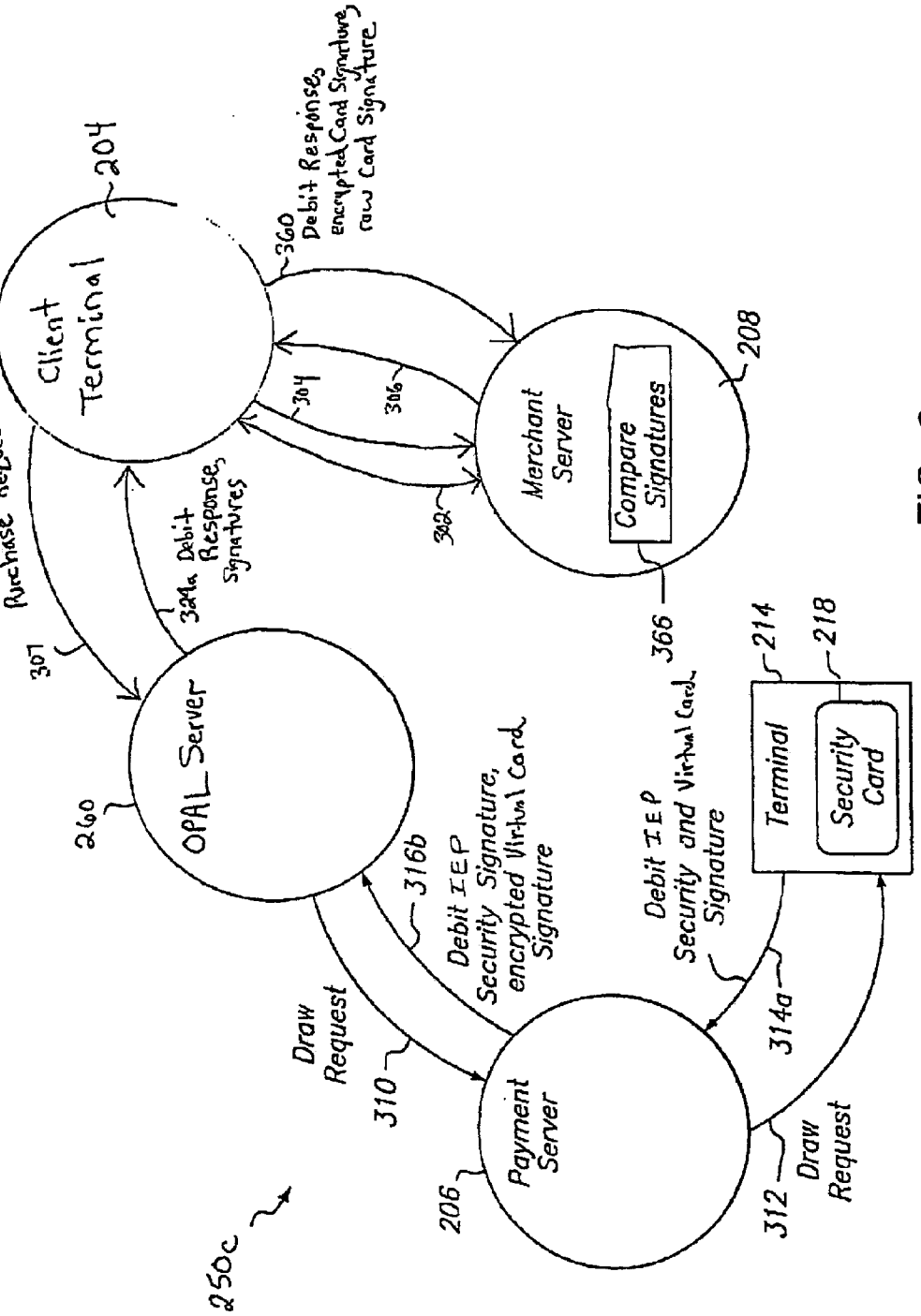


FIG. 8

Mastercard, Ex1002, p. 463

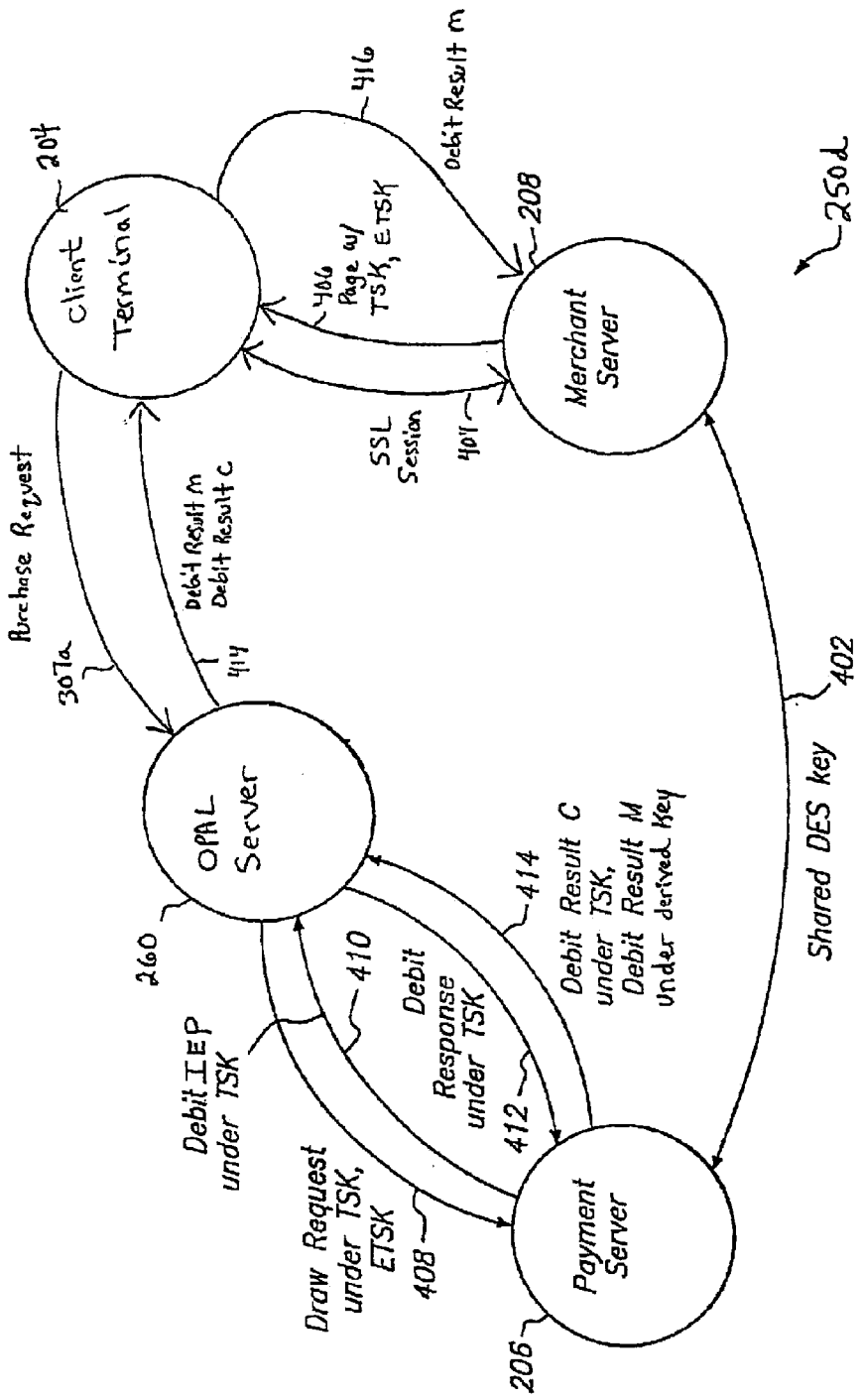

Client Terminal
204
OAL Server
260
Merchant Server
208
Payment Server
206
250d
Purchase Request
307a
Debit Result M
Debit Result C
414
SSL Session
401
416
Page w/ TSK, ETSK
Debit Result M
Debit IEP under TSK
410
Debit Response under TSK
412
Debit Result C under TSK, Debit Result M under derived Key
414
Draw Request under TSK, ETSK
408
Shared DES key
402

FIG. 9

FIG. 10

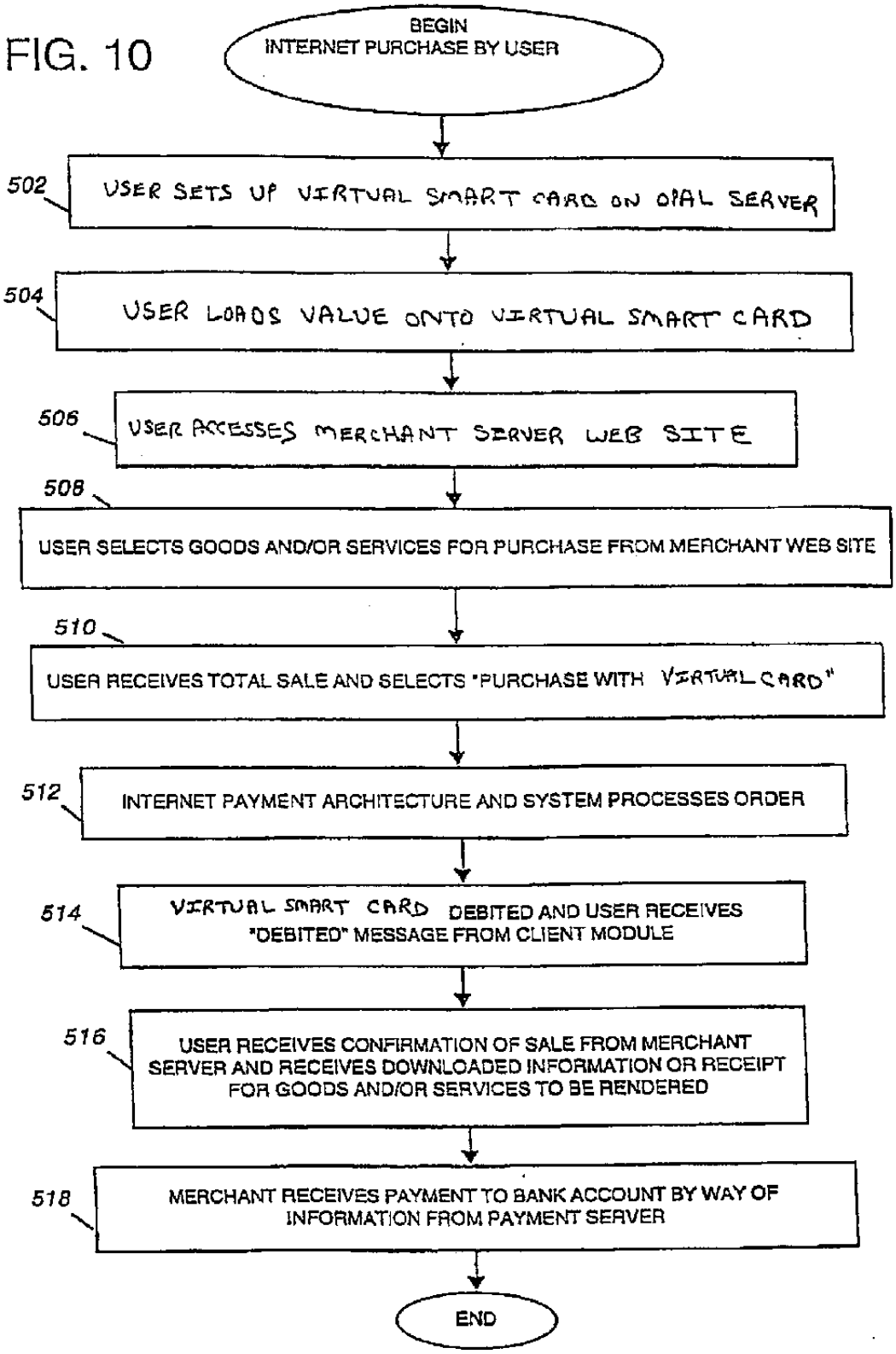

BEGIN
INTERNET PURCHASE BY USER
502
USER SETS UP VIRTUAL SMART CARD ON DIAL SERVER
504
USER LOADS VALUE ONTO VIRTUAL SMART CARD
506
USER ACCESSES MERCHANT SERVER WEB SITE
508
USER SELECTS GOODS AND/OR SERVICES FOR PURCHASE FROM MERCHANT WEB SITE
510
USER RECEIVES TOTAL SALE AND SELECTS "PURCHASE WITH VIRTUAL CARD"
512
INTERNET PAYMENT ARCHITECTURE AND SYSTEM PROCESSES ORDER
514
VIRTUAL SMART CARD DEBITED AND USER RECEIVES "DEBITED" MESSAGE FROM CLIENT MODULE
516
USER RECEIVES CONFIRMATION OF SALE FROM MERCHANT SERVER AND RECEIVES DOWNLOADED INFORMATION OR RECEIPT FOR GOODS AND/OR SERVICES TO BE RENDERED
518
MERCHANT RECEIVES PAYMENT TO BANK ACCOUNT BY WAY OF INFORMATION FROM PAYMENT SERVER
END

FIG. 11A

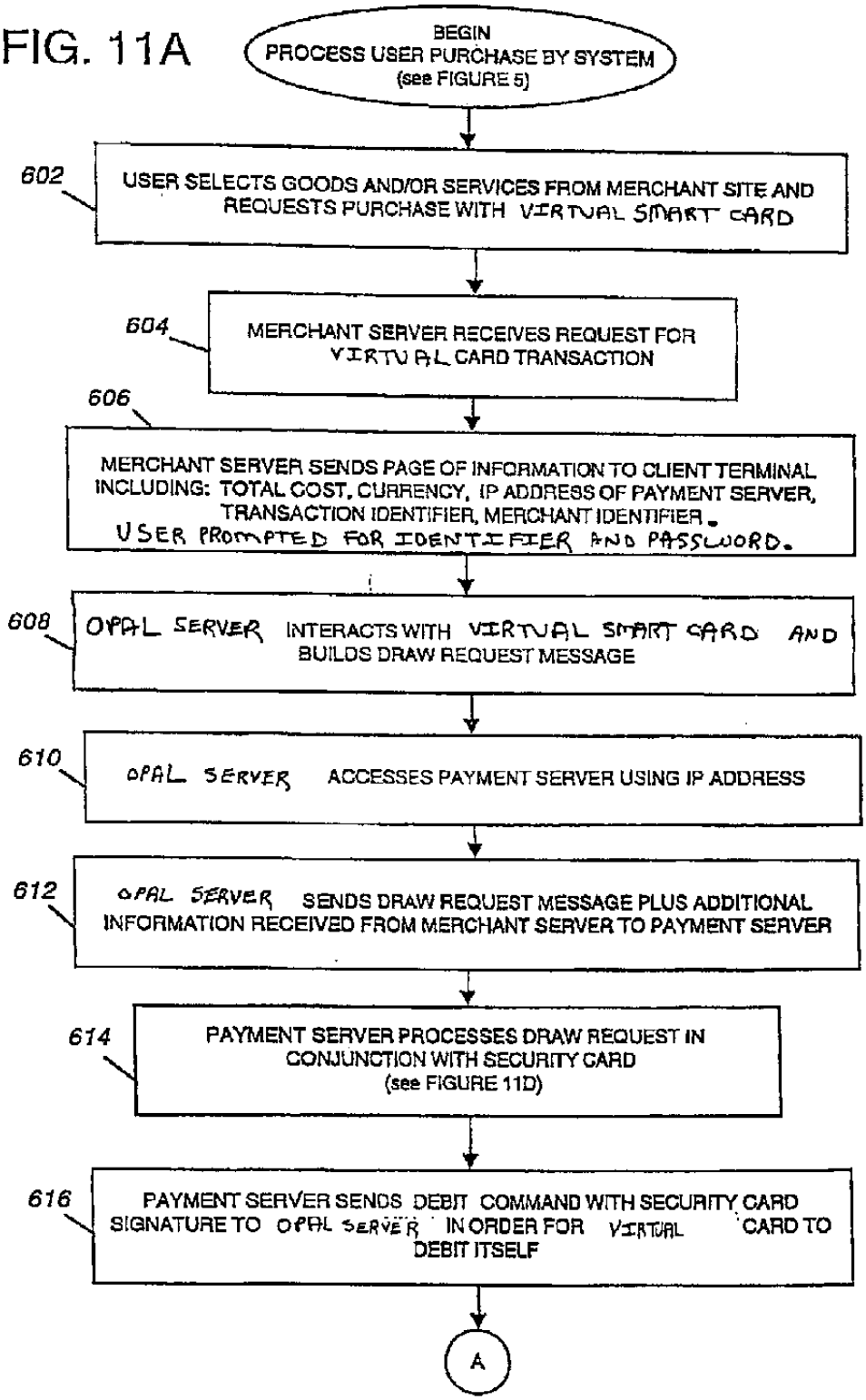
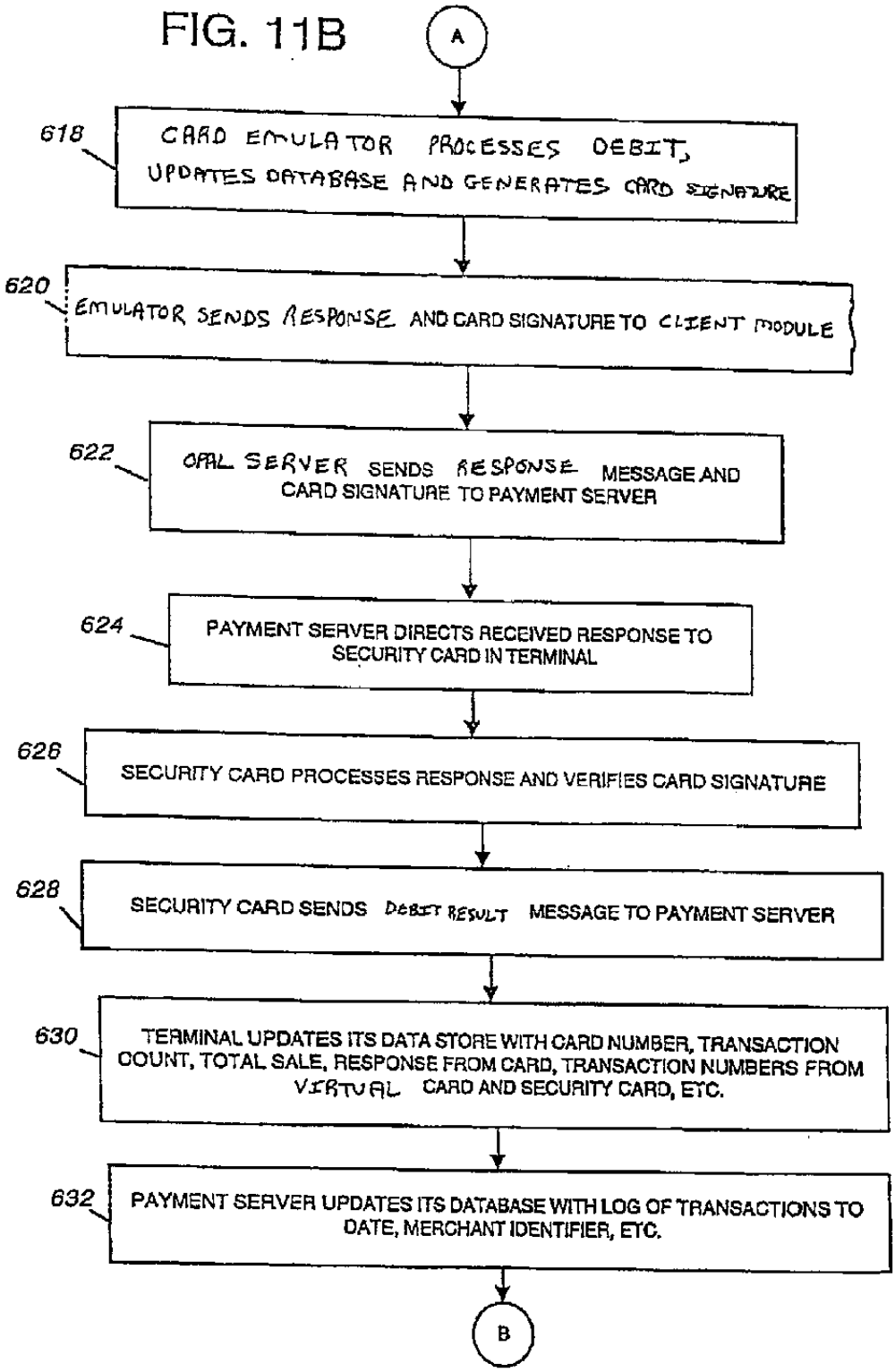

BEGIN
PROCESS USER PURCHASE BY SYSTEM
(see FIGURE 5)
602
USER SELECTS GOODS AND/OR SERVICES FROM MERCHANT SITE AND REQUESTS PURCHASE WITH VIRTUAL SMART CARD
604
MERCHANT SERVER RECEIVES REQUEST FOR VIRTUAL CARD TRANSACTION
606
MERCHANT SERVER SENDS PAGE OF INFORMATION TO CLIENT TERMINAL INCLUDING: TOTAL COST, CURRENCY, IP ADDRESS OF PAYMENT SERVER, TRANSACTION IDENTIFIER, MERCHANT IDENTIFIER. USER PROMPTED FOR IDENTIFIER AND PASSWORD.
608
OPAL SERVER INTERACTS WITH VIRTUAL SMART CARD AND BUILDS DRAW REQUEST MESSAGE
610
OPAL SERVER ACCESSES PAYMENT SERVER USING IP ADDRESS
612
OPAL SERVER SENDS DRAW REQUEST MESSAGE PLUS ADDITIONAL INFORMATION RECEIVED FROM MERCHANT SERVER TO PAYMENT SERVER
614
PAYMENT SERVER PROCESSES DRAW REQUEST IN CONJUNCTION WITH SECURITY CARD
(see FIGURE 11D)
616
PAYMENT SERVER SENDS DEBIT COMMAND WITH SECURITY CARD SIGNATURE TO OPAL SERVER IN ORDER FOR VIRTUAL CARD TO DEBIT ITSELF
A

FIG. 11B


A
618
CARD EMULATOR PROCESSES DEBIT, UPDATES DATABASE AND GENERATES CARD SIGNATURE
620
EMULATOR SENDS RESPONSE AND CARD SIGNATURE TO CLIENT MODULE
622
OPAL SERVER SENDS RESPONSE MESSAGE AND CARD SIGNATURE TO PAYMENT SERVER
624
PAYMENT SERVER DIRECTS RECEIVED RESPONSE TO SECURITY CARD IN TERMINAL
626
SECURITY CARD PROCESSES RESPONSE AND VERIFIES CARD SIGNATURE
628
SECURITY CARD SENDS DEBIT RESULT MESSAGE TO PAYMENT SERVER
630
TERMINAL UPDATES ITS DATA STORE WITH CARD NUMBER, TRANSACTION COUNT, TOTAL SALE, RESPONSE FROM CARD, TRANSACTION NUMBERS FROM VIRTUAL CARD AND SECURITY CARD, ETC.
632
PAYMENT SERVER UPDATES ITS DATABASE WITH LOG OF TRANSACTIONS TO DATE, MERCHANT IDENTIFIER, ETC.
B

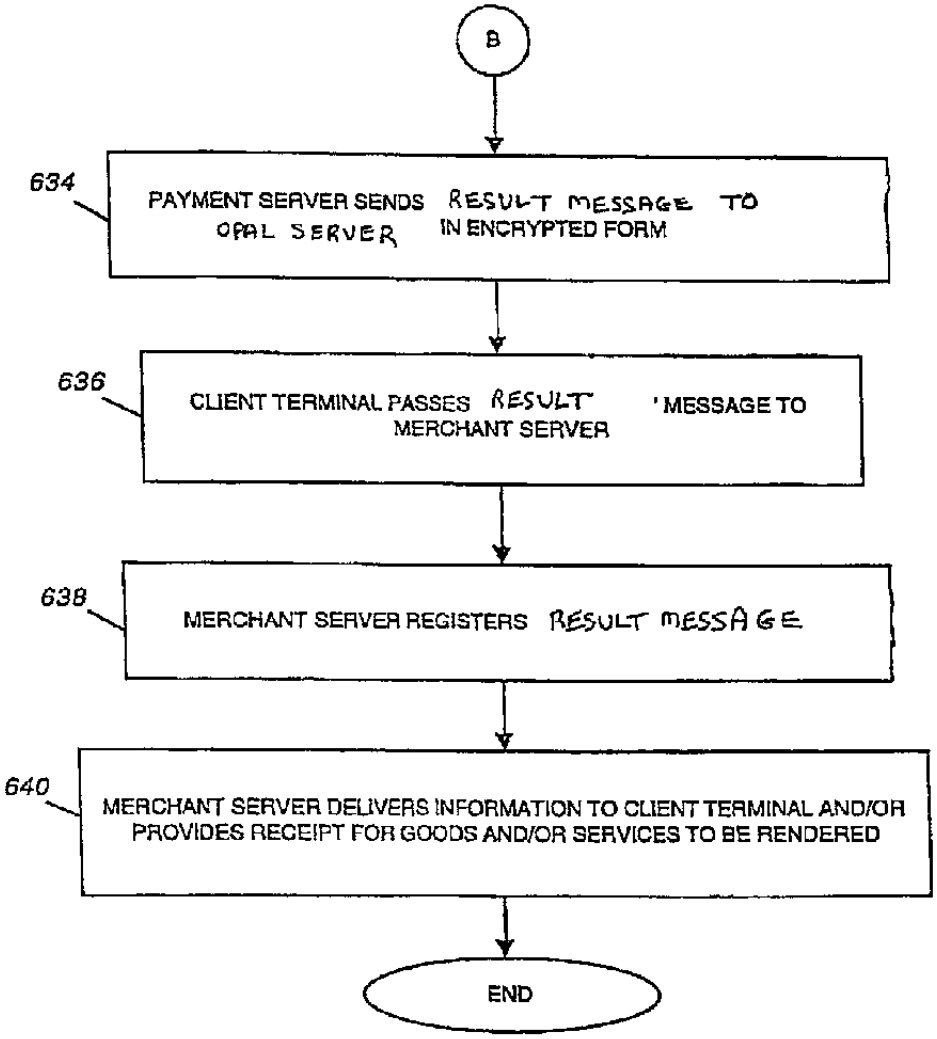
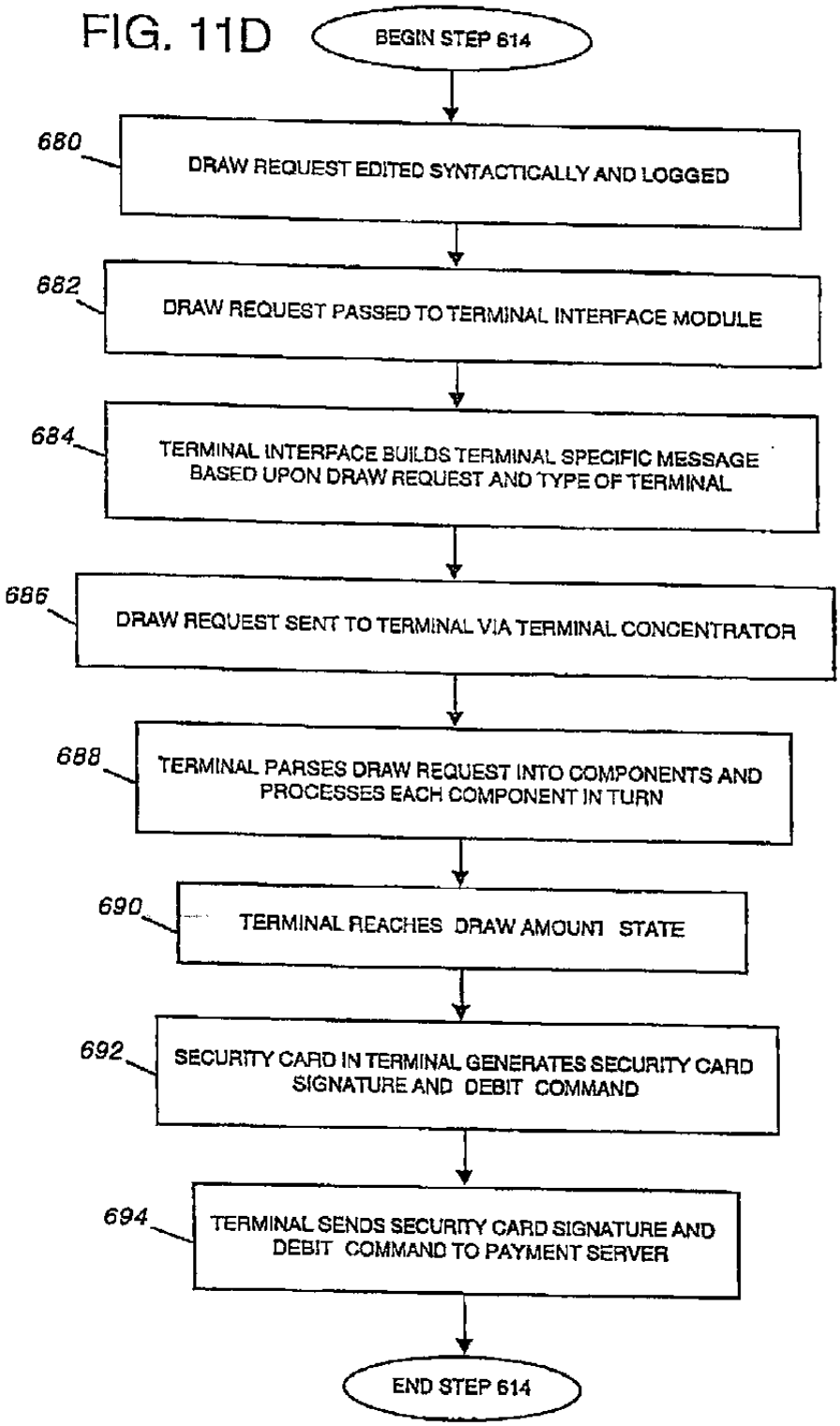

B
634
PAYMENT SERVER SENDS RESULT MESSAGE TO OPAL SERVER IN ENCRYPTED FORM
636
CLIENT TERMINAL PASSES RESULT MESSAGE TO MERCHANT SERVER
638
MERCHANT SERVER REGISTERS RESULT MESSAGE
640
MERCHANT SERVER DELIVERS INFORMATION TO CLIENT TERMINAL AND/OR PROVIDES RECEIPT FOR GOODS AND/OR SERVICES TO BE RENDERED
END

FIG. 11C

FIG. 11D


BEGIN STEP 614
680
DRAW REQUEST EDITED SYNTACTICALLY AND LOGGED
682
DRAW REQUEST PASSED TO TERMINAL INTERFACE MODULE
684
TERMINAL INTERFACE BUILDS TERMINAL SPECIFIC MESSAGE BASED UPON DRAW REQUEST AND TYPE OF TERMINAL
686
DRAW REQUEST SENT TO TERMINAL VIA TERMINAL CONCENTRATOR
688
TERMINAL PARSES DRAW REQUEST INTO COMPONENTS AND PROCESSES EACH COMPONENT IN TURN
690
TERMINAL REACHES DRAW AMOUNT STATE
692
SECURITY CARD IN TERMINAL GENERATES SECURITY CARD SIGNATURE AND DEBIT COMMAND
694
TERMINAL SENDS SECURITY CARD SIGNATURE AND DEBIT COMMAND TO PAYMENT SERVER
END STEP 614

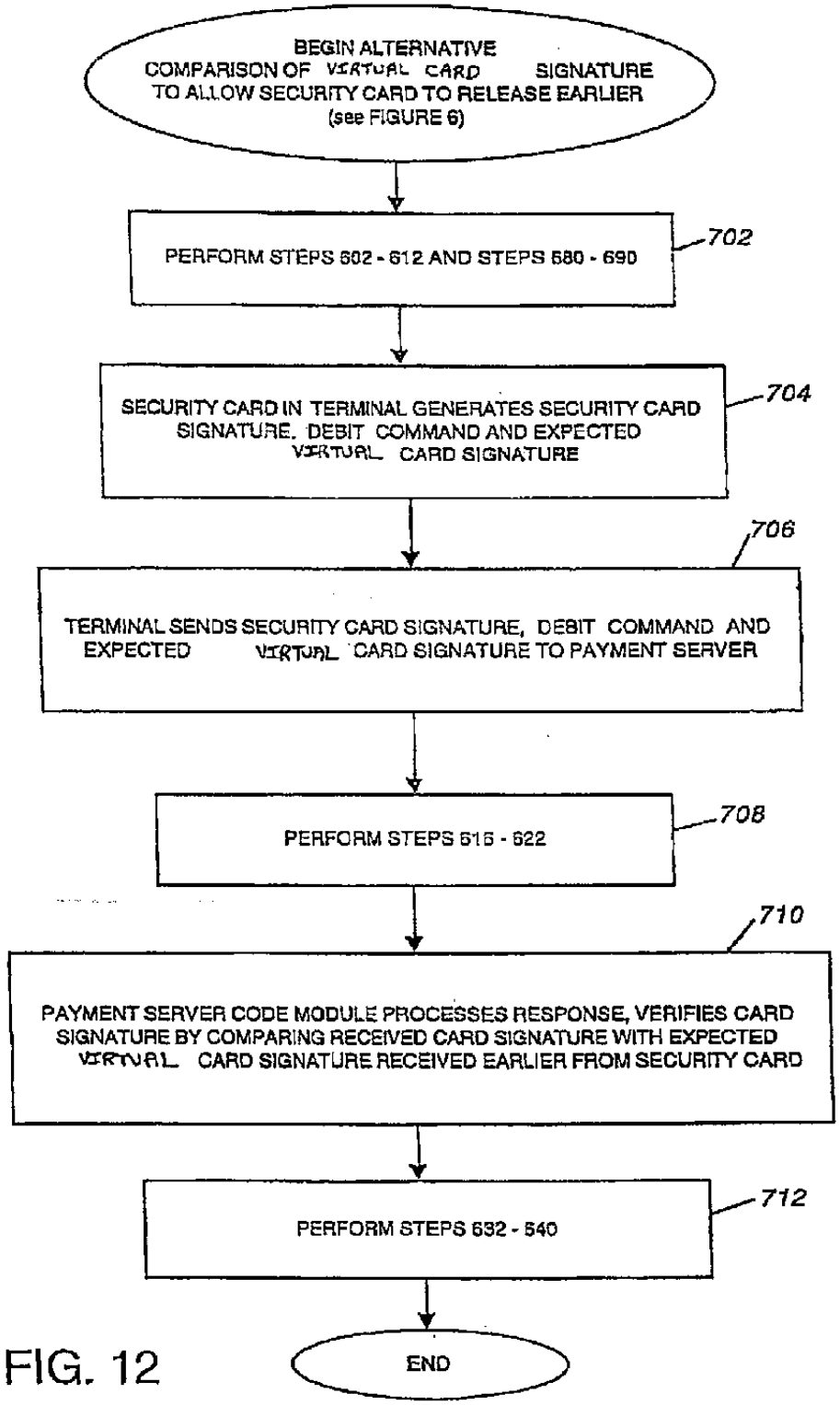

BEGIN ALTERNATIVE COMPARISON OF VIRTUAL CARD SIGNATURE TO ALLOW SECURITY CARD TO RELEASE EARLIER (see FIGURE 6)
PERFORM STEPS 602 - 612 AND STEPS 680 - 690
702
SECURITY CARD IN TERMINAL GENERATES SECURITY CARD SIGNATURE, DEBIT COMMAND AND EXPECTED VIRTUAL CARD SIGNATURE
704
706
TERMINAL SENDS SECURITY CARD SIGNATURE, DEBIT COMMAND AND EXPECTED VIRTUAL CARD SIGNATURE TO PAYMENT SERVER
PERFORM STEPS 615 - 622
708
710
PAYMENT SERVER CODE MODULE PROCESSES RESPONSE, VERIFIES CARD SIGNATURE BY COMPARING RECEIVED CARD SIGNATURE WITH EXPECTED VIRTUAL CARD SIGNATURE RECEIVED EARLIER FROM SECURITY CARD
PERFORM STEPS 632 - 640
712
END

FIG. 12

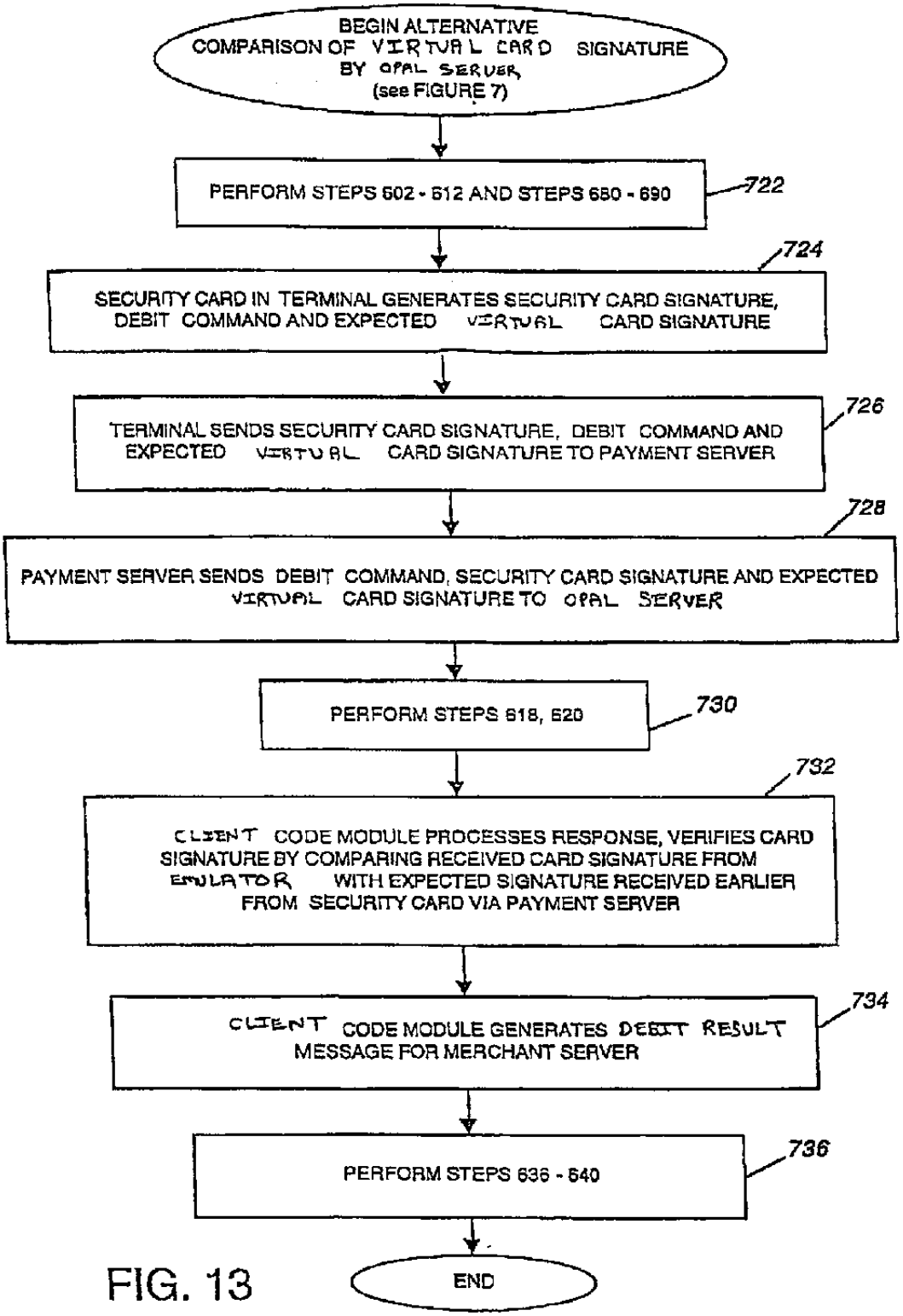

BEGIN ALTERNATIVE COMPARISON OF VIRTUAL CARD SIGNATURE BY OPAL SERVER (see FIGURE 7)
PERFORM STEPS 602 - 612 AND STEPS 680 - 690
722
724
SECURITY CARD IN TERMINAL GENERATES SECURITY CARD SIGNATURE, DEBIT COMMAND AND EXPECTED VIRTUAL CARD SIGNATURE
TERMINAL SENDS SECURITY CARD SIGNATURE, DEBIT COMMAND AND EXPECTED VIRTUAL CARD SIGNATURE TO PAYMENT SERVER
726
728
PAYMENT SERVER SENDS DEBIT COMMAND, SECURITY CARD SIGNATURE AND EXPECTED VIRTUAL CARD SIGNATURE TO OPAL SERVER
PERFORM STEPS 618, 620
730
732
CLIENT CODE MODULE PROCESSES RESPONSE, VERIFIES CARD SIGNATURE BY COMPARING RECEIVED CARD SIGNATURE FROM EMULATOR WITH EXPECTED SIGNATURE RECEIVED EARLIER FROM SECURITY CARD VIA PAYMENT SERVER
CLIENT CODE MODULE GENERATES DEBIT RESULT MESSAGE FOR MERCHANT SERVER
734
PERFORM STEPS 636 - 640
736
END

FIG. 13

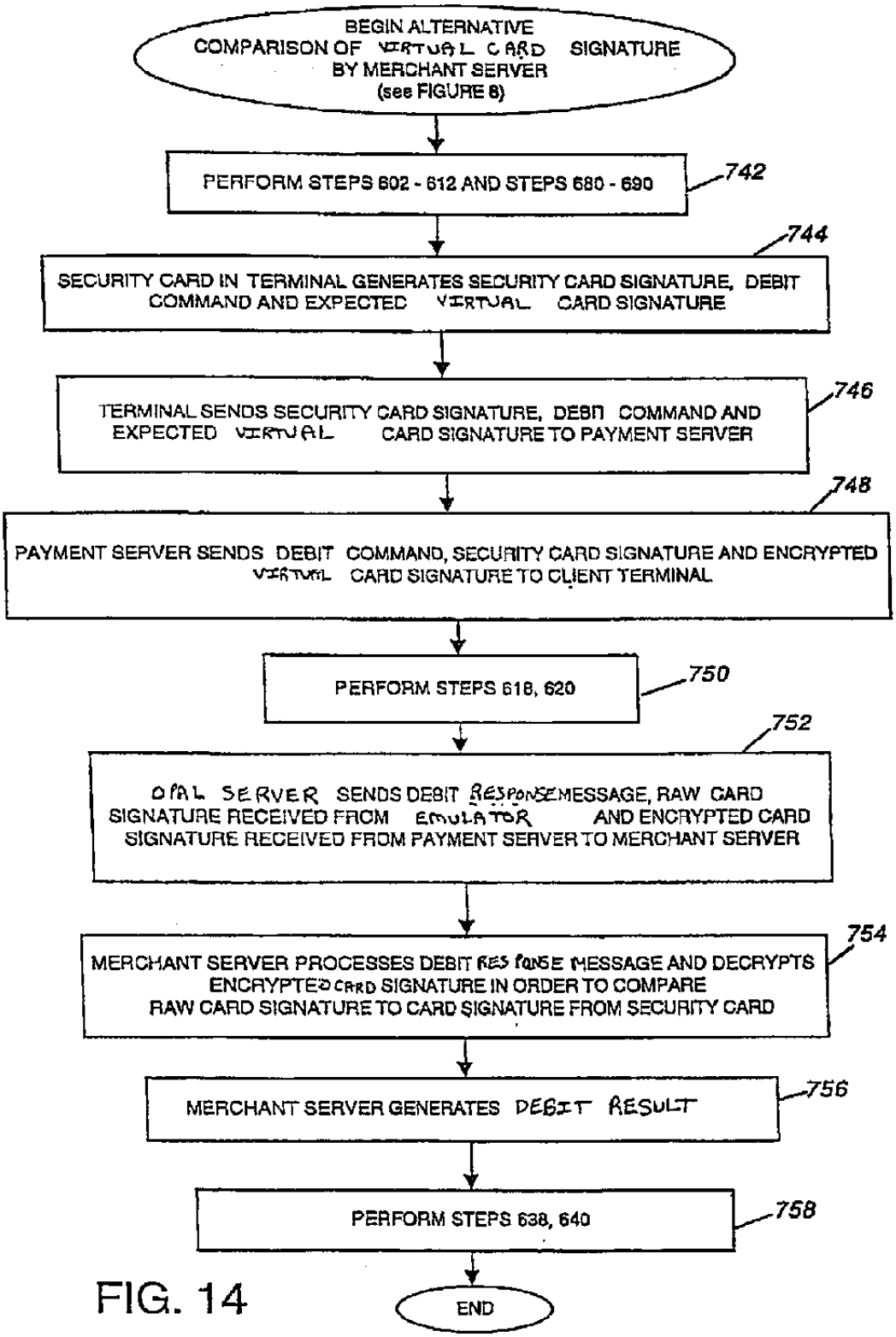

BEGIN ALTERNATIVE COMPARISON OF VIRTUAL CARD SIGNATURE BY MERCHANT SERVER (see FIGURE 8)
PERFORM STEPS 602 - 612 AND STEPS 680 - 690
742
744
SECURITY CARD IN TERMINAL GENERATES SECURITY CARD SIGNATURE, DEBIT COMMAND AND EXPECTED VIRTUAL CARD SIGNATURE
TERMINAL SENDS SECURITY CARD SIGNATURE, DEBIT COMMAND AND EXPECTED VIRTUAL CARD SIGNATURE TO PAYMENT SERVER
746
748
PAYMENT SERVER SENDS DEBIT COMMAND, SECURITY CARD SIGNATURE AND ENCRYPTED VIRTUAL CARD SIGNATURE TO CLIENT TERMINAL
PERFORM STEPS 618, 620
750
752
OPAL SERVER SENDS DEBIT RESPONSE MESSAGE, RAW CARD SIGNATURE RECEIVED FROM EMULATOR AND ENCRYPTED CARD SIGNATURE RECEIVED FROM PAYMENT SERVER TO MERCHANT SERVER
754
MERCHANT SERVER PROCESSES DEBIT RESPONSE MESSAGE AND DECRYPTS ENCRYPTED CARD SIGNATURE IN ORDER TO COMPARE RAW CARD SIGNATURE TO CARD SIGNATURE FROM SECURITY CARD
MERCHANT SERVER GENERATES DEBIT RESULT
756
PERFORM STEPS 638, 640
758
END

FIG. 14

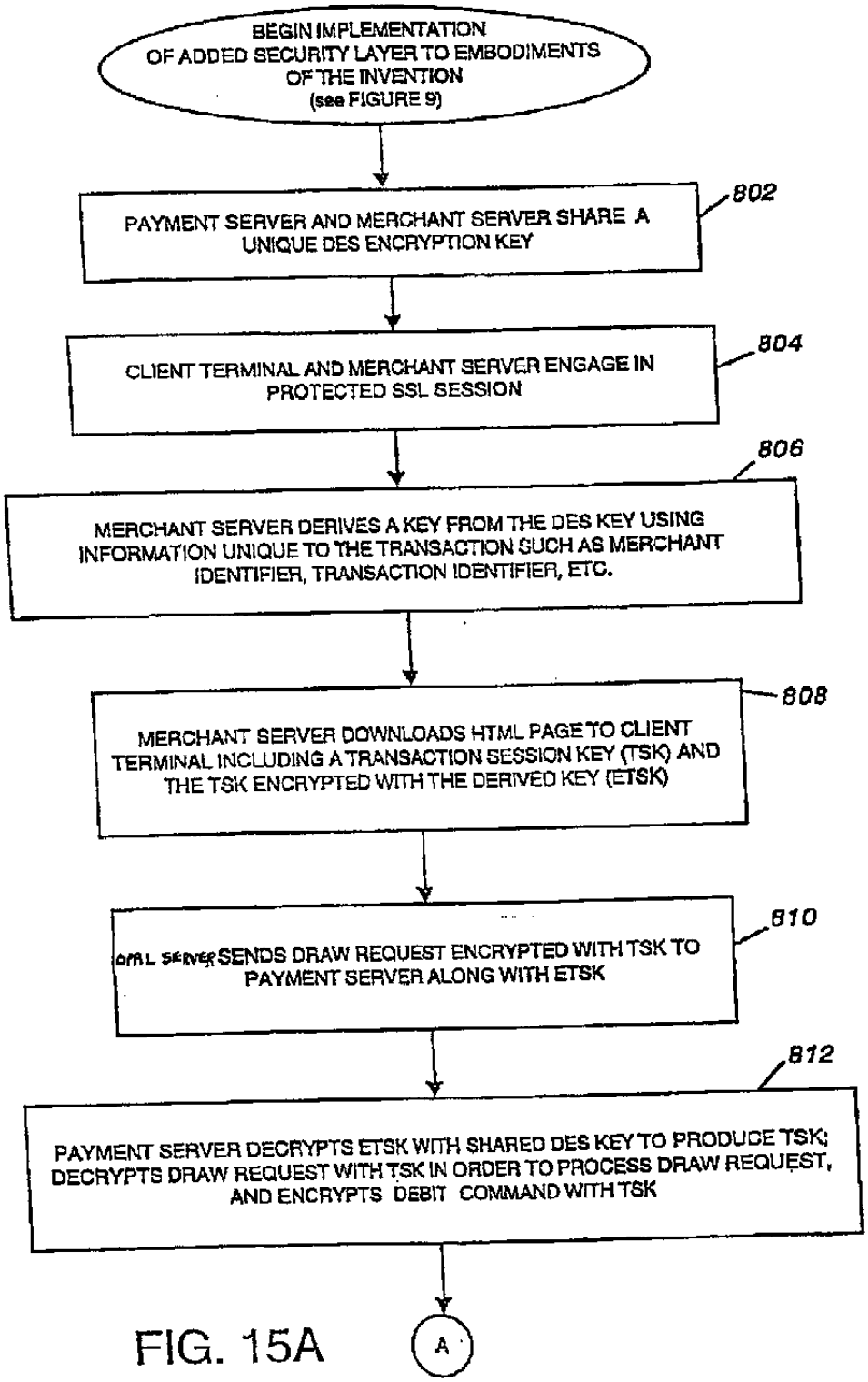

BEGIN IMPLEMENTATION OF ADDED SECURITY LAYER TO EMBODIMENTS OF THE INVENTION (see FIGURE 9)
PAYMENT SERVER AND MERCHANT SERVER SHARE A UNIQUE DES ENCRYPTION KEY
802
CLIENT TERMINAL AND MERCHANT SERVER ENGAGE IN PROTECTED SSL SESSION
804
806
MERCHANT SERVER DERIVES A KEY FROM THE DES KEY USING INFORMATION UNIQUE TO THE TRANSACTION SUCH AS MERCHANT IDENTIFIER, TRANSACTION IDENTIFIER, ETC.
808
MERCHANT SERVER DOWNLOADS HTML PAGE TO CLIENT TERMINAL INCLUDING A TRANSACTION SESSION KEY (TSK) AND THE TSK ENCRYPTED WITH THE DERIVED KEY (ETSK)
810
SENDS DRAW REQUEST ENCRYPTED WITH TSK TO PAYMENT SERVER ALONG WITH ETSK
812
PAYMENT SERVER DECRYPTS ETSK WITH SHARED DES KEY TO PRODUCE TSK; DECRYPTS DRAW REQUEST WITH TSK IN ORDER TO PROCESS DRAW REQUEST, AND ENCRYPTS DEBIT COMMAND WITH TSK
A

FIG. 15A

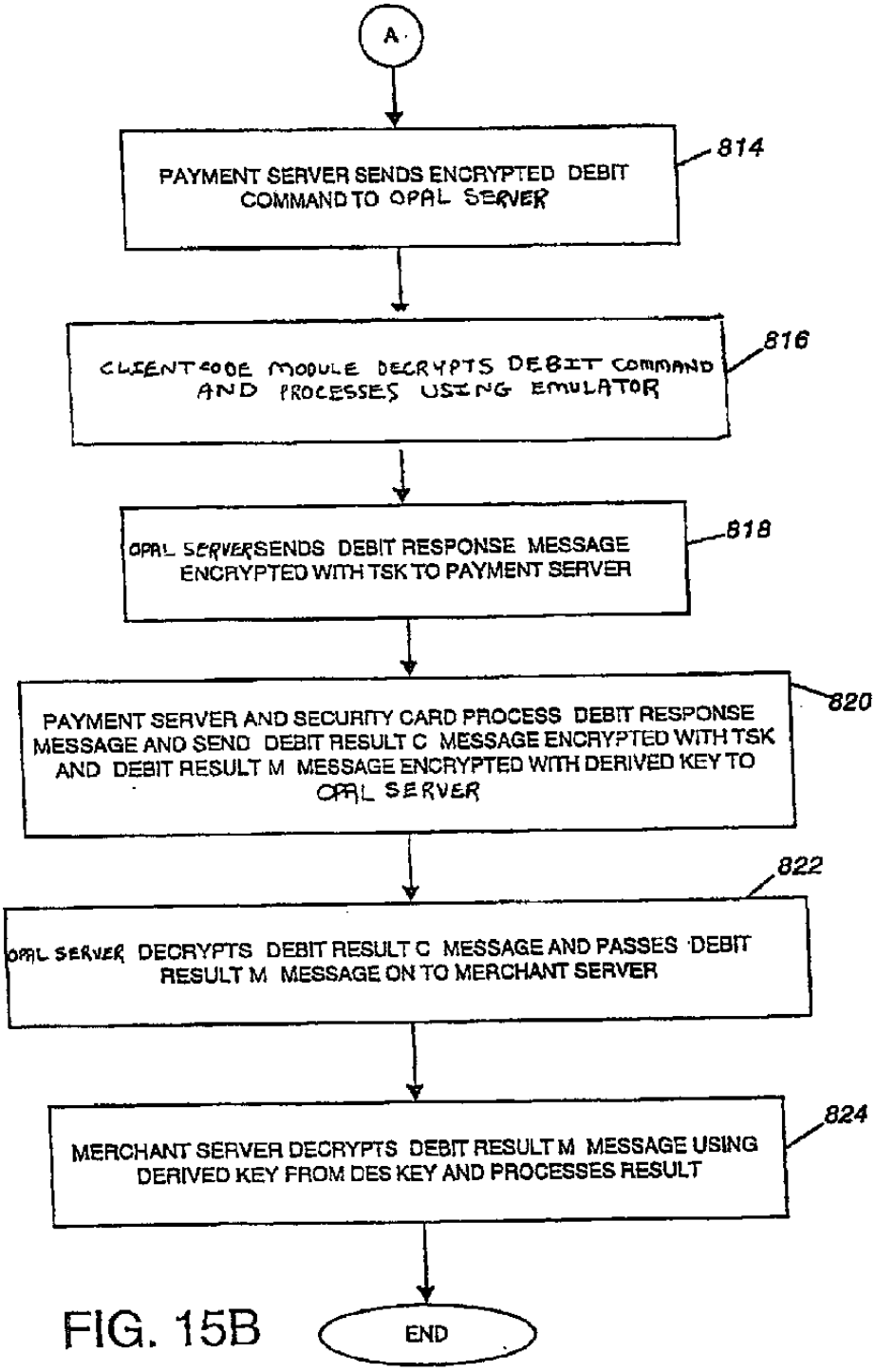

A
PAYMENT SERVER SENDS ENCRYPTED DEBIT COMMAND TO OPAL SERVER
814
CLIENT CODE MODULE DECRYPTS DEBIT COMMAND AND PROCESSES USING EMULATOR
816
OPAL SERVER SENDS DEBIT RESPONSE MESSAGE ENCRYPTED WITH TSK TO PAYMENT SERVER
818
PAYMENT SERVER AND SECURITY CARD PROCESS DEBIT RESPONSE MESSAGE AND SEND DEBIT RESULT C MESSAGE ENCRYPTED WITH TSK AND DEBIT RESULT M MESSAGE ENCRYPTED WITH DERIVED KEY TO OPAL SERVER
820
822
OPAL SERVER DECRYPTS DEBIT RESULT C MESSAGE AND PASSES DEBIT RESULT M MESSAGE ON TO MERCHANT SERVER
MERCHANT SERVER DECRYPTS DEBIT RESULT M MESSAGE USING DERIVED KEY FROM DES KEY AND PROCESSES RESULT
824
END

FIG. 15B

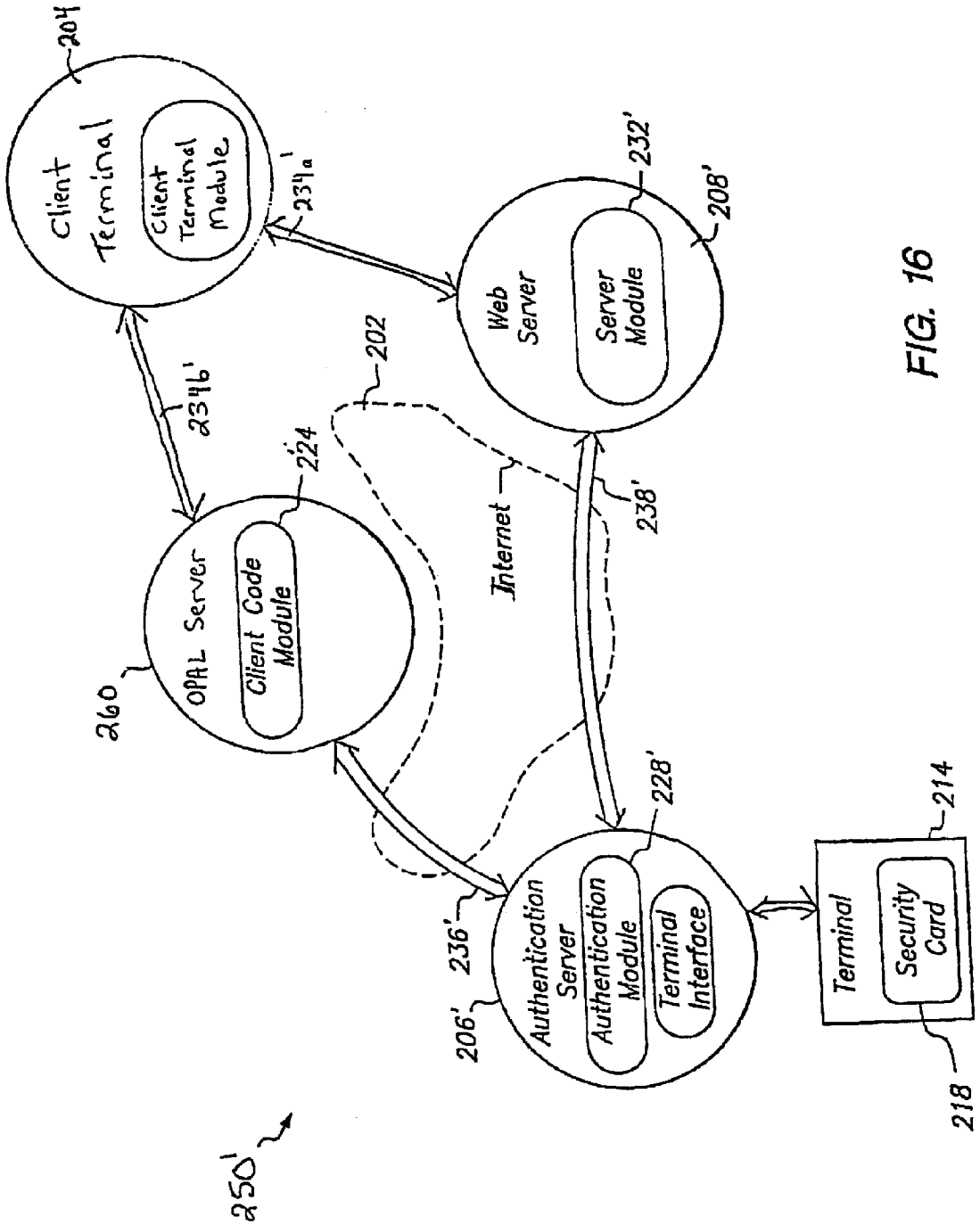


FIG. 16

Mastercard, Ex1002, p. 475

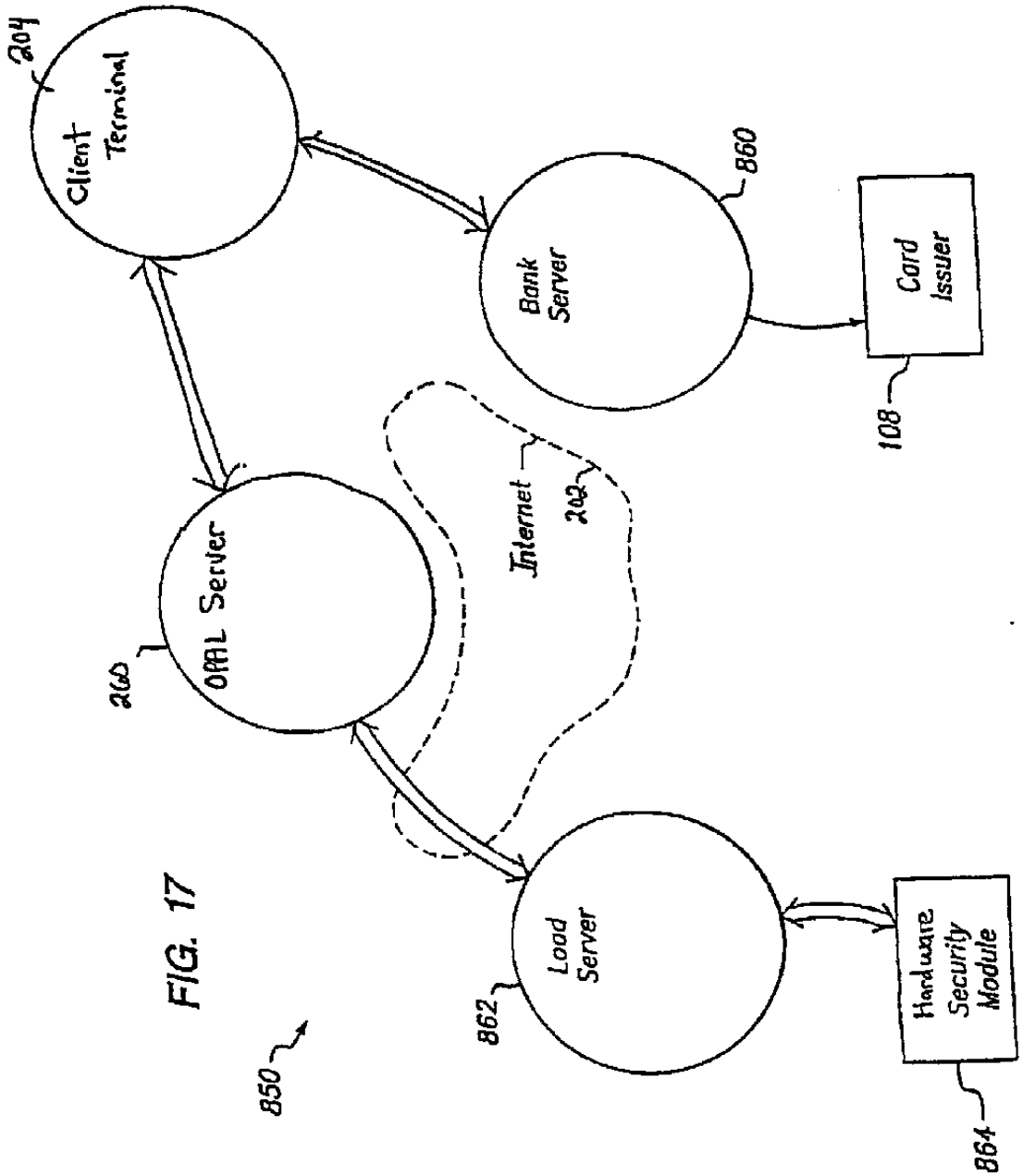

204
Client Terminal
860
Bank Server
Card Issuer
108
Internet
202
ORL Server
260
Load Server
862
Hardware Security Module
864
850

FIG. 17

FIG. 18A

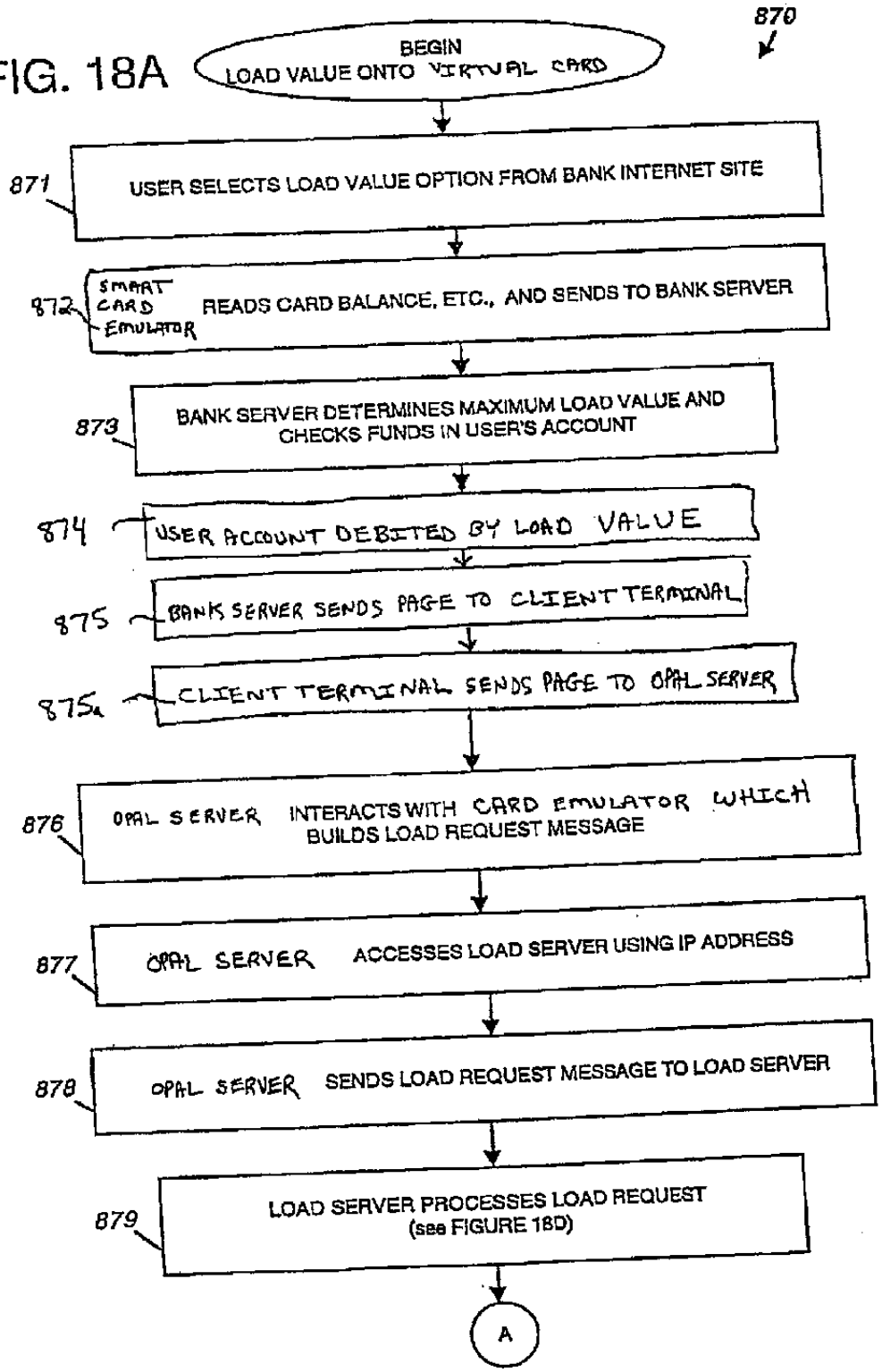
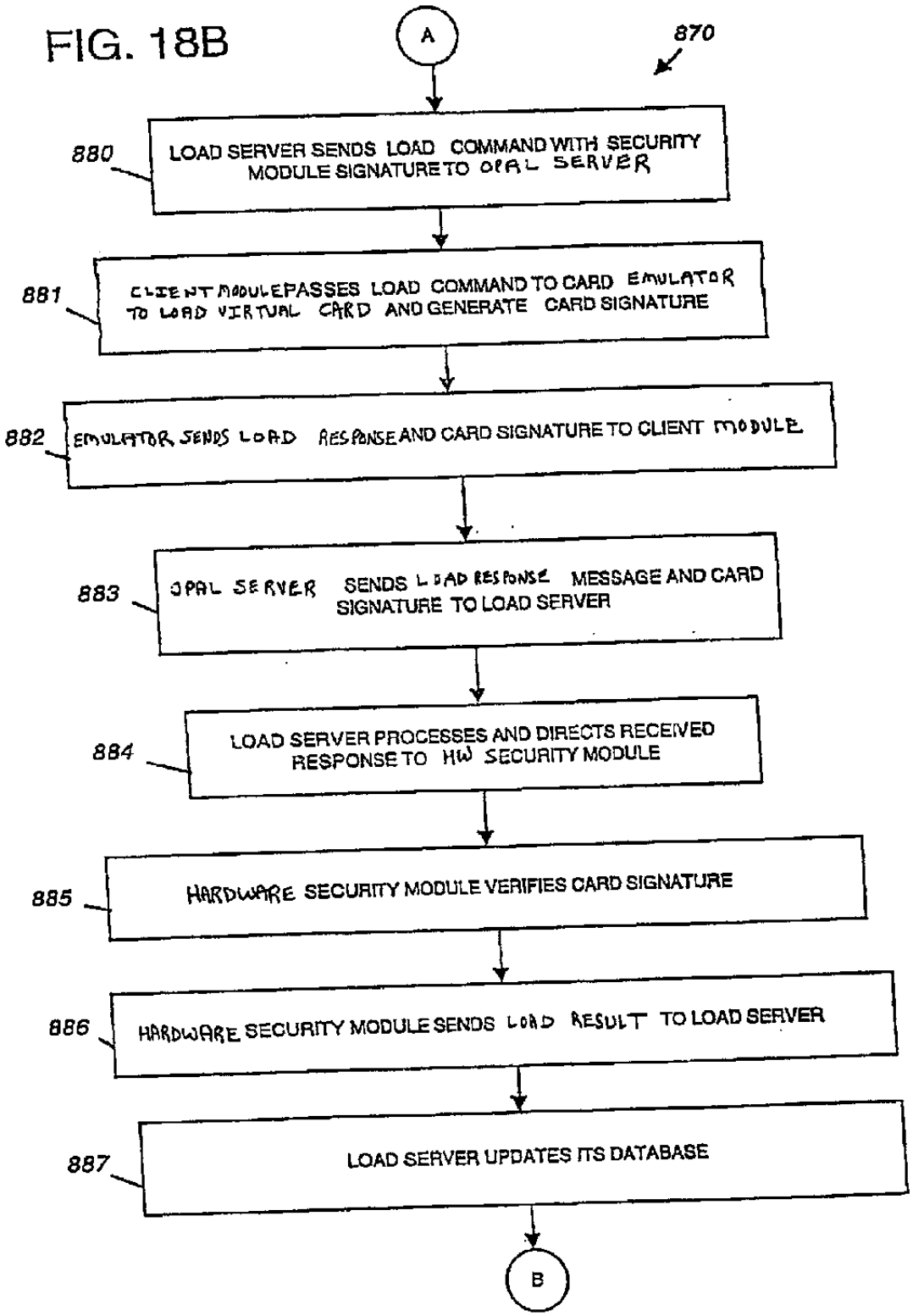
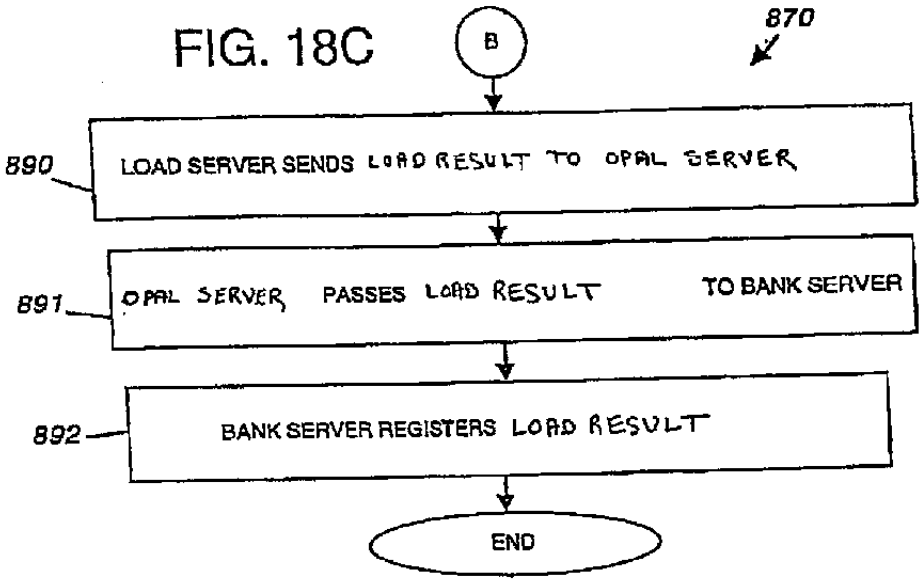

870
BEGIN
LOAD VALUE ONTO VIRTUAL CARD
871
USER SELECTS LOAD VALUE OPTION FROM BANK INTERNET SITE
872
SMART CARD EMULATOR
READS CARD BALANCE, ETC., AND SENDS TO BANK SERVER
873
BANK SERVER DETERMINES MAXIMUM LOAD VALUE AND CHECKS FUNDS IN USER'S ACCOUNT
874
USER ACCOUNT DEBITED BY LOAD VALUE
875
BANK SERVER SENDS PAGE TO CLIENT TERMINAL
875a
CLIENT TERMINAL SENDS PAGE TO OPAL SERVER
876
OPAL SERVER INTERACTS WITH CARD EMULATOR WHICH BUILDS LOAD REQUEST MESSAGE
877
OPAL SERVER ACCESSES LOAD SERVER USING IP ADDRESS
878
OPAL SERVER SENDS LOAD REQUEST MESSAGE TO LOAD SERVER
879
LOAD SERVER PROCESSES LOAD REQUEST
(see FIGURE 18D)
A

FIG. 18B



Mastercard, Ex1002, p. 478

FIG. 18C



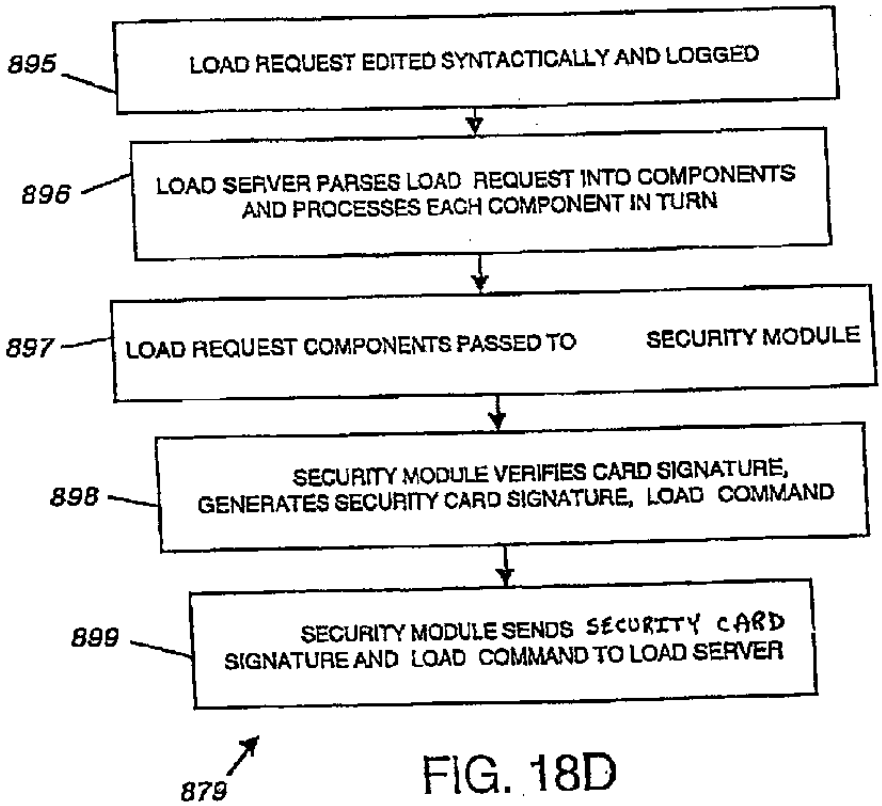


FIG. 18D

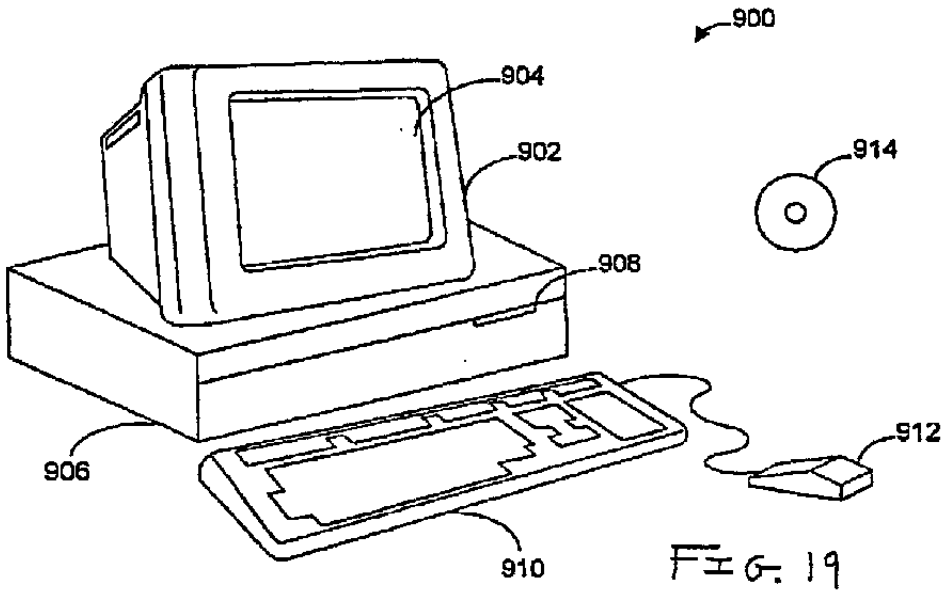

900
904
902
914
908
912
906
910

FIG. 19

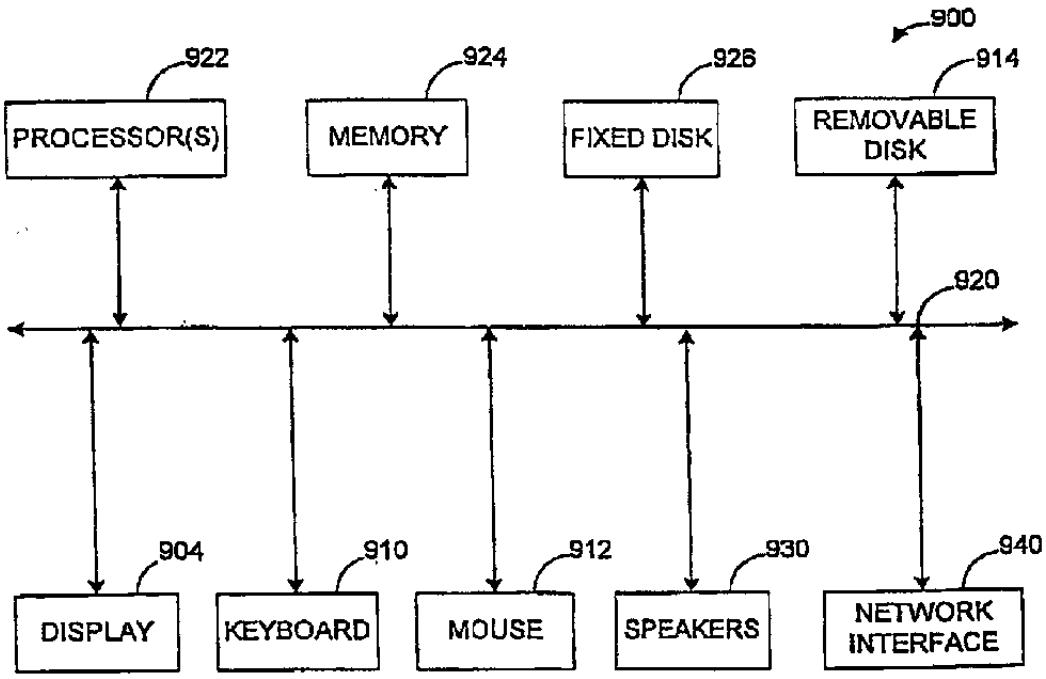

900
922
924
926
914
PROCESSOR(S)
MEMORY
FIXED DISK
REMOVABLE DISK
920
904
910
912
930
940
DISPLAY
KEYBOARD
MOUSE
SPEAKERS
NETWORK INTERFACE

FIG. 20

INTERNATIONAL SEARCH REPORT

Intern. tal Application No
PCT/US 00/19984

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 883 810 A (ROSEN DANIEL ET AL) 16 March 1999 (1999-03-16) column 1, line 65 -column 2, line 20 column 3, line 25 -column 4, line 55 column 8, line 37 -column 10, line 30 ---	1-33
A	EP 0 917 120 A (CITICORP DEV CENTER INC) 19 May 1999 (1999-05-19) column 4, line 24 - line 27 column 4, line 46 - line 57 column 8, line 43 -column 10 column 12, line 28 - line 45 column 14, line 20 -column 15, line 41 --- -/--	1-33

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 December 2000	02/01/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Wolles, B

1

Form PCT/ISA/210 (second sheet) (July 1992)

Mastercard, Ex1002, p. 481

INTERNATIONAL SEARCH REPORT

Intern. ial Application No
PCT/US 00/19984

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99 10850 A (CHASE MANHATTAN BANK) 4 March 1999 (1999-03-04) page 5, paragraph 1 page 14, line 14 -page 15, line 10 claim 1	1-11
A	WO 98 49658 A (VISA INT SERVICE ASS) 5 November 1998 (1998-11-05) cited in the application abstract	

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

Mastercard, Ex1002, p. 482

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern. ...al Application No
PCT/US 00/19984

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5883810	A	16-03-1999	NONE		
EP 0917120	A	19-05-1999	AU	1584499 A	31-05-1999
			AU	1796599 A	31-05-1999
			AU	9234698 A	03-06-1999
			BR	9806416 A	16-11-1999
			CN	1233804 A	03-11-1999
			EP	0917119 A	19-05-1999
			EP	0950972 A	20-10-1999
			JP	11250165 A	17-09-1999
			JP	11232348 A	27-08-1999
			WO	9924891 A	20-05-1999
			WO	9924892 A	20-05-1999
			EP	0951158 A	20-10-1999
			EP	0950992 A	20-10-1999
			JP	2000036049 A	02-02-2000
			JP	2000076189 A	14-03-2000
			JP	2000251006 A	14-09-2000
WO 9910850	A	04-03-1999	AU	8400098 A	16-03-1999
			EP	1010149 A	21-06-2000
WO 9849658	A	05-11-1998	AU	7272698 A	24-11-1998
			EP	1003139 A	24-05-2000
			EP	1023705 A	02-08-2000
			US	6105008 A	15-08-2000

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 February 2009 (05.02.2009)

PCT

(10) International Publication Number
WO 2009/017754 A1

(51) International Patent Classification:
G06Q 40/00 (2006.01)

(21) International Application Number:
PCT/US2008/009200

(22) International Filing Date: 30 July 2008 (30.07.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/881,920 30 July 2007 (30.07.2007) US

(71) Applicant *(for all designated States except US)*: **EBAY INC.** [US/US]; 2145 Hamilton Avenue, San Jose, California 95125 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **MURPHY, Timothy** [US/US]; 7 West 41st Avenue, PMB #420, San Mateo, California 94403 (US).

(74) Agents: **STEFFEY, Charles E.** et al.; Schwegman, Lundberg & Woessner, P.A., P.O. Box 2938, Minneapolis, Minnesota 55402 (US).

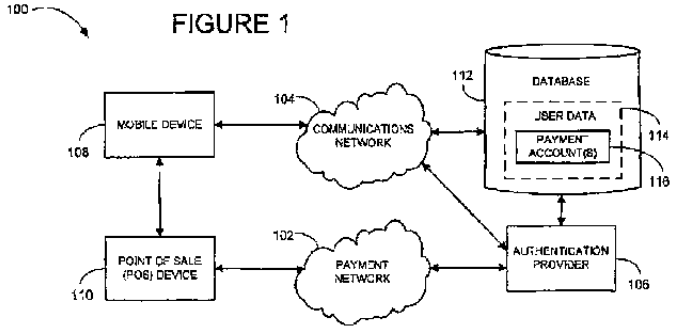
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(54) Title: METHOD AND SYSTEM FOR DYNAMIC FUNDING

FIGURE 1



(57) Abstract: An identifier of a mobile device may be accessed. The identifier may be associated with a payment account. A single use authentication code relating to the identifier may be generated. The single use authentication code may be capable of being used to authenticate the mobile device at a point of sale (POS) device and enable a funds adjustment to the payment account. The single use authentication code may be provided to the mobile device through a communications network.

WO 2009/017754 A1

METHOD AND SYSTEM FOR DYNAMIC FUNDING

RELATED MATTERS

This application claims the benefit of United States Patent Application Serial No. 11/881,920 filed July 30, 2007 ("METHOD AND SYSTEM FOR DYNAMIC FUNDING"), which application is incorporated herein by reference in its entirety.

BACKGROUND

A payment card (e.g., a credit card) may be used to authenticate payment from a payment account. A cryptographic key may be included in a magnetic stripe of the payment card and used at a point of sale to identify whether the card is a legitimate card. The information in the magnetic stripe may be subject to unauthorized capture, thereby compromising both the payment account and the card. A nefarious user that has made that unauthorized capture may be able to withdraw funds from the payment account using the card one or more times before the unauthorized activity is detected.

BRIEF DESCRIPTION OF THE DRAWINGS

Some embodiments are illustrated by way of example and not limitation in the figures of the accompanying drawings in which:

Figure 1 is a block diagram of a system, according to an example embodiment;

Figure 2 is a block diagram of an example authentication provider that may be deployed within the system of Figure 1 according to an example embodiment;

Figure 3 is a block diagram of an example mobile device that may be deployed within the system of Figure 1 according to an example embodiment;

Figure 4 is a block diagram of an example point of sale device that may be deployed within the system of Figure 1 according to an example embodiment;

Figure 5 is a flowchart illustrating a method for funding authentication according to an example embodiment;

Figures 6-8 are flowcharts illustrating a method for processing payment authorization for the payment account according to an example embodiment;

Mastercard, Ex1002, p. 485

Figure 9 is a flowchart illustrating a method for funding authentication according to an example embodiment;

Figure 10 is a flowchart illustrating a method for processing payment authorization according to an example embodiment;

Figure 11 is a flowchart illustrating a method for utilizing a mobile device according to an example embodiment;

Figure 12 is a flowchart illustrating a method for utilizing a point of sale device according to an example embodiment;

Figure 13 is a network diagram depicting a network system, according to one embodiment, having a client server architecture configured for exchanging data over a network;

Figure 14 is a block diagram illustrating an example embodiment of multiple network and marketplace applications, which are provided as part of the network-based marketplace; and

Figure 15 is a block diagram diagrammatic representation of machine in the example form of a computer system within which a set of instructions for causing the machine to perform any one or more of the methodologies discussed herein may be executed.

DETAILED DESCRIPTION

Example methods and systems for dynamic funding authentication are described. In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of example embodiments. It will be evident, however, to one skilled in the art that the present invention may be practiced without these specific details.

In an example embodiment, an identifier of a mobile device may be accessed. The identifier may be associated with a payment account. A single use authentication code relating to the identifier may be generated. The single use authentication code may be capable of being used to authenticate the mobile device at a point of sale (POS) device and enable a funds adjustment to the payment account. The single use authentication code may be provided to the mobile device through a communications network.

In an example embodiment, an identifier of a first mobile device of a first user may be accessed. The identifier of the first mobile device may be

Mastercard, Ex1002, p. 486

associated with a payment account of the first user. A single use authentication code relating to the identifier of the first mobile device may be generated. The single use authentication code may be capable of being used to authenticate a second mobile device of a second user at a POS device and enable a funds adjustment to the payment account of the first user. The single use authentication code may be provided to the second mobile device through a communications network.

In an example embodiment, funding authorization may be requested from an authentication provider through a mobile device. A single use authentication code may be received from the authentication provider. The single use authentication code may be capable of being used to authenticate the mobile device at a POS device and enable a funds adjustment to the payment account. The single use authentication code may be provided through the mobile device.

In an example embodiment, a single use authentication code may be received from a mobile device. The single use authentication code and a funding request may be provided over a payment network to an authentication provider. Funds adjustment related to the funding request may be received from the authentication provider.

Figure 1 illustrates an example system 100 in which an authentication provider 106 may communicate with a mobile device 108 through a communications network 104 and a POS device 110 through a payment network 102. The system 100 may enable a user of the mobile device 108 to be dynamically authenticated for payment with the authentication provider 106 using the mobile device 108 at the POS device 110.

The payment network 102 may be a network used by a credit card company, a debit card company, a bank, or other institution for authorization of financial or other transactions. The payment network 102 may be deployed over the Internet, intranet, and/or other type of local or global network.

The communications network 104 may be a Global System for Mobile Communications (GSM) network, an Internet Protocol (IP) network, a Wireless Application Protocol (WAP) network, a WiFi network, or a IEEE 802.11 standards network as well as various combinations thereof. Other conventional and/or later developed wired and wireless networks may also be used. In an

Mastercard, Ex1002, p. 487

example embodiment, the payment network 102 and the communications network 104 may be the same network.

The mobile device 108 may be a mobile phone, a personal digital assistant (PDA), a gaming unit, a portable computing unit, and the like. A user may use the mobile device 108 to obtain dynamic authentication for purchasing one or more items in a location (e.g., a store) in which the POS device 110 is located. The user may request that the dynamic authentication be made, or the dynamic authentication may occur automatically when a user is in proximity to the POS device 110

The authentication provider 106 may retain an identifier (e.g. a SIM card number) associated with the mobile device 108 in memory and/or stored in the user data 114 of the database 112. The identifier may enable a payment account 116 of a user to be linked to the mobile device 108 of the user or another authorized user (e.g., a child or spouse of the user associated with the payment account 116). Each user of the authentication provider 106 may have a separate payment account 116.

Figure 2 is an example of an authentication provider 106 that may be deployed in the system 100 (see Figure 1) or another system according to an example embodiment. The authentication provider 106 may include an authorization creation subsystem 202, an authorization utilization subsystem 204, and/or another subsystem.

The authorization creation subsystem 202 may include a funding request module 206, an identifier access module 208, an authentication code generation module 210, a code providing module 212, an identifier provider module 214, an identifier receiver module 216, a communication request module 218, and/or a communication receiver module 220. Other modules may also be used.

The funding request module 206 receives a request for funding authorization from the mobile device 108. The request for funding authorization may be received when the mobile device 108 is in proximity to the POS device 110 and a user is seeking dynamic authentication.

The identifier access module 208 accesses the identifier of the mobile device 108. The identifier access module 208 may associate the payment account 116 with the identifier of the mobile device 108 and/or the identifier of the mobile device 108 may already be associated with the payment account 116

Mastercard, Ex1002, p. 488

of a user. The association links the payment account 116 to the mobile device 108.

The authentication code generation module 210 generates a single use authentication code relating to the identifier. The single use authentication code may be capable of being used to authenticate the mobile device 108 at the POS device 110 and enable a funds adjustment to the payment account 116 of a user.

The code providing module 212 provides the single use authentication code and an optional access code to the mobile device 108 through the communications network 104. The access code may be capable of being used by a user at a terminal of the POS device 110 to authorize the funds adjustment.

The identifier provider module 214 sends an identifier request for the identifier to the mobile device provider (e.g., AT&T Knowledge Ventures or Sprint Nextel) and/or the mobile device 108. The identifier receiver module 216 receives the identifier of the mobile device 108 from the mobile device provider and/or the mobile device 108. The received identifier may be stored in the user data 114.

The communication request module 218 sends a communication request message to the mobile device 108 including a request for a request for a confirmation code. The communication receiver module 220 receives the confirmation code from the mobile device 108. The receipt of the confirmation code may confirm that the user is in possession of the mobile device 108.

The authorization utilization subsystem 204 may include an authentication receiver module 222, an account identification module 224, a funds availability module 226, a funds withdrawal module 228, a notification module 230, a funds evaluation module 232, an account adjustment module 234, a conference request module 236, a user determination module 238, and/or an account authorization module 240. Other modules may also be used.

The authentication receiver module 222 receives a funds adjustment request and the single use authentication code from the POS device 110 through the payment network 102. The account identification module 224 identifies the payment account 116 associated with the identifier related to the single use authentication code.

The funds availability module 226 determines availability of funds in the payment account 116 of a user for an amount indicated in the funds adjustment

Mastercard, Ex1002, p. 489

request. The funds withdrawal module 228 withdraws funds in the amount from the payment account of the user.

The notification module 230 sends a notification. The notification may be, by way of example, a notification that the funds in a particular amount have been withdrawn from the payment account 116 of a user, a notification that the payment account 116 has been adjusted by the amount, a notification identifying a merchant that has been provided the amount, or a notification identifying one or more items have been purchased with the amount. Other notifications may also be used.

The funds evaluation module 232 evaluates the funds adjustment request against an evaluation criterion. The account adjustment module 234 adjusts the payment account 116 of a user by the amount. The conference request module 236 sends a confirmation request to the mobile device 108 and receives a response to the confirmation request.

The user determination module 238 determines whether a first user associated with the payment account 116 has authorized adjustment by an amount indicated in the funds adjustment request for a second user associated with the mobile device 108. The account authorization module 240 receives account authorization for a second user from a first user.

Figure 3 is an example of a mobile device 108 that may be deployed in the system 100 (see Figure 1) or another system according to an example embodiment. The mobile device 108 may include a mobile processing subsystem 302 and/or another subsystem.

The mobile processing subsystem 302 may include a funding request receiver module 304, an authorization request module 306, a code receiver module 308, an authentication providing module 310, a presentation module 312, a pattern generation module 314, a confirmation request receiver module 316, a response receiver module 318, and/or a response provider module 320. Other modules may also be used.

The funding request receiver module 304 receives a funding request from a user of the mobile device 108. The authorization request module 306 requests funding authorization from the authentication provider 106 through the mobile device 108.

Mastercard, Ex1002, p. 490

The code receiver module 308 receives a single use authentication code and an optional access code from the authentication provider 106. The single use authentication code may be capable of being used to authenticate the mobile device 108 at the POS device 110 and enable a funds adjustment to the payment account 116. The access code may be capable of being used with a terminal of the POS device 110 to authorize the funds adjustment.

The authentication providing module 310 provides the single use authentication code and an optional authorization routing number through the mobile device 108. The authorization routing number may be capable of being used to identify the authentication provider 106 associated with the payment account 116. For example, the authorization routing number may be used to select the payment network 102 from a number of available payment networks from a number of authentication providers.

The presentation module 312 presents the access code, the single use authentication code, a single use pattern, a confirmation request, and/or the authorization routing number on a display of the mobile device 108.

The pattern generation module 314 generates a single use pattern (e.g., a bar code) from the single use authentication code and the authorization routing number. The single use pattern may be capable of being scanned by the POS device 110.

The confirmation request receiver module 316 receives a confirmation request from the authentication provider 106. The response receiver module 318 receives a response to the confirmation request. The response provider module 320 provides the response to the authentication provider 106.

Figure 4 is an example of a POS device 110 that may be deployed in the system 100 (see Figure 1) or another system according to an example embodiment. The POS device 110 may include a POS processing subsystem 402 and/or another subsystem.

The POS processing subsystem 402 may include a selection receiver module 404, a total generation module 406, a presentation module 408, an authentication receiver module 410, an authentication provider module 412, an adjustment receiver module 414, and/or a network determination module 416. Other modules may also be used.

Mastercard, Ex1002, p. 491

The selection receiver module 404 receives a selection of one or more items (e.g., for purchase). The total generation module 406 generates a total for the selection. The presentation module 408 presents the total for the selection on a display of the POS device 110.

The authentication receiver module 410 receives a single use authentication code and an optional authorization routing number from the mobile device 108. The authentication provider module 412 provides the single use authentication code and a funding request over the payment network 102 to the authentication provider 106.

The adjustment receiver module 414 receives funds adjustment related to the funding request from the authentication provider 106. The network determination module 416 determines the payment network 102 from among a number of available payment networks based on the authorization routing number.

Figure 5 illustrates a method 500 for funding authentication according to an example embodiment. The method 500 may be performed by the authentication provider 106 (see Figure 1) or another provider.

A request for funding authorization may be received from the mobile device 108 at block 502. The request may be sent from the mobile device 108 through the communications network 104. The request may be sent via a text message, an e-mail, a SMS message, or the like.

An identifier of the mobile device 108 is accessed at block 504. The identifier may be unique or substantially unique (e.g., to distinguish the mobile device 108 of one user from other users). The identifier may be associated with the payment account 116 of a user. The identifier may be stored on a Subscriber Identity Module (SIM) card of the mobile device 108, a Removable User Identity Module (RUIM) of the mobile device 108, and/or known by a mobile device provider. The payment account 116 may be associated with the identifier of the mobile device 108 during the operations of block 504 or prior to initiating the operations of block 504.

In an example embodiment, the association of the payment account 116 with the identifier may include, by way of example, sending an identifier request for the identifier to a mobile device provider and receiving the identifier of the mobile device 108 from the mobile device provider, sending an identifier request

Mastercard, Ex1002, p. 492

for the identifier to the mobile device 108 and receiving the identifier of the mobile device 108 from the mobile device 108, or the like.

A single use authentication code relating to the identifier is generated at block 506. The single use authentication code may be capable of being used to authenticate the mobile device 108 at the POS device 110 and enable a funds adjustment to the payment account 116. The single use authentication code may include, by way of example, a single use universal product code (UPC), a single use debit card number, a single use credit card number, a single use account reference number, or the like. Providing a single use authentication code to the mobile device 108 may enable a user of the mobile device to have a two-factor authentication at the POS device 110. The single use authentication code may enable a dynamically generated code to be used to provide greater security for the payment account 116 and to reduce a potential for fraud with the payment account 116.

The single use authentication code and an optional access code is provided to the mobile device 108 through the communications network 104 at block 508. The access code may be capable of being used with a terminal of the POS device 110 to authorize the funds adjustment.

Payment authorization for the payment account 116 may be processed at block 510. An example embodiment of the payment authorization is described in greater detail below.

Figure 6 illustrates a method 600 for processing payment authorization for the payment account 116 according to an example embodiment. The method 600 may be performed at block 510 (see Figure 5) by the authentication provider 106 or otherwise performed.

A funds adjustment request and the single use authentication code is received from the POS device 110 through the payment network 102 at block 602. The payment account 116 is identified from the identifier related to the single use authentication code at block 604.

A determination may be made at decision block 606 as to the availability of funds in the payment account 116 for an amount indicated in the funds adjustment request. If a determination is made that funds are not available in the payment account 116, a notice of funding failure may be provided at block 608. If a determination is made at decision block 606 that funds are available in the

Mastercard, Ex1002, p. 493

payment account 116, funds are withdrawn in the amount from the payment account 116 at block 610 and a notice of funding success may be provided at block 612.

In an example embodiment, the notification of funding success may include, for example, a notification that the funds in the amount have been withdrawn from the payment account 116, a notification identifying a merchant that has been provided the amount, or a notification identifying one or more items that have been purchased with the amount. Other notifications may also be used.

Figure 7 illustrates a method 700 for processing payment authorization for the payment account 116 according to an example embodiment. The method 700 may be performed at block 510 (see Figure 5) by the authentication provider 106 or otherwise performed.

At block 702, a funds adjustment request and the single use authentication code is received from the POS device 110 through the payment network 102. The payment account 116 is identified from the identifier related to the single use authentication code at block 704.

An evaluation of the funds adjustment request against an evaluation criterion is made at block 706. The evaluation criterion may include a limit on a period of time since a pin code (e.g. for access to the mobile device 108) was entered into the mobile device 108, a calling pattern made with the mobile device 108, a transaction pattern made with the payment account 116, a period of time between when the single use authentication code was generated and provided to the mobile device 108 and received back from the POS device 110, a specified sum of money, a specified type of item, and/or a specified merchant. Other criterion may also be used.

A determination may be made at decision block 708 as to whether the evaluation was successful. If a determination is made that the evaluation was successful, the method 700 may proceed to block 718. If a determination is made at decision block 708 that the evaluation is not successful, the method 700 may proceed to block 710.

At block 710, a confirmation request may be sent. The confirmation request may be sent to the mobile device 108, provided orally to a user of the mobile device 108, or otherwise provided. The confirmation request may

Mastercard, Ex1002, p. 494

include a request for a pin code to be received by the mobile device 108, a request for an audible confirmation to be received by the mobile device 108, and/or a request for a log in to a web site provided by the authentication provider 106. Other confirmation requests may also be used. A response to the confirmation request may be received at block 712. For example, the confirmation request may be provided through the mobile device 108 or to an agent speaking with the user of the mobile device 108.

A determination may be made at decision block 714 as to whether the response was successful. If a determination is made that the response was not successful, a notice of funding failure may be provided at block 716. If a determination is made at decision block 714 that the response was successful, the payment account 116 is adjusted by the amount at block 718 and a notice of funding success may be provided at block 720. For example, adjusting the payment account 116 may include adding or subtracting funds (e.g., money or other stored value) from the payment account 116.

Figure 8 illustrates a method 800 for processing payment authorization for the payment account 116 according to an example embodiment. The method 800 may be performed at block 510 (see Figure 5) by the authentication provider 106 or otherwise performed.

At block 802, a funds adjustment request and the single use authentication code is received from the POS device 110 through the payment network 102. The payment account 116 is identified from the identifier related to the single use authentication code at block 804.

A determination may be made at decision block 806 as to whether a first user (e.g., a parent0 associated with the payment account 116 has authorized adjustment by an amount indicated in the funds adjustment request for a second user (e.g., a child) associated with the mobile device 108. If a determination is made that the payment account has not been authorized, a notice of funding failure may be provided at block 808. If a determination is made at decision block 806 that the payment account 116 has been authorized, the payment account 116 is adjusted by the amount at block 810 and a notification of funding success may be provided at block 812.

Mastercard, Ex1002, p. 495

Figure 9 illustrates a method 900 for funding authentication according to an example embodiment. The method 900 may be performed by the authentication provider 106 (see Figure 1) or another provider.

Account authorization for a second user may be received from a first user at block 902. For example, a parent may provide account authorization for a child, a user may provide account authorization for a spouse, and the like. A request for funding authorization is received from the second user at block 904.

An identifier of a first mobile device of a first user is accessed at block 906. The identifier of the first mobile device 108 may be associated with the payment account 116 of the first user.

The identifier of the second mobile device of the second user may be accessed at block 908. The identifier of the second mobile device 108 may be associated with the payment account 118 of the second user.

A single use authentication code relating to the identifier of the first mobile device is generated at block 910. The single use authentication code may be capable of being used to authenticate the second mobile device 108 of the second user at the POS device 110 and may enable a funds adjustment to the payment account 116 of the first user.

In an example embodiment, the single use authentication code may related to the identifier of the first mobile device 108 and the second mobile device 108 and may be capable of being used to authenticate the second mobile device 108 of the second user at the POS device 110 and enable a funds adjustment to the payment account 116 of the first user and/or or the second user.

The single use authentication code may be provided to the second mobile device 108 through the communications network 104 at block 912. Payment authorization may be processed for the payment account at block 914. For example, payment authorization may be processed according to the methods 600, 700, 800 (see Figures 6-8).

Figure 10 illustrates a method 1000 for processing payment authorization for the payment account 116 according to an example embodiment. The method 1000 may be performed at block 510 or block 912 (see Figure 5 and 9) by the authentication provider 106 or otherwise performed.

Mastercard, Ex1002, p. 496

A funds adjustment request and a single use authentication code is received from the POS device 110 through the payment network 102 at block 1002. The payment account 116 is identified from the identifier related to the single use authentication code at block 1004.

A determination may be made at decision block 1006 as to whether the payment account 116 of the first user is adjustable by an amount indicated in the funds adjustment request. If the payment account of the first user is not adjustable by the amount, a notice of a failure of the funds adjustment request may be provided at block 1008. If the payment account of the first user is adjustable by the amount, the payment account of the first user may be adjusted by the amount at block 1010 and a notice of a success of the funds adjustment (e.g., the payment account has been adjusted by the amount) may be provided at block 1012.

In an example embodiment, the payment account 116 of the first user may be adjusted by a first portion of the amount and the payment account 116 of the second user may be adjusted by a second portion of the amount. For example, the first portion may be a sum of money designated by the first user and the second portion may be a remaining portion of the amount not designated by the first user.

Figure 11 illustrates a method 1100 for utilizing the mobile device 108 according to an example embodiment. A funding request may be received from a user of the mobile device 108 at block 1102. At block 1104, funding authorization is requested from the authentication provider 106 through the mobile device 108.

A single use authentication code and an optional access code is received from the authentication provider 106 at block 1106. The single use authentication code may be capable of being used to authenticate the mobile device 108 at the POS device 110 and enable a funds adjustment to the payment account 116. The access code may be capable of being used with a terminal of the POS device 110 to authorize the funds adjustment.

The single use authentication code and an optional authorization routing number is provided through the mobile device 108 to the POS device 110 at block 1108. The single use authentication code and an optional authorization routing number may be provided simultaneously or sequentially. The

Mastercard, Ex1002, p. 497

authorization routing number may be capable of being used to identify the authentication provider 106 (e.g., as a provider of the payment account 116).

In an example embodiment, the single use authentication code and the authorization routing number may be a virtual debit card number and the access code may be a pin number. The single use authentication code and the authorization routing number may be a credit debit card number and the access code is a card identification number or credit card security code. Other embodiments of the single use authentication code, the authorization routing number, and/or the access code may also be used.

Authorization information may be presented on a display of the mobile device 108 at block 1110. For example, the presented authorization information may include the access code, the single use authentication code, and/or the authorization routing number. Other authorization information may also be presented.

In an example embodiment, a single use pattern may be generated from the single use authentication code and the authorization routing number and the single use pattern may be presented on the display of the mobile device 108. The single use pattern may be capable of being scanned by the POS device 110. The single use pattern may be a bar code or other type of cryptographic or non-cryptographic pattern.

A confirmation request may be received from the authentication provider 106 at block 1112.

The confirmation request may be presented on the mobile device 108 at block 1114. A response to the confirmation request may be received at block 1116. The response to the authentication provider 106 may be provided at block 1118. A notification may be received from the authentication provider 106 at block 1120.

Figure 12 illustrates a method 1200 for utilizing the POS device 110 according to an example embodiment. A selection of one or more items may be received at block 1202. A total for the selection may be generated at block 1204. The total for the selection may be presented on a display of a point of sale (POS) device at block 1206.

At block 1208, a single use authentication code and an optional authorization routing number is received from the mobile device 108. The single

Mastercard, Ex1002, p. 498

use authentication code and an optional authorization routing number may be received simultaneously or sequentially. The authorization routing number may be capable of being used to identify a provider of the payment account 116. The receipt of the single use authentication code and the optional authorization routing number may enable authorization of a funds adjustment to be made.

In an example embodiment, a display of the mobile device 108 may be scanned to receive the single use authentication code and an authorization routing number. The single use authentication code and an authorization routing number may be in the form of a single use pattern presented on the display of the mobile device 108. The single use authentication code and an authorization routing number may be provided from the mobile device 108 wirelessly (e.g., IR or RF), through a portable media card, or otherwise provided.

The payment network may be determined based on the authorization routing number at block 1210. The single use authentication code and a funding request is provided over the payment network 102 to the authentication provider 106 at block 1212. A funds adjustment related to the funding request is received from the authentication provider 106 at block 1214.

Figure 13 is a network diagram depicting a client-server system 1300, within which one example embodiment may be deployed. By way of example, a network 1304 may include the functionality of the communications network 104, the authentication provider 106 may be deployed on the application server 1318 as a payment application 1322, a client machine 1310 or a client machine 1312 may include the functionality of the mobile device 108, and a database 1326 may include the functionality of the database 112. The system 100 may also be deployed in other systems.

A networked system 1302, in the example forms of a network-based marketplace or publication system, provides server-side functionality, via a network 1304 (e.g., the Internet or Wide Area Network (WAN)) to one or more clients. Figure 13 illustrates, for example, a web client 1306 (e.g., a browser, such as the Internet Explorer browser developed by Microsoft Corporation of Redmond, Washington State), and a programmatic client 1308 executing on respective client machines 1310 and 1312.

An Application Program Interface (API) server 1314 and a web server 1316 are coupled to, and provide programmatic and web interfaces respectively

Mastercard, Ex1002, p. 499

to, one or more application servers 1318. The application servers 1318 host one or more marketplace applications 1320 and authentication providers 1322. The application servers 1318 are, in turn, shown to be coupled to one or more databases servers 1324 that facilitate access to one or more databases 1326.

The marketplace applications 1320 may provide a number of marketplace functions and services to users that access the networked system 1302. The authentication providers 1322 may likewise provide a number of payment services and functions to users. The authentication providers 1322 may allow users to accumulate value (e.g., in a commercial currency, such as the U.S. dollar, or a proprietary currency, such as "points") in accounts, and then later to redeem the accumulated value for products (e.g., goods or services) that are made available via the marketplace applications 1320. While the marketplace and authentication providers 1320 and 1322 are shown in Figure 13 to both form part of the networked system 1302, in alternative embodiments the authentication providers 1322 may form part of a payment service that is separate and distinct from the networked system 1302.

Further, while the system 1300 shown in Figure 13 employs a client-server architecture, the present invention is of course not limited to such an architecture, and could equally well find application in a distributed, or peer-to-peer, architecture system, for example. The various marketplace and authentication providers 1320 and 1322 could also be implemented as standalone software programs, which need not have networking capabilities.

The web client 1306 accesses the various marketplace and authentication providers 1320 and 1322 via the web interface supported by the web server 1316. Similarly, the programmatic client 1308 accesses the various services and functions provided by the marketplace and authentication providers 1320 and 1322 via the programmatic interface provided by the API server 1314. The programmatic client 1308 may, for example, be a seller application (e.g., the TurboLister™ application developed by eBay Inc., of San Jose, California) to enable sellers to author and manage listings on the networked system 1302 in an off-line manner, and to perform batch-mode communications between the programmatic client 1308 and the networked system 1302.

Figure 13 also illustrates a third party application 1328, executing on a third party server machine 1330, as having programmatic access to the

Mastercard, Ex1002, p. 500

networked system 1302 via the programmatic interface provided by the API server 1314. For example, the third party application 1328 may, utilizing information retrieved from the networked system 1302, support one or more features or functions on a website hosted by the third party. The third party may, for example, provide one or more promotional, marketplace or payment functions that are supported by the relevant applications of the networked system 1302.

Figure 14 is a block diagram illustrating multiple applications 1320 and 1322 that, in one example embodiment, are provided as part of the networked system 1302 (see Figure 13). The applications 1320 may be hosted on dedicated or shared server machines (not shown) that are communicatively coupled to enable communications between server machines. The applications themselves are communicatively coupled (e.g., via appropriate interfaces) to each other and to various data sources, so as to allow information to be passed between the applications or so as to allow the applications to share and access common data. The applications may furthermore access one or more databases 1326 via the database servers 1324.

The networked system 1302 may provide a number of publishing, listing and price-setting mechanisms whereby a seller may list (or publish information concerning) goods or services for sale, a buyer can express interest in or indicate a desire to purchase such goods or services, and a price can be set for a transaction pertaining to the goods or services. To this end, the marketplace applications 1320 are shown to include at least one publication application 1400 and one or more auction applications 1402 which support auction-format listing and price setting mechanisms (e.g., English, Dutch, Vickrey, Chinese, Double, Reverse auctions etc.). The various auction applications 1402 may also provide a number of features in support of such auction-format listings, such as a reserve price feature whereby a seller may specify a reserve price in connection with a listing and a proxy-bidding feature whereby a bidder may invoke automated proxy bidding.

A number of fixed-price applications 1404 support fixed-price listing formats (e.g., the traditional classified advertisement-type listing or a catalogue listing) and buyout-type listings. Specifically, buyout-type listings (e.g., including the Buy-It-Now (BIN) technology developed by eBay Inc., of San

Mastercard, Ex1002, p. 501

Jose, California) may be offered in conjunction with auction-format listings, and allow a buyer to purchase goods or services, which are also being offered for sale via an auction, for a fixed-price that is typically higher than the starting price of the auction.

Store applications 1406 allow a seller to group listings within a "virtual" store, which may be branded and otherwise personalized by and for the seller. Such a virtual store may also offer promotions, incentives and features that are specific and personalized to a relevant seller.

Reputation applications 1408 allow users that transact, utilizing the networked system 1302, to establish, build and maintain reputations, which may be made available and published to potential trading partners. Consider that where, for example, the networked system 1302 supports person-to-person trading, users may otherwise have no history or other reference information whereby the trustworthiness and credibility of potential trading partners may be assessed. The reputation applications 1408 allow a user, for example through feedback provided by other transaction partners, to establish a reputation within the networked system 1302 over time. Other potential trading partners may then reference such a reputation for the purposes of assessing credibility and trustworthiness.

Personalization applications 1410 allow users of the networked system 1302 to personalize various aspects of their interactions with the networked system 1302. For example a user may, utilizing an appropriate personalization application 1410, create a personalized reference page at which information regarding transactions to which the user is (or has been) a party may be viewed. Further, a personalization application 1410 may enable a user to personalize listings and other aspects of their interactions with the networked system 1302 and other parties.

The networked system 1302 may support a number of marketplaces that are customized, for example, for specific geographic regions. A version of the networked system 1302 may be customized for the United Kingdom, whereas another version of the networked system 1302 may be customized for the United States. Each of these versions may operate as an independent marketplace, or may be customized (or internationalized and/or localized) presentations of a common underlying marketplace. The networked system 1302 may accordingly

Mastercard, Ex1002, p. 502

include a number of internationalization applications 1412 that customize information (and/or the presentation of information) by the networked system 1302 according to predetermined criteria (e.g., geographic, demographic or marketplace criteria). For example, the internationalization applications 1412 may be used to support the customization of information for a number of regional websites that are operated by the networked system 1302 and that are accessible via respective web servers 1316.

Navigation of the networked system 1302 may be facilitated by one or more navigation applications 1414. For example, a search application (as an example of a navigation application) may enable key word searches of listings published via the networked system 1302. A browse application may allow users to browse various category, catalogue, or system inventory structures according to which listings may be classified within the networked system 1302. Various other navigation applications may be provided to supplement the search and browsing applications.

In order to make listings available via the networked system 1302 as visually informing and attractive as possible, the marketplace applications 1320 may include one or more imaging applications 1416 utilizing which users may upload images for inclusion within listings. An imaging application 1416 also operates to incorporate images within viewed listings. The imaging applications 1416 may also support one or more promotional features, such as image galleries that are presented to potential buyers. For example, sellers may pay an additional fee to have an image included within a gallery of images for promoted items.

Listing creation applications 1418 allow sellers conveniently to author listings pertaining to goods or services that they wish to transact via the networked system 1302, and listing management applications 1420 allow sellers to manage such listings. Specifically, where a particular seller has authored and/or published a large number of listings, the management of such listings may present a challenge. The listing management applications 1420 provide a number of features (e.g., auto-relisting, inventory level monitors, etc.) to assist the seller in managing such listings. One or more post-listing management applications 1422 also assist sellers with a number of activities that typically occur post-listing. For example, upon completion of an auction facilitated by

Mastercard, Ex1002, p. 503

one or more auction applications 1402, a seller may wish to leave feedback regarding a particular buyer. To this end, a post-listing management application 1422 may provide an interface to one or more reputation applications 1408, so as to allow the seller conveniently to provide feedback regarding multiple buyers to the reputation applications 1408.

Dispute resolution applications 1424 provide mechanisms whereby disputes arising between transacting parties may be resolved. For example, the dispute resolution applications 1424 may provide guided procedures whereby the parties are guided through a number of steps in an attempt to settle a dispute. In the event that the dispute cannot be settled via the guided procedures, the dispute may be escalated to a merchant mediator or arbitrator.

A number of fraud prevention applications 1426 implement fraud detection and prevention mechanisms to reduce the occurrence of fraud within the networked system 1302.

Messaging applications 1428 are responsible for the generation and delivery of messages to users of the networked system 1302, such messages for example advising users regarding the status of listings at the networked system 1302 (e.g., providing "outbid" notices to bidders during an auction process or to provide promotional and merchandising information to users). Respective messaging applications 1428 may utilize any one have a number of message delivery networks and platforms to deliver messages to users. For example, messaging applications 1428 may deliver electronic mail (e-mail), instant message (IM), Short Message Service (SMS), text, facsimile, or voice (e.g., Voice over IP (VoIP)) messages via the wired (e.g., the Internet), Plain Old Telephone Service (POTS), or wireless (e.g., mobile, cellular, WiFi, WiMAX) networks.

Merchandising applications 1430 support various merchandising functions that are made available to sellers to enable sellers to increase sales via the networked system 1302. The merchandising applications 1430 also operate the various merchandising features that may be invoked by sellers, and may monitor and track the success of merchandising strategies employed by sellers.

The networked system 1302 itself, or one or more parties that transact via the networked system 1302, may operate loyalty programs that are supported by one or more loyalty/promotions applications 1432. For example, a buyer may

Mastercard, Ex1002, p. 504

earn loyalty or promotions points for each transaction established and/or concluded with a particular seller, and may be offered a reward for which accumulated loyalty points can be redeemed.

Figure 15 shows a diagrammatic representation of machine in the example form of a computer system 1500 within which a set of instructions may be executed causing the machine to perform any one or more of the methods, processes, operations, or methodologies discussed herein. The authentication provider 106 may operate on or more computer systems 1500 and/or the authentication provider 106, the mobile device 108, and/or the POS device 110 may include the functionality of the computer system 1500.

In an example embodiment, the machine operates as a standalone device or may be connected (e.g., networked) to other machines. In a networked deployment, the machine may operate in the capacity of a server or a client machine in server-client network environment, or as a peer machine in a peer-to-peer (or distributed) network environment. The machine may be a server computer, a client computer, a personal computer (PC), a tablet PC, a set-top box (STB), a Personal Digital Assistant (PDA), a cellular telephone, a web appliance, a network router, switch or bridge, or any machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that machine. Further, while only a single machine is illustrated, the term "machine" shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein.

The example computer system 1500 includes a processor 1502 (e.g., a central processing unit (CPU) a graphics processing unit (GPU) or both), a main memory 1504 and a static memory 1506, which communicate with each other via a bus 1508. The computer system 1500 may further include a video display unit 1510 (e.g., a liquid crystal display (LCD) or a cathode ray tube (CRT)). The computer system 1500 also includes an alphanumeric input device 1512 (e.g., a keyboard), a cursor control device 1514 (e.g., a mouse), a drive unit 1516, a signal generation device 1518 (e.g., a speaker) and a network interface device 1520.

The drive unit 1516 includes a machine-readable medium 1522 on which is stored one or more sets of instructions (e.g., software 1524) embodying any

Mastercard, Ex1002, p. 505

one or more of the methodologies or functions described herein. The software 1524 may also reside, completely or at least partially, within the main memory 1504 and/or within the processor 1502 during execution thereof by the computer system 1500, the main memory 1504 and the processor 1502 also constituting machine-readable media.

The software 1524 may further be transmitted or received over a network 1526 via the network interface device 1520.

While the machine-readable medium 1522 is shown in an example embodiment to be a single medium, the term "machine-readable medium" should be taken to include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that store the one or more sets of instructions. The term "machine-readable medium" shall also be taken to include any medium that is capable of storing, encoding or carrying a set of instructions for execution by the machine and that cause the machine to perform any one or more of the methodologies of the present invention. The term "machine-readable medium" shall accordingly be taken to include, but not be limited to, solid-state memories, optical and magnetic media, and carrier wave signals.

Certain systems, apparatus, applications or processes are described herein as including a number of modules or mechanisms. A module or a mechanism may be a unit of distinct functionality that can provide information to, and receive information from, other modules. Accordingly, the described modules may be regarded as being communicatively coupled. Modules may also initiate communication with input or output devices, and can operate on a resource (e.g., a collection of information). The modules be implemented as hardware circuitry, optical components, single or multi-processor circuits, memory circuits, software program modules and objects, firmware, and combinations thereof, as appropriate for particular implementations of various embodiments.

Thus, methods and systems for dynamic funding have been described. Although the present invention has been described with reference to specific example embodiments, it will be evident that various modifications and changes may be made to these embodiments without departing from the broader spirit and scope of the invention. Accordingly, the specification and drawings are to be regarded in an illustrative rather than a restrictive sense.

Mastercard, Ex1002, p. 506

The Abstract of the Disclosure is provided to comply with 37 C.F.R. §1.72(b), requiring an abstract that will allow the reader to quickly ascertain the nature of the technical disclosure. It is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, it can be seen that various features are grouped together in a single embodiment for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter lies in less than all features of a single disclosed embodiment. Thus the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separate embodiment.

Mastercard, Ex1002, p. 507

CLAIMS

What is claimed is:

1. A method comprising:

accessing an identifier of a mobile device, the identifier associated with a payment account;

generating a single use authentication code relating to the identifier, the single use authentication code capable of being used to authenticate the mobile device at a point of sale (POS) device and enable a funds adjustment to the payment account; and

providing the single use authentication code to the mobile device through a communications network.

2. The method of claim 1, wherein the accessing comprises:

receiving a request for funding authorization from the mobile device; and

accessing the identifier of the mobile device.

3. The method of claim 1, wherein the accessing comprises:

associating the payment account with the identifier of the mobile device.

4. The method of claim 3, wherein the associating comprises:

sending an identifier request for the identifier to a mobile device provider; and

receiving the identifier of the mobile device from the mobile device provider.

5. The method of claim 3, wherein the associating comprises:

sending an identifier request for the identifier to the mobile device; and

receiving the identifier of the mobile device from the mobile device.

Mastercard, Ex1002, p. 508

6. The method of claim 3, 4, or 5, wherein the associating further comprises:

sending a communication request message to the mobile device, the communication request message including request for a confirmation code; and

receiving the confirmation code from the mobile device.

7. The method of claim 1, 2, 3, 4, 5, or 6, wherein the providing comprises:

providing the single use authentication code and an access code to the mobile device through a communications network, the access code capable of being used with a terminal of the POS device to authorize the funds adjustment.

8. The method of claim 1, 2, 3, 4, 5, 6, or 7, further comprising:

processing payment authorization for the payment account.

9. The method of claim 8, wherein the processing comprises:

receiving a funds adjustment request and the single use authentication code from the POS device through an payment network;

identifying the payment account associated with the identifier related to the single use authentication code;

determining availability of funds in the payment account for an amount indicated in the funds adjustment request; and

based on the determination, withdrawing funds in the amount from the payment account.

10. The method of claim 9, further comprising:

providing a notification that the funds in the amount have been withdrawn from the payment account.

11. The method of claim 9, further comprising:

providing a notification identifying a merchant that has been provided the amount of the funds.

Mastercard, Ex1002, p. 509

12. The method of claim 9, further comprising:

providing a notification identifying one or more items that have been purchased with the amount of the funds.

13. The method of claim 8, wherein the processing comprises:

receiving a funds adjustment request and the single use authentication code from the POS device through an payment network;

identifying the payment account associated with the identifier related to the single use authentication code;

evaluating the funds adjustment request against an evaluation criterion; and

based on the evaluation, adjusting the payment account by the amount.

14. The method of claim 13, wherein the evaluation criterion comprises at least one criterion selected from the group consisting of:

a limit on a period of time since a pin code was entered into the mobile device,

a calling pattern made with the mobile device,

a transaction pattern made with the payment account,

a period of time between providing the single use authentication code to the mobile device and receiving the single use authentication code back from the POS device,

a specified sum of money,

a specified type of item,

a specified merchant, and

a combination thereof.

Mastercard, Ex1002, p. 510

15. The method of claim 8, wherein the processing comprises:

receiving a funds adjustment request and the single use authentication code from the POS device through a payment network;

identifying the payment account associated with the identifier related to the single use authentication code;

evaluating the funds adjustment request against an evaluation criterion; and

based on the evaluation, providing a confirmation request to the mobile device;

receiving a response to the confirmation request; and

based on the response, adjusting the payment account by the amount.

16. The method of claim 15, wherein the confirmation request comprises at least one of:

a request for a pin code to be received by the mobile device,

a request for an audible confirmation to be received by the mobile device, and

a request for a log in to an authentication provider associated with the payment account.

17. The method of claim 8, wherein the processing comprises:

receiving a funds adjustment request and the single use authentication code from the POS device through an payment network;

identifying the payment account associated with the identifier related to the single use authentication code;

determining whether a first user associated with the payment account has authorized adjustment by an amount indicated in the funds adjustment request for a second user associated with the mobile device; and

based on the determination, adjusting the payment account by the amount.

Mastercard, Ex1002, p. 511

18. The method of claim 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, or 17, wherein the single use authentication code includes a single use universal product code (UPC), a single use debit card number, a single use credit card number, or a single use account reference number.

19. The method of claim 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, or 18, wherein the identifier is stored on a Subscriber Identity Module (SIM) card of the mobile device or a Removable User Identity Module (RUIM) of the mobile device.

20. The method of claim 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, or 19, wherein the identifier is a unique identifier.

21. A method comprising:

accessing an identifier of a first mobile device of a first user, the identifier of the first mobile device associated with a payment account of the first user;

generating a single use authentication code relating to the identifier of the first mobile device, the single use authentication code capable of being used to authenticate a second mobile device of a second user at a point of sale (POS) device and enable a funds adjustment to the payment account of the first user; and

providing the single use authentication code to the second mobile device through a communications network.

22. The method of claim 21, wherein the accessing comprises:

receiving account authorization for the second user from the first user;

receiving a request for funding authorization from the second user; and

accessing the identifier of the first mobile device of the first user, the identifier associated with the payment account of the first user.

Mastercard, Ex1002, p. 512

23. The method of claim 22, wherein the generating comprises:

accessing the identifier of the second mobile device of the second user, the identifier of the second mobile device associated with the payment account of the second user; and

generating the single use authentication code relating to the identifier of the first mobile device and the second mobile device, the single use authentication code capable of being used to authenticate the second mobile device of the second user at the point of sale (POS) device and enable a funds adjustment to the payment account of at least one of the first user or the second user.

24. The method of claim 21, 22, or 23, further comprising:

processing payment authorization for the payment account.

25. The method of claim 24, wherein the processing comprises:

receiving a funds adjustment request and the single use authentication code from the POS device through an payment network;

identifying the payment account associated with the identifier related to the single use authentication code;

determining whether the payment account of the first user is adjustable by an amount indicated in the funds adjustment request; and

based on the determination, adjusting the payment account of the first user by the amount.

26. The method of claim 25, wherein the adjusting based on the determination comprises:

based on the determination, adjusting the payment account of the first user by a first portion of the amount and adjusting the payment account of the second user by a second portion of the amount.

27. The method of claim 26, wherein the first portion is a sum of money designated by the first user and the second portion is a remaining portion of the amount not designated by the first user.

Mastercard, Ex1002, p. 513

28 The method of claim 26 or 27, further comprising:

providing a notification that the payment account has been adjusted by the amount.

29. A method comprising:

requesting funding authorization from an authentication provider through a mobile device;

receiving a single use authentication code from the authentication provider, the single use authentication code capable of being used to authenticate the mobile device at a point of sale (POS) device and enable a funds adjustment to the payment account; and

providing, through the mobile device, the single use authentication code.

30. The method of claim 29, wherein the requesting comprises:

receiving a funding request from a user of the mobile device; and

requesting funding authorization from the authentication provider through the mobile device.

31. The method of claim 29 or 30, wherein the receiving of the single use authentication code comprises:

receiving the single use authentication code and an access code from the authentication provider, the access code capable of being used with a terminal of the POS device to authorize the funds adjustment.

32. The method of claim 31, wherein the providing comprises:

providing, through the mobile device, the single use authentication code and an authorization routing number to a POS device, the authorization routing number capable of being used to identify an authentication provider; and

presenting the access code on a display of the mobile device.

33. The method of claim 32, wherein the single use authentication code and an authorization routing number is a virtual debit card number and the access code is a pin number.

Mastercard, Ex1002, p. 514

34. The method of claim 29, 30, or 31, wherein the providing comprises:

providing, through the mobile device, the single use authentication code and an authorization routing number, the authorization routing number capable of being used to identify a provider of the payment account.

35. The method of claim 34, wherein the providing comprises:

presenting the single use authentication code and the authorization routing number on a display of the mobile device.

36. The method of claim 35, wherein the presenting comprises:

generating a single use pattern from the single use authentication code and the authorization routing number; and

presenting the single use pattern on the display of the mobile device, the single use pattern capable of being scanned by a point of sale device.

37. The method of claim 36, wherein the single use pattern is a single use bar code.

38. The method of claim 29, 30, 31, 32, 33, 34, 35, 36, or 37, further comprising:

receiving a notification from the authentication provider.

39. The method of claim 29, 30, 31, 32, 33, 34, 35, 36, 37, or 38, further comprising:

receiving a confirmation request from an authentication provider;

presenting the confirmation request on the mobile device;

receiving a response to the confirmation request; and

providing the response to the authentication provider.

Mastercard, Ex1002, p. 515

40. A method comprising:

receiving a single use authentication code from a mobile device;

providing the single use authentication code and a funding request over a payment network to an authentication provider; and

receiving a funds adjustment related to the funding request from the authentication provider.

41. The method of claim 40, wherein the receiving of the single use authentication code comprises:

receiving the single use authentication code and an authorization routing number from a mobile device, the authorization routing number capable of being used to identify a provider of the payment account; and

determining the payment network based on the authorization routing number.

42. The method of claim 40, wherein the receiving of the single use authentication code comprises:

scanning a display of the mobile device to receive the single use authentication code and an authorization routing number, the single use authentication code and an authorization routing number being in the form of a single use pattern presented on the display.

43. The method of claim 40, wherein the receiving of the single use authentication code comprises:

receiving a selection of one or more items;

generating a total for the selection;

presenting the total for the selection on a display of a point of sale (POS) device; and

receiving a single use authentication code from a mobile device.

Mastercard, Ex1002, p. 516

44. A machine-readable medium comprising instructions, which when implemented by one or more processors perform the following operations:

access an identifier of a mobile device, the identifier associated with a payment account;

generate a single use authentication code relating to the identifier, the single use authentication code capable of being used to authenticate the mobile device at a point of sale (POS) device and enable a funds adjustment to the payment account; and

provide the single use authentication code to the mobile device through a communications network.

45. The machine-readable medium of claim 44 comprising instructions, which implemented by one or more processors perform the following additional operations:

receive a funds adjustment request and the single use authentication code from the POS device through an payment network;

identify the payment account associated with the identifier related to the single use authentication code;

determine availability of funds in the payment account for an amount indicated in the funds adjustment request; and

based on the determination, withdraw funds in the amount from the payment account.

46. The machine-readable medium of claim 44 or 45 comprising instructions, which implemented by one or more processors perform the following additional operations:

receive a funds adjustment request and the single use authentication code from the POS device through an payment network;

identify the payment account associated with the identifier related to the single use authentication code;

evaluate the funds adjustment request against an evaluation criterion; and

based on the evaluation, adjust the payment account by the amount.

Mastercard, Ex1002, p. 517

47. The machine-readable medium of claim 44, 45, or 46, comprising instructions, which implemented by one or more processors perform the following additional operations:

receive a funds adjustment request and the single use authentication code from the POS device through an payment network;

identify the payment account associated with the identifier related to the single use authentication code;

evaluate the funds adjustment request against an evaluation criterion; and

based on the evaluation, provide a confirmation request to the mobile device;

receive a response to the confirmation request; and

based on the response, adjust the payment account by the amount.

48. The machine-readable medium of claim 44, 45, 46, or 47, comprising instructions, which implemented by one or more processors perform the following additional operations:

receive a funds adjustment request and the single use authentication code from the POS device through an payment network;

identify the payment account associated with the identifier related to the single use authentication code;

determine whether a first user associated with the payment account has authorized adjustment by an amount indicated in the funds adjustment request for a second user associated with the mobile device; and

based on the determination, adjust the payment account by the amount.

49. A machine-readable medium comprising instructions, which when implemented by one or more processors perform the following operations:

request funding authorization from an authentication provider through a mobile device;

receive a single use authentication code from the authentication provider, the single use authentication code capable of being used to authenticate the mobile device at a point of sale (POS) device and enable a funds adjustment to the payment account; and

provide, through the mobile device, the single use authentication code.

Mastercard, Ex1002, p. 518

50. The machine-readable medium of claim 49 comprising instructions, which implemented by one or more processors perform the following additional operations:

receive a confirmation request from an authentication provider;

present the confirmation request on the mobile device;

receive a response to the confirmation request; and

provide the response to the authentication provider.

Mastercard, Ex1002, p. 519

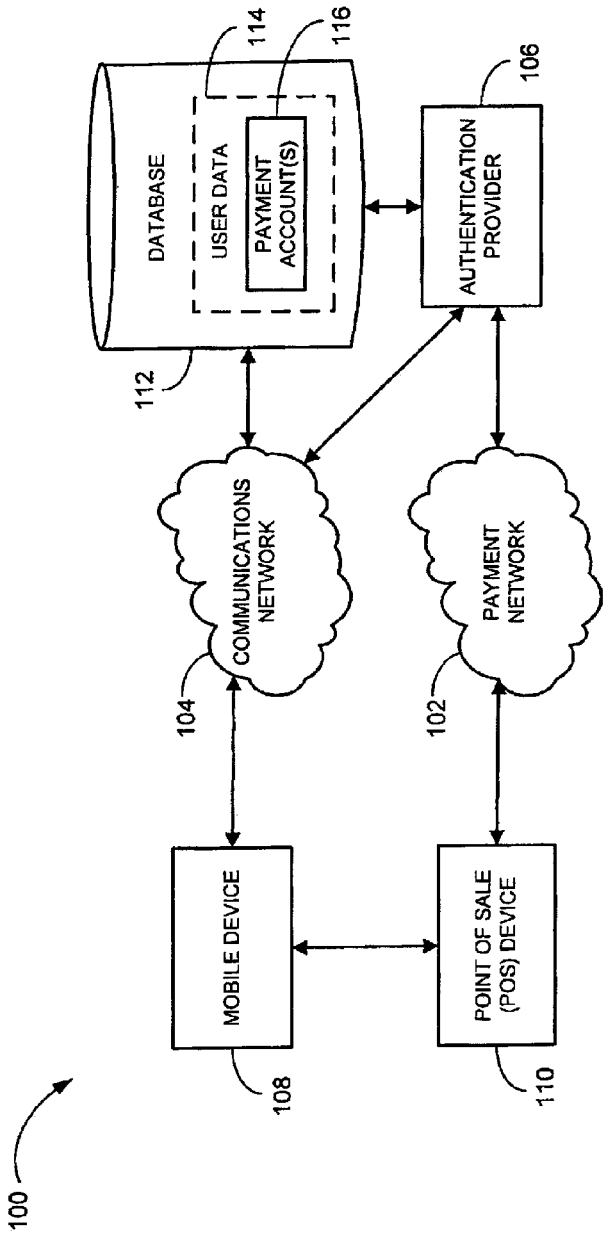

DATABASE
USER DATA
PAYMENT ACCOUNT(S)
AUTHENTICATION PROVIDER
COMMUNICATIONS NETWORK
PAYMENT NETWORK
MOBILE DEVICE
POINT OF SALE (POS) DEVICE
100
102
104
106
108
110
112
114
116

FIGURE 1

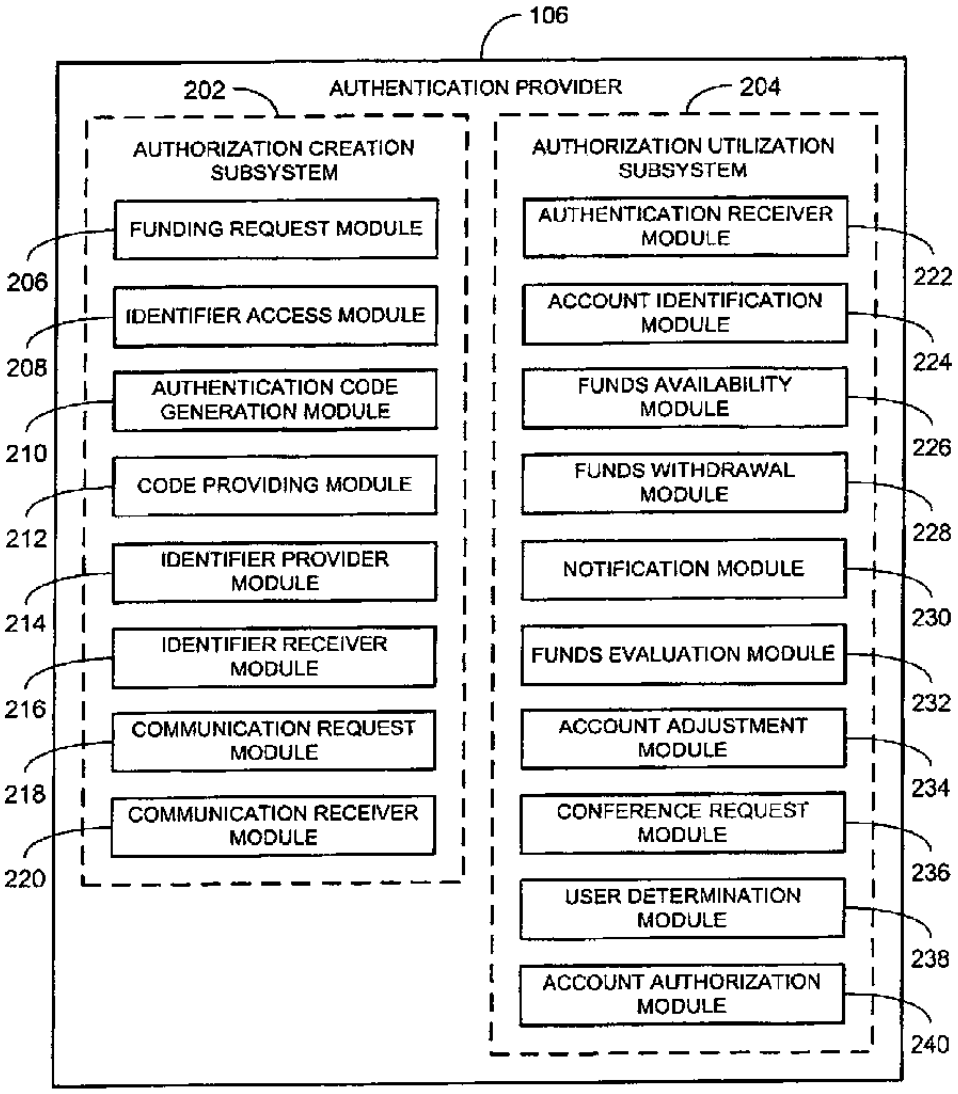

106
AUTHENTICATION PROVIDER
202
204
AUTHORIZATION CREATION SUBSYSTEM
AUTHORIZATION UTILIZATION SUBSYSTEM
FUNDING REQUEST MODULE
206
IDENTIFIER ACCESS MODULE
208
AUTHENTICATION CODE GENERATION MODULE
210
CODE PROVIDING MODULE
212
IDENTIFIER PROVIDER MODULE
214
IDENTIFIER RECEIVER MODULE
216
COMMUNICATION REQUEST MODULE
218
COMMUNICATION RECEIVER MODULE
220
AUTHENTICATION RECEIVER MODULE
222
ACCOUNT IDENTIFICATION MODULE
224
FUNDS AVAILABILITY MODULE
226
FUNDS WITHDRAWAL MODULE
228
NOTIFICATION MODULE
230
FUNDS EVALUATION MODULE
232
ACCOUNT ADJUSTMENT MODULE
234
CONFERENCE REQUEST MODULE
236
USER DETERMINATION MODULE
238
ACCOUNT AUTHORIZATION MODULE
240

FIGURE 2

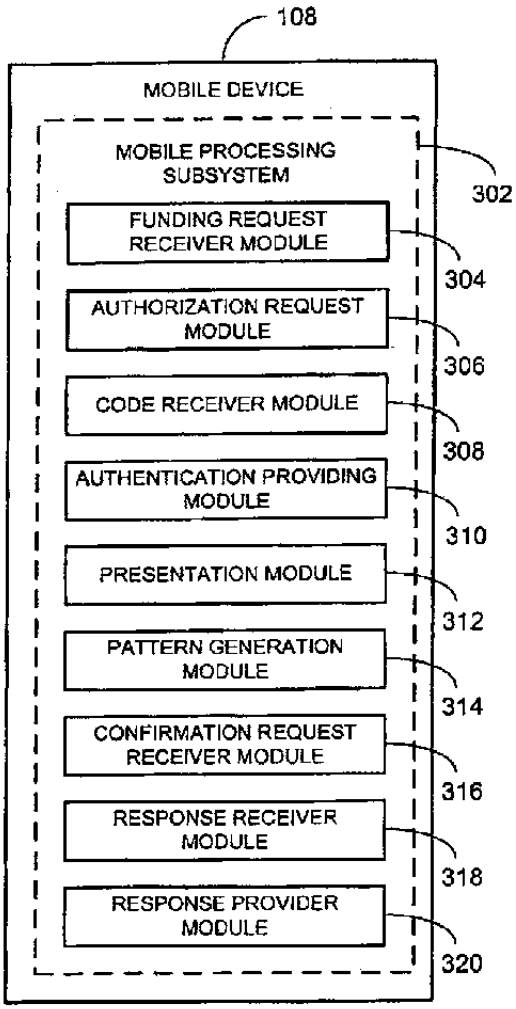

108
MOBILE DEVICE
MOBILE PROCESSING SUBSYSTEM
302
FUNDING REQUEST RECEIVER MODULE
304
AUTHORIZATION REQUEST MODULE
306
CODE RECEIVER MODULE
308
AUTHENTICATION PROVIDING MODULE
310
PRESENTATION MODULE
312
PATTERN GENERATION MODULE
314
CONFIRMATION REQUEST RECEIVER MODULE
316
RESPONSE RECEIVER MODULE
318
RESPONSE PROVIDER MODULE
320

FIGURE 3

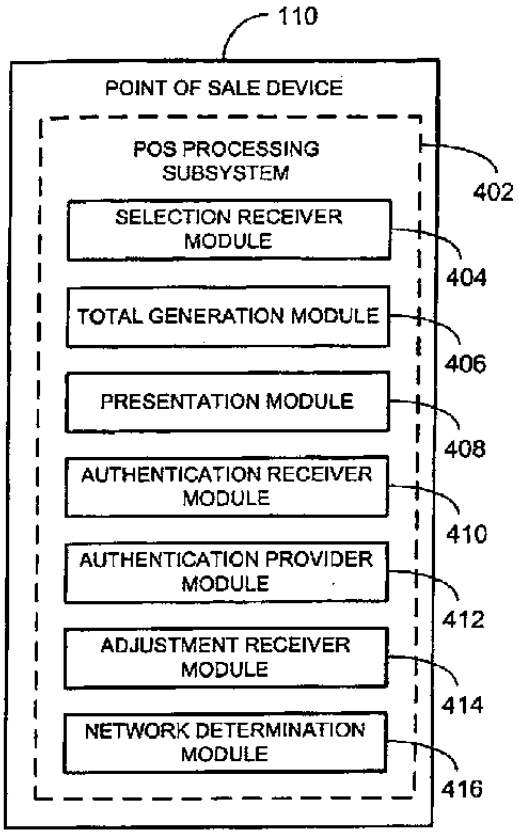

110
POINT OF SALE DEVICE
POS PROCESSING SUBSYSTEM
402
SELECTION RECEIVER MODULE
404
TOTAL GENERATION MODULE
406
PRESENTATION MODULE
408
AUTHENTICATION RECEIVER MODULE
410
AUTHENTICATION PROVIDER MODULE
412
ADJUSTMENT RECEIVER MODULE
414
NETWORK DETERMINATION MODULE
416

FIGURE 4

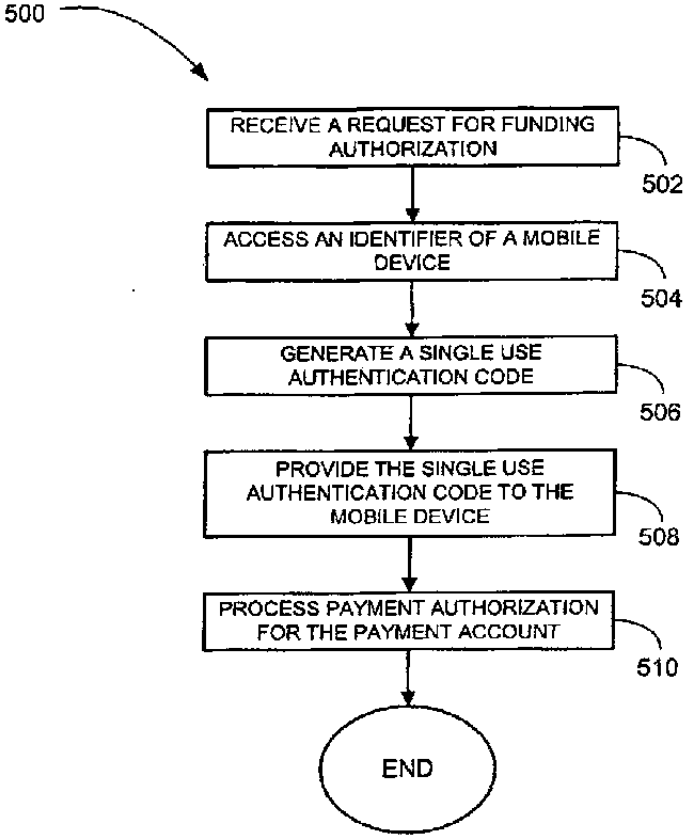

500
RECEIVE A REQUEST FOR FUNDING AUTHORIZATION
502
ACCESS AN IDENTIFIER OF A MOBILE DEVICE
504
GENERATE A SINGLE USE AUTHENTICATION CODE
506
PROVIDE THE SINGLE USE AUTHENTICATION CODE TO THE MOBILE DEVICE
508
PROCESS PAYMENT AUTHORIZATION FOR THE PAYMENT ACCOUNT
510
END

FIGURE 5

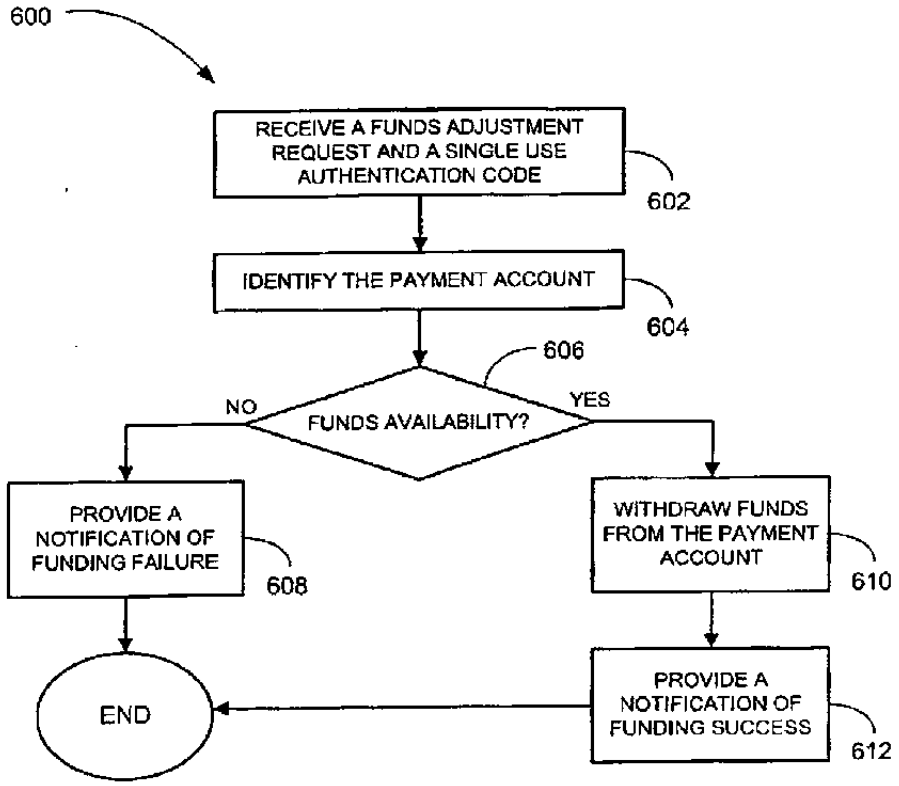

600
RECEIVE A FUNDS ADJUSTMENT REQUEST AND A SINGLE USE AUTHENTICATION CODE
602
IDENTIFY THE PAYMENT ACCOUNT
604
606
FUNDS AVAILABILITY?
NO
YES
PROVIDE A NOTIFICATION OF FUNDING FAILURE
608
WITHDRAW FUNDS FROM THE PAYMENT ACCOUNT
610
END
PROVIDE A NOTIFICATION OF FUNDING SUCCESS
612

FIGURE 6

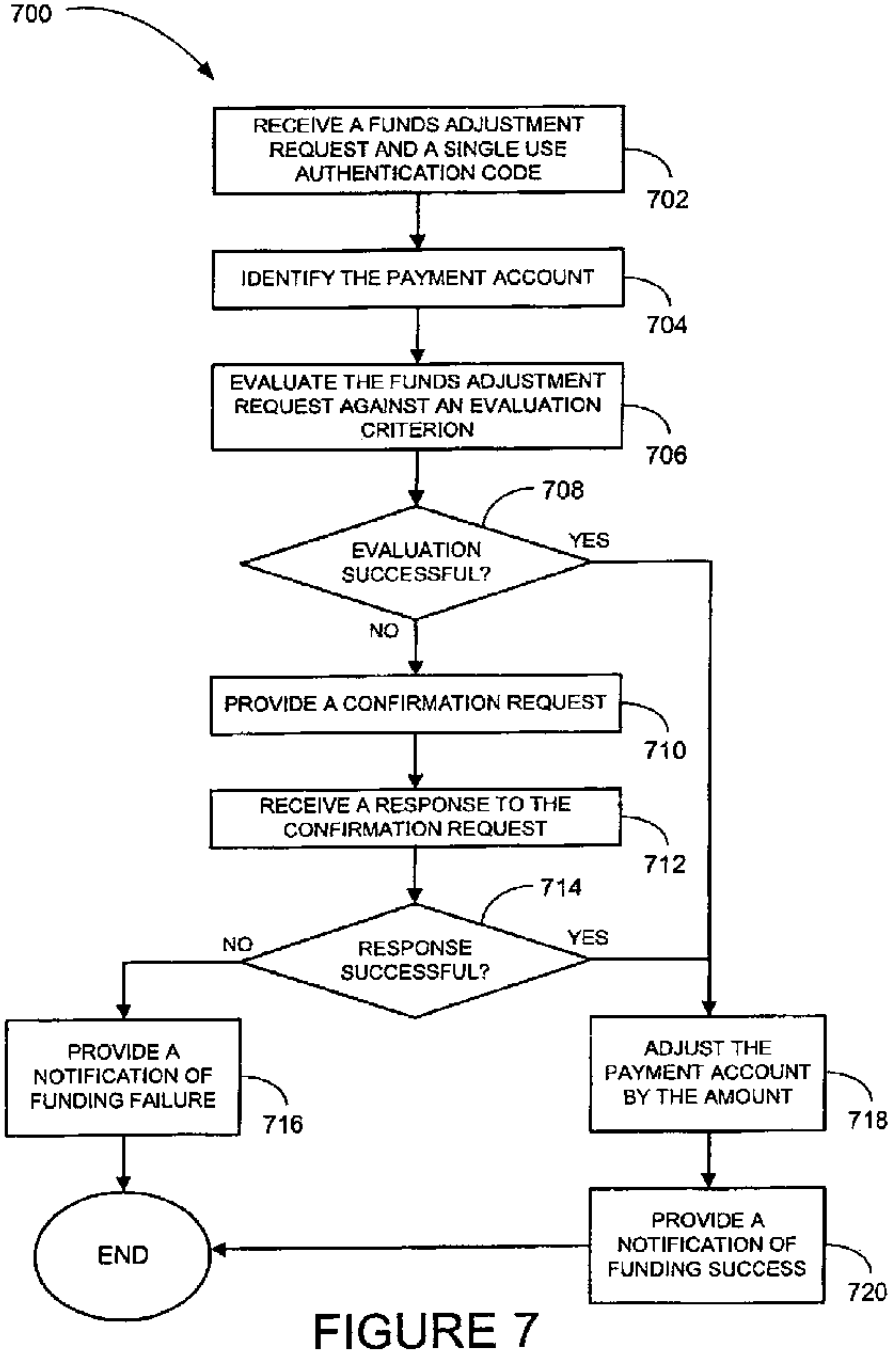

700
RECEIVE A FUNDS ADJUSTMENT REQUEST AND A SINGLE USE AUTHENTICATION CODE
702
IDENTIFY THE PAYMENT ACCOUNT
704
EVALUATE THE FUNDS ADJUSTMENT REQUEST AGAINST AN EVALUATION CRITERION
706
708
EVALUATION SUCCESSFUL?
YES
NO
PROVIDE A CONFIRMATION REQUEST
710
RECEIVE A RESPONSE TO THE CONFIRMATION REQUEST
712
714
RESPONSE SUCCESSFUL?
NO
YES
PROVIDE A NOTIFICATION OF FUNDING FAILURE
716
ADJUST THE PAYMENT ACCOUNT BY THE AMOUNT
718
END
PROVIDE A NOTIFICATION OF FUNDING SUCCESS
720

FIGURE 7

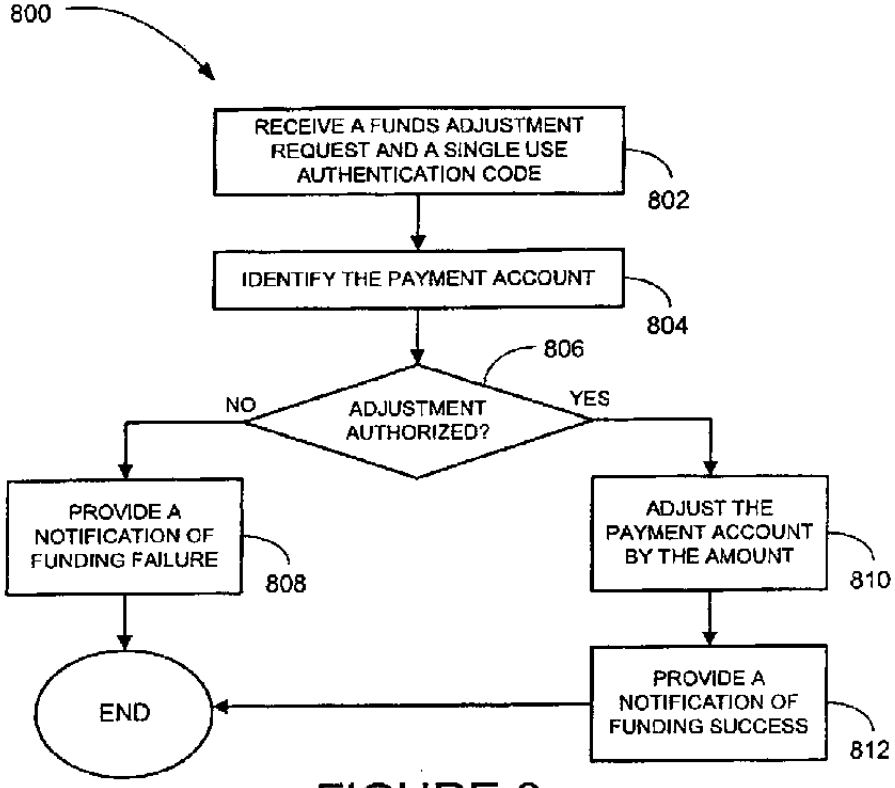

800
RECEIVE A FUNDS ADJUSTMENT REQUEST AND A SINGLE USE AUTHENTICATION CODE
802
IDENTIFY THE PAYMENT ACCOUNT
804
806
ADJUSTMENT AUTHORIZED?
NO
YES
PROVIDE A NOTIFICATION OF FUNDING FAILURE
808
ADJUST THE PAYMENT ACCOUNT BY THE AMOUNT
810
END
PROVIDE A NOTIFICATION OF FUNDING SUCCESS
812

FIGURE 8

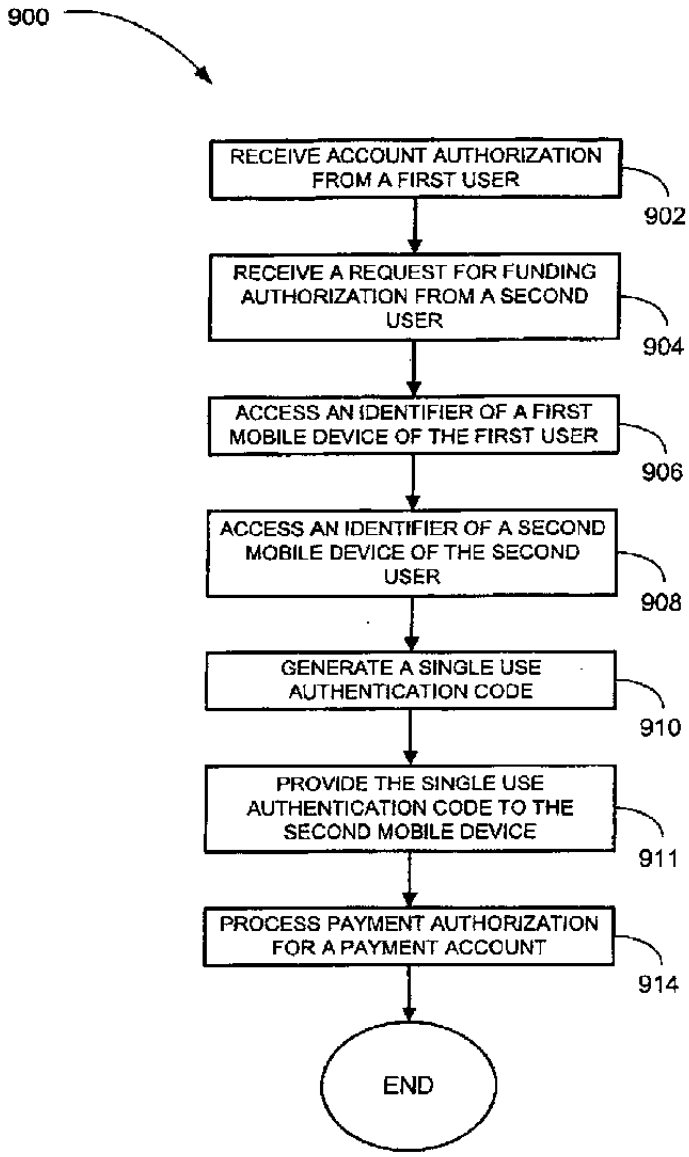

900
RECEIVE ACCOUNT AUTHORIZATION FROM A FIRST USER
902
RECEIVE A REQUEST FOR FUNDING AUTHORIZATION FROM A SECOND USER
904
ACCESS AN IDENTIFIER OF A FIRST MOBILE DEVICE OF THE FIRST USER
906
ACCESS AN IDENTIFIER OF A SECOND MOBILE DEVICE OF THE SECOND USER
908
GENERATE A SINGLE USE AUTHENTICATION CODE
910
PROVIDE THE SINGLE USE AUTHENTICATION CODE TO THE SECOND MOBILE DEVICE
911
PROCESS PAYMENT AUTHORIZATION FOR A PAYMENT ACCOUNT
914
END

FIGURE 9

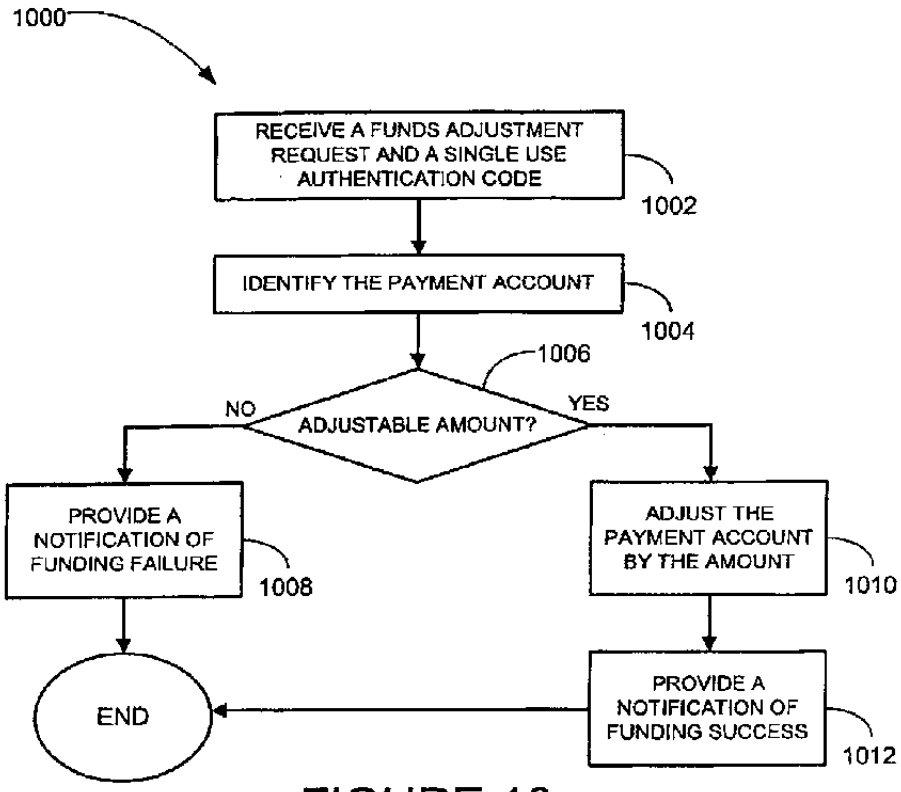

1000
RECEIVE A FUNDS ADJUSTMENT REQUEST AND A SINGLE USE AUTHENTICATION CODE
1002
IDENTIFY THE PAYMENT ACCOUNT
1004
1006
ADJUSTABLE AMOUNT?
NO
YES
PROVIDE A NOTIFICATION OF FUNDING FAILURE
1008
ADJUST THE PAYMENT ACCOUNT BY THE AMOUNT
1010
END
PROVIDE A NOTIFICATION OF FUNDING SUCCESS
1012

FIGURE 10

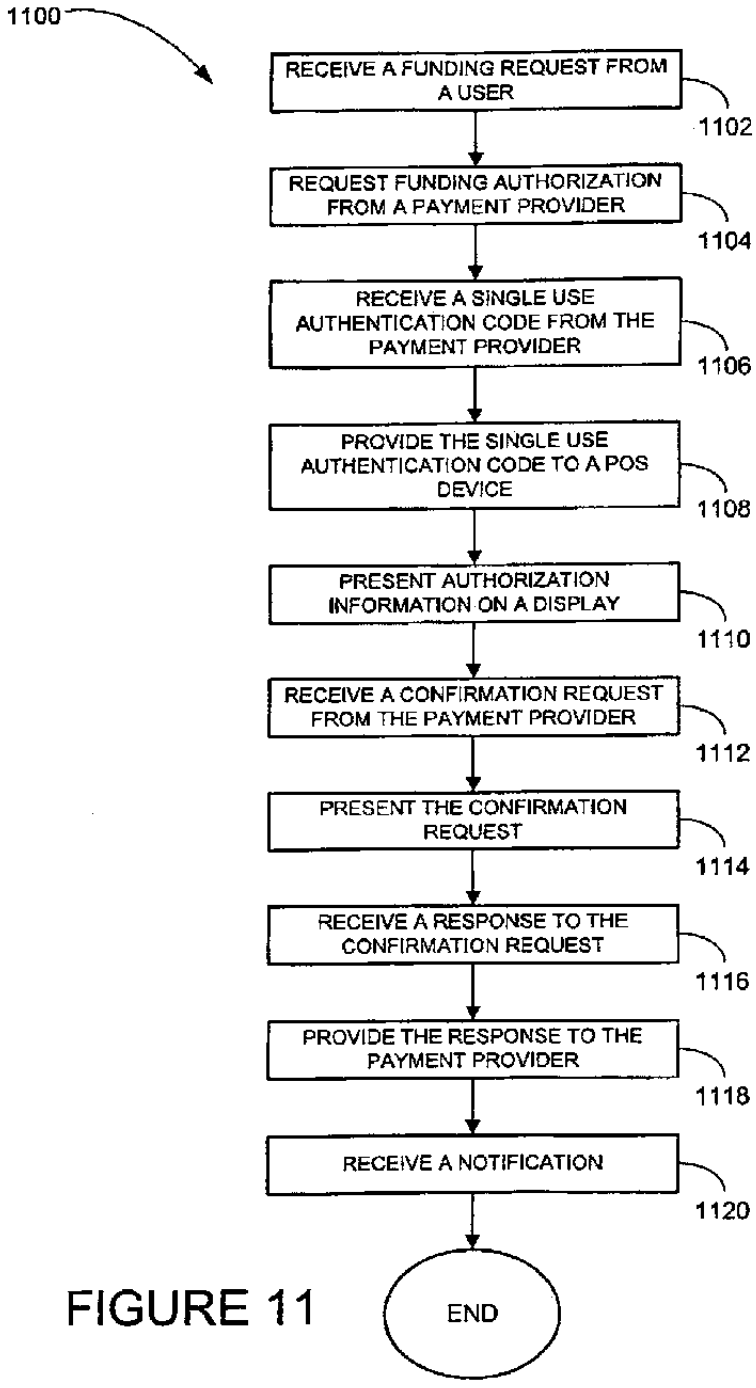

1100
RECEIVE A FUNDING REQUEST FROM A USER
1102
REQUEST FUNDING AUTHORIZATION FROM A PAYMENT PROVIDER
1104
RECEIVE A SINGLE USE AUTHENTICATION CODE FROM THE PAYMENT PROVIDER
1106
PROVIDE THE SINGLE USE AUTHENTICATION CODE TO A POS DEVICE
1108
PRESENT AUTHORIZATION INFORMATION ON A DISPLAY
1110
RECEIVE A CONFIRMATION REQUEST FROM THE PAYMENT PROVIDER
1112
PRESENT THE CONFIRMATION REQUEST
1114
RECEIVE A RESPONSE TO THE CONFIRMATION REQUEST
1116
PROVIDE THE RESPONSE TO THE PAYMENT PROVIDER
1118
RECEIVE A NOTIFICATION
1120
END

FIGURE 11

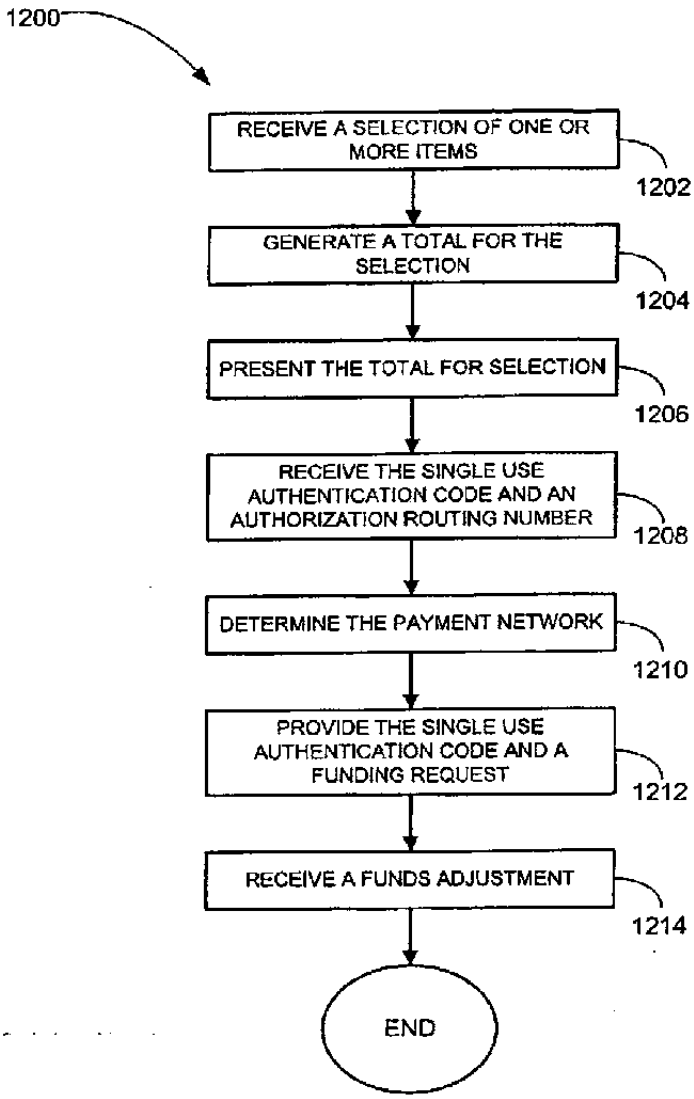

1200
RECEIVE A SELECTION OF ONE OR MORE ITEMS
1202
GENERATE A TOTAL FOR THE SELECTION
1204
PRESENT THE TOTAL FOR SELECTION
1206
RECEIVE THE SINGLE USE AUTHENTICATION CODE AND AN AUTHORIZATION ROUTING NUMBER
1208
DETERMINE THE PAYMENT NETWORK
1210
PROVIDE THE SINGLE USE AUTHENTICATION CODE AND A FUNDING REQUEST
1212
RECEIVE A FUNDS ADJUSTMENT
1214
END

FIGURE 12

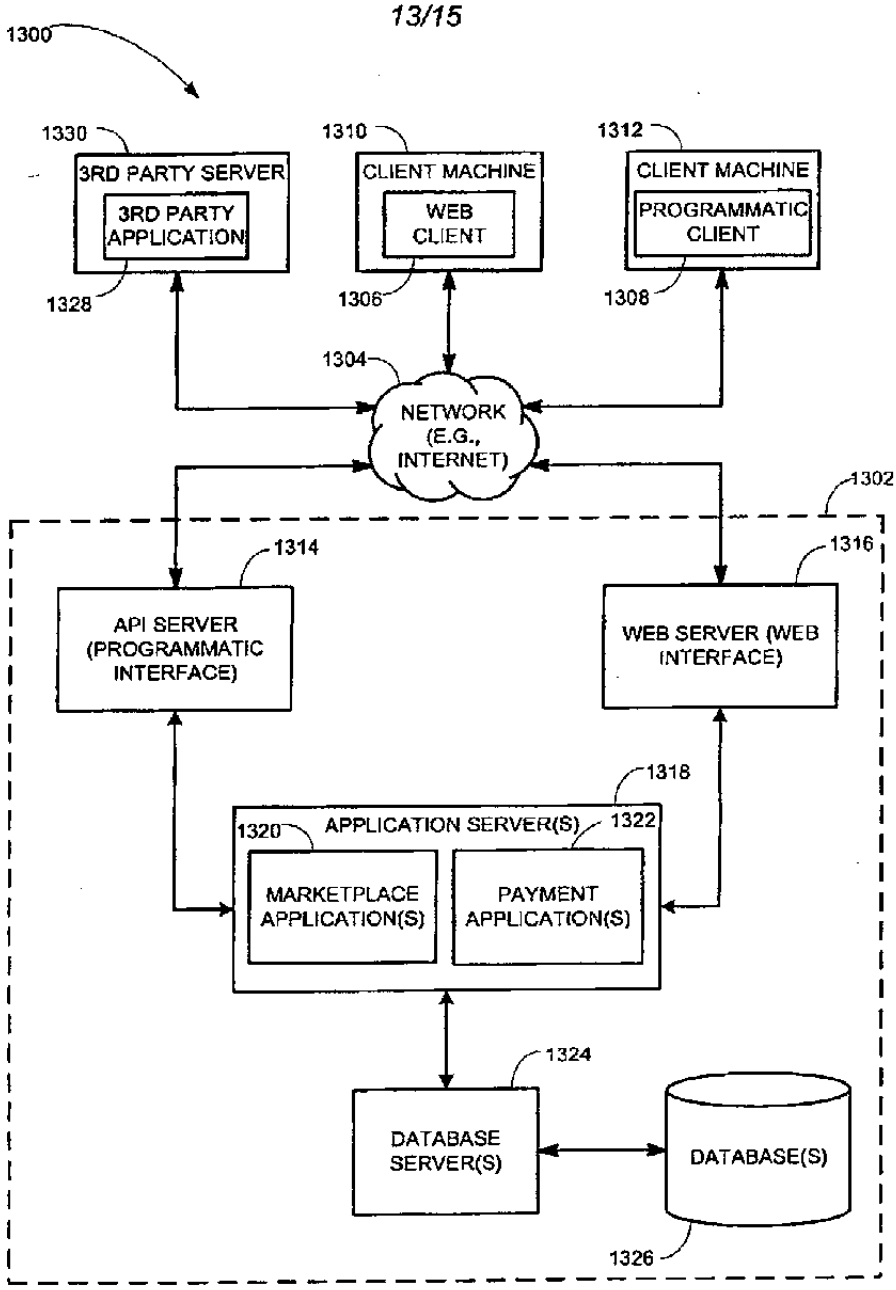

1300
1330
3RD PARTY SERVER
3RD PARTY APPLICATION
1328
1310
CLIENT MACHINE
WEB CLIENT
1306
1312
CLIENT MACHINE
PROGRAMMATIC CLIENT
1308
1304
NETWORK (E.G., INTERNET)
1302
1314
API SERVER (PROGRAMMATIC INTERFACE)
1316
WEB SERVER (WEB INTERFACE)
1318
1320
APPLICATION SERVER(S)
1322
MARKETPLACE APPLICATION(S)
PAYMENT APPLICATION(S)
1324
DATABASE SERVER(S)
DATABASE(S)
1326

FIGURE 13

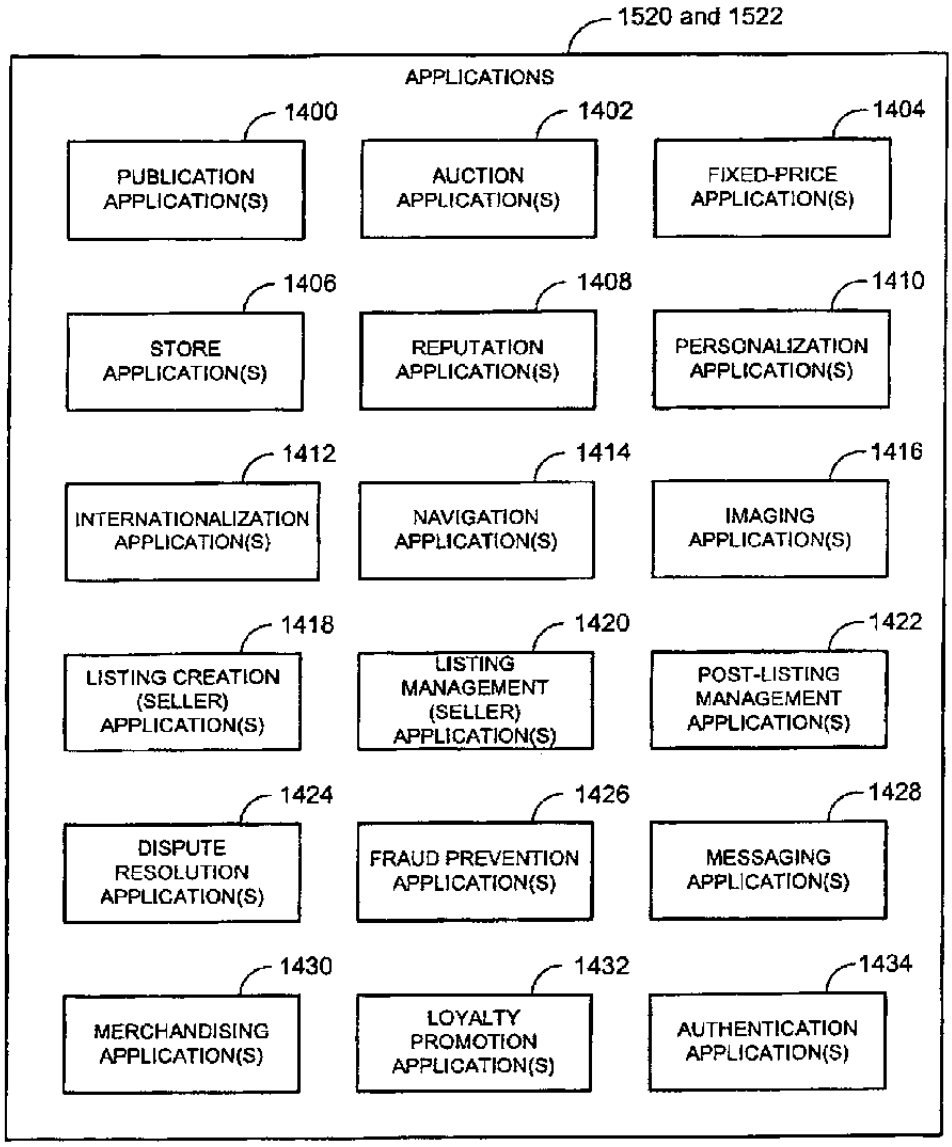

1520 and 1522
APPLICATIONS
1400
PUBLICATION APPLICATION(S)
1402
AUCTION APPLICATION(S)
1404
FIXED-PRICE APPLICATION(S)
1406
STORE APPLICATION(S)
1408
REPUTATION APPLICATION(S)
1410
PERSONALIZATION APPLICATION(S)
1412
INTERNATIONALIZATION APPLICATION(S)
1414
NAVIGATION APPLICATION(S)
1416
IMAGING APPLICATION(S)
1418
LISTING CREATION (SELLER) APPLICATION(S)
1420
LISTING MANAGEMENT (SELLER) APPLICATION(S)
1422
POST-LISTING MANAGEMENT APPLICATION(S)
1424
DISPUTE RESOLUTION APPLICATION(S)
1426
FRAUD PREVENTION APPLICATION(S)
1428
MESSAGING APPLICATION(S)
1430
MERCHANDISING APPLICATION(S)
1432
LOYALTY PROMOTION APPLICATION(S)
1434
AUTHENTICATION APPLICATION(S)

FIGURE 14

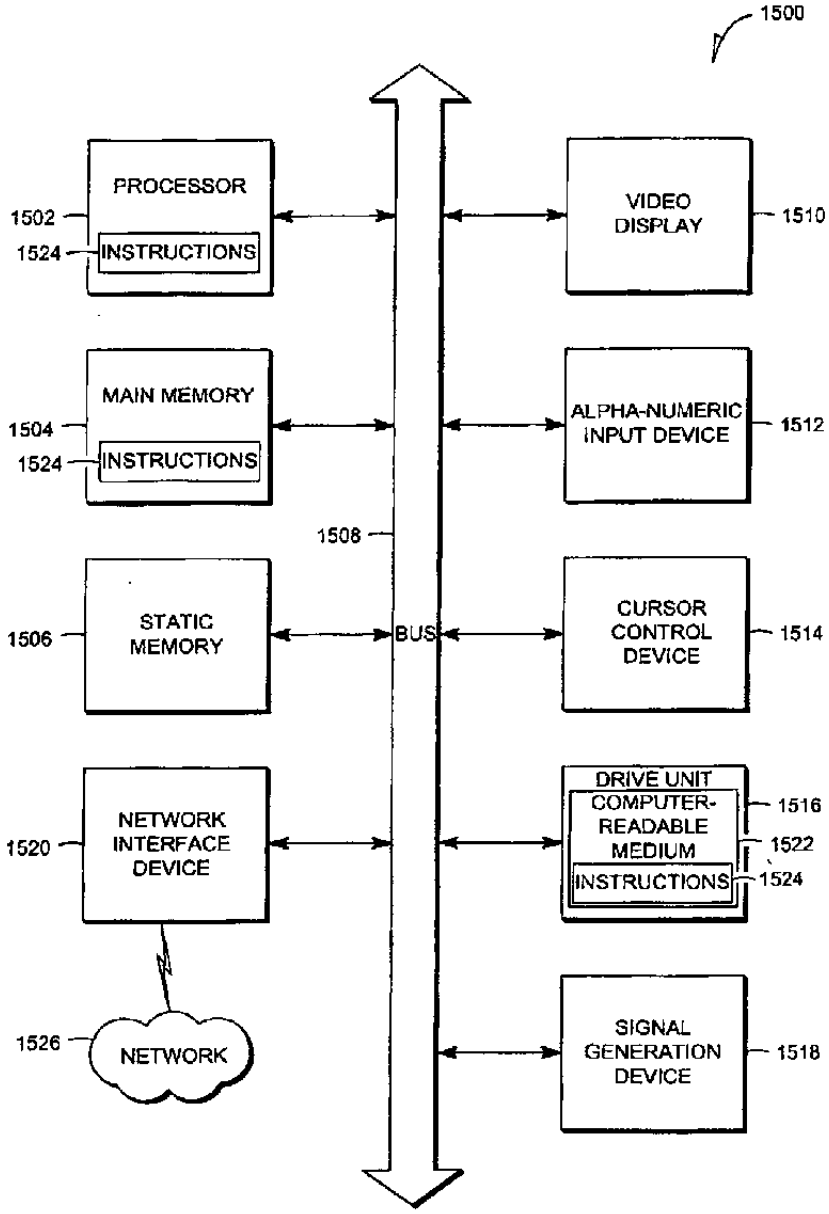

1500
PROCESSOR
1502
1524
INSTRUCTIONS
MAIN MEMORY
1504
1524
INSTRUCTIONS
1508
STATIC MEMORY
1506
BUS
NETWORK INTERFACE DEVICE
1520
1526
NETWORK
VIDEO DISPLAY
1510
ALPHA-NUMERIC INPUT DEVICE
1512
CURSOR CONTROL DEVICE
1514
DRIVE UNIT
COMPUTER-READABLE MEDIUM
1516
1522
INSTRUCTIONS
1524
SIGNAL GENERATION DEVICE
1518

FIGURE 15

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2008/009200

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 40/00 (2008.04)
USPC - 705/44
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - G06Q 40/00 (2008.04)
USPC - 705/44

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase, MicroPatent

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/0267663 A1 (KARNS et al) 30 December 2004 (30.12.2004), entire document	1-6, 21-27, 29-33, 40-46, 49, 50

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 October 2008	05 NOV 2008
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2008/009200

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☒ Claims Nos.: 7-20, 28, 34-39, 47, 48
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

Mastercard, Ex1002, p. 536

Electronic Patent Application Fee Transmittal

Application Number:	13599647
Filing Date:	30-Aug-2012
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Filer:	John L. Adair/Delia Narvaiz
Attorney Docket Number:	Simplytapp0002US1
Filed as Small Entity	

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission Information Disclosure Stmt	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt	
EFS ID:	25379823
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Customer Number:	122870
Filer:	John L. Adair/Delia Narvaiz
Filer Authorized By:	John L. Adair
Attorney Docket Number:	Simplytapp0002US1
Receipt Date:	01-APR-2016
Filing Date:	30-AUG-2012
Time Stamp:	19:33:34
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$90
RAM confirmation Number	5439
Deposit Account	503183
Authorized User	ADAIR, JOHN L
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 CFR 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)

Charge any Additional Fees required under 37 CFR 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		STAPP1100-5_IDS_0401162.pdf	1350549 e1752837a9d43a6e87532961ea4405e21d4 41a0c	yes	4
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Transmittal Letter		1	2	
	Information Disclosure Statement (IDS) Form (SB08)		3	4	
Warnings:					
Information:					
2	Other Reference-Patent/App/Search documents	STAPP1100_Ref_C1.pdf	1235831 0937994161aabbea...0f0fc9e2058fd13429bb8fd 21ed7	no	15
Warnings:					
Information:					
3	Other Reference-Patent/App/Search documents	STAPP1100_Ref_C2.pdf	856298 bd6f669ec962767e0e22d178e77ae2d1189 14272	no	12
Warnings:					
Information:					
4	Other Reference-Patent/App/Search documents	STAPP1100 Ref C3.pdf	1174029 aa53476d91893a0aad7d268e7716cc4a f046b	no	14
Warnings:					
Information:					
5	Other Reference-Patent/App/Search documents	STAPP1100_Ref_C4.pdf	790485 df33cdc93229e4040891363e8f60504dd24 19276	no	11
Warnings:					
Information:					
6	Other Reference-Patent/App/Search documents	STAPP1100_Ref_C5.pdf	13639330 46c03c053a58bc656d9986c7e2dcf7e5748 6ee26	no	14
Warnings:					
Information:					

7	Non Patent Literature	STAPP1100_Ref_C6.pdf	469823 c4491a80e559f1f5f672b52869e7465553231e2ce51	no	14
Warnings:					
Information:					
8	Foreign Reference	STAPP1100_Ref_B1.pdf	5190313 9df4ca186e97dbacc9d3bb01f061ef30a7e5a1df	no	93
Warnings:					
Information:					
9	Foreign Reference	STAPP1100_Ref_B2.pdf	2508542 7579786fd2f5ce5254633 1c1b5d3ecb4f5f74b87	no	53
Warnings:					
Information:					
10	Fee Worksheet (SB06)	fee-info.pdf	31049 8a77f442d6ddddc60aa6d76837564 1f35f4b5cdc	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	27246249		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. (Opt.) **STAPP1100-5**

First Named Inventor **C. Douglas Yeager**	
Application Number **13/599,647**	Date Filed **August 30, 2012**
Title **Systems and Methods for Secure Application-Based Participation in an Interrogation by Mobile Device (as amended)**	
Group Art Unit **3695**	Examiner **Puttaiah, Asha**
Confirmation Number **1919**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certification of Transmission Under 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on April 1 2016.

Delia Narvaiz

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. A copy of foreign patent documents as well as the information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

☐ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☐ This Information Disclosure Statement is being submitted before the mailing of a first Office action on the merits; or

☐ This Information Disclosure Statement is being submitted before the mailing of a first Office action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

☒ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(b) and before the mailing date of any of a final action under 37 C.F.R. § 1.113, a notice of allowance under 37 C.F.R. § 1.311, or an action that otherwise closes prosecution in the application, and is accompanied by one of:

☐ The statement specified in 37 C.F.R. § 1.97(e); or

☒ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $90 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(c) and on or before payment of the issue fee and is accompanied by:

☐ The statement specified in 37 C.F.R. § 1.97(e); and

☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $90 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

Furthermore, pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application.

Applicant does not believe any fees are due and owing at this time. If Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

SPRINKLE IP LAW GROUP
Attorneys for Applicant

John L. Adair
Reg. No. 48,828

Dated: 4/11, 2016

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 317-9088

Power of Attorney to Transact Business with the United States Patent and Trademark Office

I hereby revoke all previous Powers of Attorney given in the application(s) identified in the attached Transmittal for Power of Attorney to One or More Registered Practitioners ("Transmittal Form").

I hereby appoint practitioners associated with the following Customer Number associated with Sprinkle IP Law Group, PC:

44654

as my/our attorney(s) or agent(s) and to transact all business before the United States Patent and Trademark Office (USPTO) in connection with any and all patents and patent applications that are assigned to **SimplyTapp, Inc.** (the "assignee's patents/patent applications") in which they shall appear, any and all assignee's patents/patent applications associated with the above-referenced customer number, and any and all patents and patent applications referenced in the attached Transmittal Form.

Please recognize or change the correspondence address for the patents and patent applications referenced in the attached Transmittal Form to the address associated with the above-referenced customer number.

The undersigned is:

- ☐ Inventor or Joint Inventor
- ☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign
  *the undersigned has authority to act on behalf of the Assignee or Person to Whom the Inventor is Under an Obligation to Assign.
- ☐ Legal Representative of a Deceased or Legally Incapacitated Inventor
- ☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is currently being filed in this document)

The Transmittal Form may be completed and executed by one of the practitioners associated with the above-referenced customer number.

SIGNATURE OF APPLICANT

Signature:		**Date:**	5/2/2016
Name:	**Charles Douglas Yeager**		
Title:	**Chief Executive Officer**		
Company:	**SimplyTapp, Inc.**		

Electronic Acknowledgement Receipt

EFS ID:	25872181
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Customer Number:	122870
Filer:	John L. Adair/Delia Narvaiz
Filer Authorized By:	John L. Adair
Attorney Docket Number:	Simplytapp0002US1
Receipt Date:	24-MAY-2016
Filing Date:	30-AUG-2012
Time Stamp:	16:31:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		STAPP1100-5_Trans_POA_052416.pdf	3608867 35d218c31f461dd6adf6c55dcdaac72eb7e882	yes	4

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Miscellaneous Incoming Letter	1	1
	Assignee showing of ownership per 37 CFR 3.73	2	3
	Power of Attorney	4	4
Warnings:			
Information:			
	Total Files Size (in bytes):	3608867	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
CERTIFICATE OF TRANSMISSION VIA EFS-WEB SYSTEM	Atty. Docket No. **STAPP1100-5**

	First Named Inventor **C. Douglas Yeager**	
	Application Number **13/599,647**	Filing or 371(c) Date **August 30, 2012**
Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450 **Dear Sir**	Title Systems and Methods for Secure Application-Based Participation in an Interrogation by Mobile Device	
	Group Art Unit **3695**	Examiner Name **Puttalah, Asha**
	Conf. No. **1919**	

I hereby certify that the attached Power of Attorney and Transmittal for Power of Attorney are being deposited electronically using the United States Patent and Trademark Office EFS-Web System on **May** 24, **2016**.

Respectfully submitted,

Sprinkle IP Law Group

Delia Narvaiz

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

Patent No./Application No.:	**13/599,647**
Issue Date/Filing Date:	**August 30, 2012**
First Named Inventor:	**C. Douglas Yeager**
Title:	Systems and Methods for Secure Application-Based Participation in an Interrogation by Mobile Device
Assignee:	**SimplyTapp, Inc.**

Assignee is:

1. ☒ Assignee of the entire right, title and interest in the above-referenced patent/patent application;

2. ☐ Assignee of less than the entire right, title and interest in the above-referenced patent/patent application:

☐ The extent (by percentage) of its ownership interest is _____%; or

☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ Assignee of an undivided interest in the entirety of the above-referenced patent/patent application (a complete assignment by one or more of the joint inventors was made). The other parties, including inventor, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ Recipient, via court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is/are attached.

The interest identified in option 1, 2 or 3 above as evidenced by either:

A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 031642, Frame 0304, or for which a copy thereof is attached.

or

B. ☐ A chain of title from the inventor(s) of the patent/patent application identified above, to the current assignee;

1. From: _____ To: _____

   The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame_____, or for which a copy thereof is attached hereto.

2. From: _____ To: _____

   The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame_____, or for which a copy thereof is attached hereto.

3. From: _____ To: _____

   The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame_____, or for which a copy thereof is attached hereto.

☐ Additional documents in the chain of title are listed on the supplemental sheet(s).

☒ Documentary evidence of chain of title from the original owner to the assignee was, or concurrently is being submitted for recordation pursuant to 37 CFR 3.11 [NOTE: A separate copy (i.e., a true copy the original assignment document(s)) must be/have been submitted to the Assignment Division to record the assignment in the records of the USPTO]

Signature of Applicant or Practitioner		
Signature:		**Date:** 5-24-2016
Name:	John L. Adair	**Telephone: 512-637-9220**
Registration No.	48,828	

Mastercard, Ex1002, p. 549

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/599,647	08/30/2012	C. Douglas YEAGER	STAPP1100-5

CONFIRMATION NO. 1919

44654
Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705

POA ACCEPTANCE LETTER

OC000000083383707

Date Mailed: 06/03/2016

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 05/24/2016.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/sleutchit/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/599,647	08/30/2012	C. Douglas YEAGER	Simplytapp0002US1

CONFIRMATION NO. 1919

122870
Hanchuk Kheit LLP
258 Saint Nicholas Avenue, No. 8A
New York, NY 10027-5353

POWER OF ATTORNEY NOTICE

OC000000083383685

Date Mailed: 06/03/2016

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 05/24/2016.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/sleutchit/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/599,617	08/30/2012	C. Douglas YEAGER	STAPP1100-5	1919

44654 7590 06/14/2016

Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705

EXAMINER
PUTTALAH, ASHA

ART UNIT	PAPER NUMBER
3695	

MAIL DATE	DELIVERY MODE
06/14/2016	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 13/599,647	Applicant(s) YEAGER, C. DOUGLAS	
	Examiner ASHA PUTTAIAH	Art Unit 3695	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 March 2016*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *30-58* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *30-58* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *1 April 16*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

4) ☐ Other: _____.

DETAILED ACTION

1. The present application is being examined under the pre-AIA first to invent provisions.

2. The following is a final office action in response to the application filed 22 March 2016.

3. Applicant's amendments to the specification, addition of claims 30-58 and cancellation of Claims 1-29 have been received and are acknowledged. Claims 30-58 have been examined and are pending.

Specification

4. The use of the trademark VISA® and MASTERCARD® has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology (® or ™).

5. Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Information Disclosure Statement

6. The information disclosure statement filed 1 April 2016 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. No copy of the PCT/US2012/053129, mailed 12/10/2013 has been received. As such the listing has been struck-through. It has been placed in the application file, but the information referred to therein has not been considered.

Response to Arguments

7. Applicant's arguments filed 22 March 2016 have been fully considered but they are not persuasive.

8. With regard to the rejections under 35 USC 101, the claims are rejected as cited below. Applicant argues that the new claims are sufficient to pass the Alice test. Examiner notes that the instant claims recite known technology being used in a routine and conventional manner (to send, receive and process data). The recited claims also do not seem to be 'rooted in technology' as the claimed process could be executed by human analogs in the real world. As such Applicant's arguments are not persuasive. Applicant may wish to clarify technological distinctions/improvements of the inventions, if any.

9. With regard to the rejections under 35 USC 102 and 103, Applicant's arguments are moot as the previously rejected claims have been cancelled and a new grounds of rejection have been applied to the new claims.

Claim Rejections - 35 USC § 112

10. The following is a quotation of 35 U.S.C. 112(b):

> (B) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. **Claims 36, 42, 43, 50, 57 and 58** are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

12. **Claims 36 and 50** recite "*...wherein the mobile device does not have connectivity to the wireless network during the interrogation...*" It is unclear what is meant by this recitation as the 'mobile device' must be 'connected to the wireless' system in order to transmit data to the POS during the interrogation. As such the metes and bounds of claims are unclear. Examiner will interpret as an "offline transaction."

13. **Claims 42 and 57** recite "Track 2 format." The limitation seems to be specifying a 'standard format.' As such render the claim indefinite as an industry standard can change upon updates and is therefore, transitory-in-nature. Consequently,

the standard limitation without a set-in-stone definition renders the metes and bounds of the claim confusing.

14. **Claims 43 and 58** recite a "BER-TLV format." The limitation specifying an ISO standard (BER-TLV format) render the claim indefinite as the ISO standard is an industry standard which can change upon updates and is therefore, transitory-in-nature. Consequently, the ISO standard limitation without a set-in-stone definition renders the metes and bounds of the claim confusing.

15. Applicant is respectfully requested to correct the deficiencies noted above. Applicant is also required to provide citation to the original disclosure for any amendments.

Claim Rejections - 35 USC § 101

16. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

17. **Claims 30-58** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

18. When considering subject matter eligibility under 35 U.S.C. 101, (1) it must be determined whether the claim is directed to one of the four statutory categories of invention, i.e., process, machine, manufacture, or composition of matter. If the claim does fall within one of the statutory categories, (2a) it must then be determined whether the claim is directed to a judicial exception (i.e., law of nature, natural phenomenon, and abstract idea), and if so (2b), it must additionally be determined whether the claim is a patent-eligible application of the exception. If an abstract idea is present in the claim, any element or combination of elements in the claim must be sufficient to ensure that the claim amounts to significantly more than the abstract idea itself. Examples of abstract ideas include fundamental economic practices; certain methods of organizing human activities; an idea itself; and mathematical relationships/formulas. *Alice Corporation Pty. Ltd. v. CLS Bank International, et al.*, 573 U.S. ____ (2014).

19. The claimed invention is directed to a judicial exception (i.e. a law of nature, a natural phenomenon, or an abstract idea) without significantly more. In the instant case, the claim(s) as a whole, considering all claim elements both

individually and in combination, do not amount to significantly more than an abstract idea.

20. (1) In the instant case, the claims are directed towards payment and authorization methods using cryptography by a mobile device.

21. (2a) Payment systems and authorization of payments is akin to comparing new and store information and using rules to identify options and an algorithm for calculating parameters indicating an abnormal condition. As such, the claims include an abstract idea. The invention is directed to *a method for secure application-based participation in a payment card transaction authorization process by a mobile device, the method comprising:*

- *receiving over a wireless network at a mobile device a first non-permanent cryptographic key associated with an account having a corresponding digital credential, wherein the mobile device comprises an operating system and an application executable in the operating system, the application interrogable for digital credential data corresponding to the account, wherein the application does not access a permanent cryptographic key associated with the account during interrogations;* which is considered to be receiving, processing and storing data, which are both insignificant extra-solution operations of any general purpose computer (wherein the mobile device/general purpose computer is used in a conventional and routine manner)
- *locally storing a first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;* which is

considered to be receiving, processing and storing data, which are both insignificant extra-solution operations of any general purpose computer (wherein the mobile device/general purpose computer is used in a conventional and routine manner)

- *participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device* (wherein the mobile device/POS is used in a conventional and routine manner)*comprising:*
    - *receiving at least one POS command communication sent by the POS terminal over a communications channel, wherein the at least one POS command communication comprises a request for digital credential data to authorize a transaction against the account;* which is considered to be receiving, processing and storing data, which are both insignificant extra-solution operations of any general purpose computer
    - *generating a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram; and* which is considered to be data matching and receiving, processing and storing data, which are both insignificant extra-solution operations of any general purpose computer.

responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to an electronic reader through the communication channel, the at least one device response communication comprising at least a portion of the digital credential data, wherein the at least a portion of the digital credential data comprises the response cryptogram and an account identifier for the account; which is considered to be receiving or transmitting data over a network, e.g. using the Internet to gather data, which is an insignificant extra-solution operation of any general purpose computer

- *receiving a second non-permanent cryptographic key at the mobile device, wherein the second non-permanent cryptographic key is associated with the account; and ;*
- *replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key as the local cryptographic key associated with the account prior to the application participating in a subsequent interrogation,* which is considered to be performing repetitive transmissions/calculations, which is a conventional operation of any general purpose computer.

22. (2b) In the instant case, Claims 1-2, 3-27 and 28-29 are directed to processes.

23. Additionally, the claims do not include additional elements individually or in combination are sufficient to amount to significantly more than the judicial exception of abstract idea because the claims do not include an improvement to another technology or technical field, an improvement to the functioning of the

computer itself, or meaningful limitations beyond generally linking the use of an abstract idea to a particular technological environment. The dependent claims do not correct the deficiencies of the independent claims.

24. Further, note that the limitations, in the instant claims, are done by the generically recited computing devices (mobile device communicating with a POS terminal). The limitations are merely instructions to implement the abstract idea on a computer and require no more than a generic computer to perform generic computer functions that are well-understood, routine and conventional activities previously known to the industry (mobile device communicating with a POS terminal to send and receive data is known in the industry). Therefore, claims 30-58 are rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter.

Claim Rejections - 35 USC § 103

25. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

26. **Claims 30, 31, 33, 34, 35, 37, 38, 39, 40, 41, 42, 44, 45, 47, 48, 49, 51, 52, 53, 54, 55, 56, and 57** are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over US 20100185545 A1, Royyuru et al. hereinafter referred to as Royyuru further in view of US 5737423, Manduley hereinafter referred to as Manduley.

27. **Claims 30 and 44**

Royurro *discloses a method for secure application-based participation in a payment card transaction authorization process by a mobile device, and a system for secure application-based participation by a mobile device in point-of-sale interrogations, the system comprising:*

a mobile device (See at least Royurro, Fig. 3 [0021] mobile device) *comprising:*

a controller configured to route communications received over a communication channel from an electronic reader; a wireless interface to connect to a wireless network; a processor; a computer readable storage medium

accessible by the processor storing an application interrogable for digital credential data to authorize transactions against an account having a digital credential, the application executable in an operating system of the mobile device to participate in interrogations, (See at least Royurro, Fig. 1-3 [0021] mobile device) *wherein the application is executable to: during an interrogation:*

- *receiving over a wireless network at a mobile device a first non-permanent cryptographic key associated with an account having a corresponding digital credential, wherein the mobile device comprises an operating system and an application executable in the operating system, the application interrogable for digital credential data corresponding to the account, wherein the application does not access a permanent cryptographic key associated with the account during interrogations;* (See at least Royurro, Fig. 3 [0021] mobile device, [0033] dynamic cryptograms… Dynamic Transaction Cryptogram)
- *locally storing a first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account; ;* (See at least Royurro, pg. 9, Table, Card-Key, CK, random CK can by system generated…)
- *participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device comprising:*
    - *receiving at least one POS command communication sent by the POS terminal over a communications channel, wherein the at least*

one POS command communication comprises a request for digital credential data to authorize a transaction against the account; (See at least Royurro, [0044-46] read information from presentation instrument... passed from POS... and/or merchant system via network to payment processor system for approval and/or processing of the transaction)

- *generating a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram; and* (See at least Royurro, Claim 1, Fig. 3 [0021] mobile device, [0033] dynamic cryptograms… Dynamic Transaction Cryptogram)
- *responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to an electronic reader through the communication channel, the at least one device response communication comprising at least a portion of the digital credential data,* (See at least Royurro, [0033] dynamic cryptograms… Dynamic Transaction Cryptogram)

- *wherein the at least a portion of the digital credential data comprises the response cryptogram and an account identifier for the account;* (See at least Royurro, Fig. 3 [0021] mobile device, [0033] dynamic cryptograms… Dynamic Transaction Cryptogram ; pg. 9 table Pseudo-PAN, DTC)

Royurro further discloses the single use cryptogram and a random card key which is system-generated (See at least Royurro, [0033] dynamic cryptograms… Dynamic Transaction Cryptogram…valid for single transaction; pg. 9 table)

Royurro does not directly disclose the following; however, Manduley teaches:

- *receiving a second non-permanent cryptographic key at the mobile device, wherein the second non-permanent cryptographic key is associated with the account; and* (See at least Manduley, Fig. 4 update encryption key, C2L 29-35, update an encryption key used to generate the encryption)
- *replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key as the local cryptographic key associated with the account prior to the application participating in a subsequent interrogation.* (See at least Manduley, Fig. 4 update encryption key, C2L 29-35, update an

encryption key used to generate the encryption; C4L22-41 updated key)

The Supreme Court has supported in *KSR International Co. Teleflex Inc. (KSR), 550US___, 82 USPQ2d 1385 (2007),* that merely applying a known technique to a known method, yield predictable results, render the claimed invention obvious over such combination. In the instant case, Royurro discloses a method and system of handling information related to a financial transactions including mobile devices/card including utilizing dynamic cryptograms including a single use cryptographic key. Manduley is merely another method and system of inspecting transactions of smart cards and updating/re-keying of encryption keys. One of ordinary skill in the art would clearly recognize that this combination would lead to a predictable result (i.e. a method and system of handling information related to a financial transactions including mobile devices/card including utilizing dynamic cryptograms including a single use cryptographic key including updating/re-keying/re-placing the cryptographic key). As such the claimed invention is obvious over Royurro / Manduley.

28. Claims 31 and 45

Royurro and Manduley disclose the invention as claims above in Claims 30 and 44.

Royurro further discloses:

- *wherein the mobile device is an NFC emulating device.* (See at least Royurro, [0044-0046] NFC modules)

29. Claims 33 and 47

Royurro and Manduley disclose the invention as claims above in Claims 30 and 44.

Royurro further discloses:

- *wherein the interrogation conforms to a card specification, the set of inputs is specified by the card specification and the at least one device response is formulated according to the card specification.* (See at least Royurro, pg. 9 table Pseudo-PAN, DTC)

30. Claims 34 and 48

Royurro and Manduley disclose the invention as claims above in Claims 33 and 47.

Royurro further discloses:

- *wherein the request for digital credential data comprises a request for a first cryptogram according to the card specification and the at least one device response communication comprises a second cryptogram, wherein the second cryptogram is the response cryptogram.* (See at least Royurro, pg. 9 table Pseudo-PAN, DTC…wherein the DTC is the response cryptogram)

31. Claims 35 and 49

Royurro and Manduley disclose the invention as claims above in Claims 30 and 44.

Royurro further discloses:

- *wherein generating the response cryptogram comprises encrypting the set of inputs using the local cryptographic key according to a digital encryption standard (DES) calculation to generate an output, wherein the response cryptogram includes a portion, but not all, of the output.* (See at least Royurro, [0032] dynamic Primary Account Number (PAN)…portion of the real PAN can be retained)

32. Claim 37

Royurro and Manduley disclose the invention as claims above in Claims 30 and 44.

Royurro further discloses:

- *prior to the interrogation, generating at a remote system the first non-permanent cryptographic key,* (See at least Royurro, pg. 9, Table, Card-Key, CK, random CK can by system generated…)
- *associating the first non-permanent cryptographic key with the account, and* (See at least Royurro, Claim 1, Fig. 3 [0021] mobile device, [0033] dynamic cryptograms… Dynamic Transaction Cryptogram)

- *sending the first non-permanent cryptographic key and the account identifier to the mobile device over the wireless network; and* (See at least Royurro, pg. 9, Table, Card-Key, CK, random CK can by system generated…)

Royurro does not directly disclose; however, Manduley teaches:

- *after the interrogation generating at the remote system, the second non-permanent cryptographic key, associating the second non-permanent cryptographic key with the account and* (See at least Manduley, Fig. 4 update encryption key, C2L 29-35, update an encryption key used to generate the encryption)
- *sending the second non-permanent cryptographic key and the account identifier to the mobile device over the wireless network.* (See at least Manduley, Fig. 4 update encryption key, C2L 29-35, update an encryption key used to generate the encryption; C4L22-41 updated key)

33. Claims 38 and 53

Royurro and Manduley disclose the invention as claims above in Claims 37 and 52.

Royurro further discloses:

- *wherein the digital credential comprises a secure element representation maintained at the remote system.* (See at least Royurro, [0033] institution key;

pg. 8-9 table [0057] institution key…stored in the database or repository of the payment processor)

34. Claims 39 and 54

Royurro and Manduley disclose the invention as claims above in Claims 30 and 44.

Royurro further discloses:

- *receiving an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the response cryptogram and the account identifier;* (See at least Royurro, [0048] authorization request…PAN …DTC)
- *determining a current non-permanent cryptographic key associated with the account using the account identifier;* (See at least Royurro, pg. 9, Table, Card-Key, CK, random CK can by system generated…)
- *calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account;* (See at least Royurro, Fig. 3 [0021] mobile device, [0033] dynamic cryptograms… Dynamic Transaction Cryptogram ; pg. 9 table Pseudo-PAN, DTC [0047])
- *verifying a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram;* (See at least Royurro, [0044-46] read information from presentation instrument... passed from POS... and/or merchant

system via network to payment processor system for approval and/or processing of the transaction…approval or denial response….)

- *and sending an authorization response to the POS terminal,* (See at least Royurro, [0044-46] read information from presentation instrument... passed from POS... and/or merchant system via network to payment processor system for approval and/or processing of the transaction [0049-0050] if authorized, and authorization code…)
- *wherein the data contained in the authorization response is determined, at least in part, by the verifying the correctness of the response cryptogram.* (See at least Royurro, [0044-46] read information from presentation instrument... passed from POS... and/or merchant system via network to payment processor system for approval and/or processing of the transaction[0048-0050] DTC… decryption module)

35. Claims 40 and 55

Royurro and Manduley disclose the invention as claims above in Claims 39 and 54.

Royurro further discloses:

- *wherein: the set of inputs comprises unpredictable data; the authorization data comprises the unpredictable data; and the calculated cryptogram is calculated using the unpredictable data.* (See at least Royurro, [0051] unpredictable

numbers or counters; pg. 10 table, unpredictable number, DTC … combining several fields including unpredictable number)

36. Claims 41 and 56

Royurro and Manduley disclose the invention as claims above in Claims 40 and 55.

Royurro further discloses:

- *wherein the POS command communications comprise the unpredictable data.* (See at least Royurro, [0051] unpredictable numbers or counters; pg. 10 table, unpredictable number)

37. Claims 42 and 57

Royurro and Manduley disclose the invention as claims above in Claims 41 and 55.

Royurro further discloses:

- *wherein the authorization data further comprises values from the transaction and wherein the POS terminal communicates the values from the transaction, the response cryptogram and the account identifier to the remote system in track 2 format.* (See at least Royurro, pg. 7 [0049] Track 2 layout)

38. Claim 51

Royurro and Manduley disclose the invention as claims above in Claim 44.

Royurro does not directly disclose; however, Manduley teaches:

- *wherein the mobile device is programmed to request a new non-permanent cryptographic key after the interrogation.* (See at least Manduley, Fig. 4 update encryption key, C2L 29-35, update an encryption key used to generate the encryption; C4L22-41 updated key)

39. Claim 52

Royurro and Manduley disclose the invention as claims above in Claim 44.

Royurro further discloses:

- *further comprising a remote computer system configured to generate the non-permanent cryptographic keys associated with the account and send each of the non-permanent cryptographic keys and the account identifier to the mobile device over the wireless network.* (See at least Royurro, [0037] wireless network)

40. **Claims 32 and 46** are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Royyuru further in view of Manduley further in view of non-patent literature Wikipedia: Cryptographic hash function (https://en.wikipedia.org/w/index.php?title=Cryptographic_hash_function&oldid=344034775) 14 Feb 2010 hereinafter referred to as Wikipedia:Hash

41. Claims 32 and 46

Royurro and Manduley disclose the invention as claims above in Claims 30 and 44.

Royurro does not directly disclose the following; however, Wikipedia teaches:

Cryptographic hash function teaches:

- *wherein the response cryptogram is a hash.* (See at least Wikipedia: Cryptographic hash function : functions have many information security applications including authentication)

The Supreme Court has supported in *KSR International Co. Teleflex Inc. (KSR), 550US___, 82 USPQ2d 1385 (2007),* that merely applying a known technique to a known method, yield predictable results, render the claimed invention obvious over such combination. In the instant case, Royurro discloses a method and system of handling information related to a financial transactions including mobile devices/card including utilizing dynamic cryptograms including encrypting keys. Wikipedia: Hash is merely a description/definition of a known procedure used in encryption. One of ordinary skill in the art would clearly recognize that this combination would lead to a predictable result (i.e. a method and system of handling information related to a financial transactions including mobile devices/card including utilizing dynamic cryptograms including using known techniques/procedures such as the use of hash). As such the claimed invention is obvious over Royurro / Wikipedia: Hash.

42. **Claims 36 and 50** are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Royyuru further in view of Manduley further in view of US 2010/0317318 Al, Carter hereinafter referred to as Carter.

43. **Claims 36 and 50**

Royurro and Manduley disclose the invention as claims above in Claims 30 and 44.

Royurro does not directly disclose; however, Carter teaches:

- *wherein the mobile device does not have connectivity to the wireless network during the interrogation.* (See Carter, [0032] offline purchase transaction…proximity reader… POS terminal…mobile telephone [0042] transaction clearing application.... clear office transactions)

The Supreme Court has supported in *KSR International Co. Teleflex Inc. (KSR), 550US___, 82 USPQ2d 1385 (2007),* that merely applying a known technique to a known method, yield predictable results, render the claimed invention obvious over such combination. In the instant case, Royurro discloses a method and system of handling information related to a financial transactions including mobile devices/card including utilizing dynamic cryptograms including encrypting keys. Carter is a method of authorizing transactions using a mobile device including an offline feature. One of ordinary skill in the art would clearly recognize that this combination would lead to a predictable result (i.e. a method and system of handling information related to a financial transactions including

mobile devices/card including utilizing dynamic cryptograms including authorizing transactions using a mobile device including an offline feature). As such the claimed invention is obvious over Royurro /Carter.

44. **Claims 43 and 58** are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Royyuru further in view of Manduley further in view of ISO 7816-4(http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816-4_annex-d.aspx) 13 Feb 2009 hereinafter referred to as ISO 7816-4.

45. **Claims 43 and 58**

Royurro and Manduley disclose the invention as claims above in Claims 41 and 55.

Royurro does not directly disclose; however, ISO 7816-4 teaches:

- *wherein the authorization data further comprises values from the transaction and wherein the POS terminal communicates values from the transaction, the response cryptogram and the account identifier in BER-TLV format.* (See at least ISO 7816-4, BER-TLV data object…)

The Supreme Court has supported in *KSR International Co. Teleflex Inc. (KSR), 550US___, 82 USPQ2d 1385 (2007),* that merely applying a known technique to a known method, yield predictable results, render the claimed invention obvious over such combination. In the instant case, Royurro discloses a method and system of handling information related to a financial transactions

including mobile devices/card including utilizing dynamic cryptograms including a single use cryptographic key. ISO 7816-4 is a known protocol standard/technology to establish communications. One of ordinary skill in the art would clearly recognize that this combination would lead to a predictable result (i.e. a method and system of handling information related to a financial transactions including mobile devices/card including utilizing dynamic cryptograms including a single use cryptographic key which uses a known protocol standard to establish communications). As such the claimed invention is obvious over Royurro / ISO 7816-4.

Conclusion

46. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

47. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

48. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ASHA PUTTAIAH whose telephone number is (571)270-1352. The examiner can normally be reached on Monday- Friday 8:00am - 5:00 pm EST.

49. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ryan Donlon can be reached on (571) 270-3602. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

50. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ASHA PUTTAIAH/
Primary Examiner, Art Unit 3695

Notice of References Cited	Application/Control No. 13/599,647	Applicant(s)/Patent Under Reexamination YEAGER, C. DOUGLAS	
	Examiner ASHA PUTTAIAH	Art Unit 3695	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-5,636,280 A	06-1997	Kelly; Tadhg	G06F21/31	380/281
*	B	US-2012/0109764 A1	05-2012	Martin; Philippe	G06Q20/204	705/17
*	C	US-2004/0143550 A1	07-2004	Creamer, Thomas E.	G06Q20/04	705/41
*	D	US-2008/0040285 A1	02-2008	Wankmueller; John	G06Q20/32	705/67
*	E	US-2010/0185545 A1	07-2010	Royyuru; Vijay K.	G06Q20/04	705/67
*	F	US-5,737,423 A	04-1998	Manduley; Flavio M.	G06K19/0723	380/273
*	G	US-2010/0317318 A1	12-2010	Carter; Ronald D.	G06Q20/20	455/408
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author. Title Date, Publisher. Edition or Volume. Pertinent Pages)
	U	ISO 7816-4(http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816-4_annex-d.aspx) 13 Feb 2009
	V	Wikipedia: Cryptographic hash function (https://en.wikipedia.org/w/index.php?title=Cryptographic_hash_function&oldid=344034775) 14 Feb 2010
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

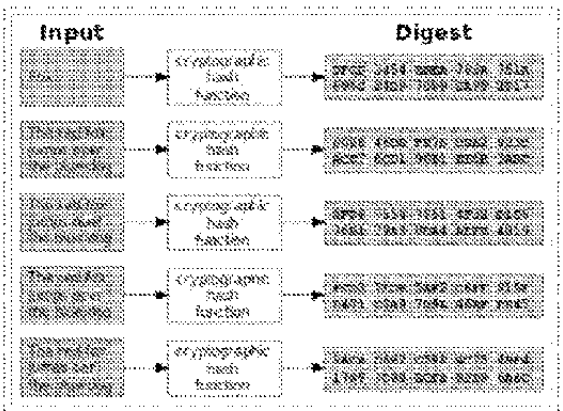
Cryptographic hash function

From Wikipedia, the free encyclopedia

This is an old revision of this page, as edited by 87.212.60.124 (talk) at 15:44, 14 February 2010 (→See also). The present address (URL) is a permanent link to this revision, which may differ significantly from the current revision (https://en.wikipedia.org/wiki/Cryptographic_hash_function).

(diff) ← Previous revision | Latest revision (diff) | Newer revision → (diff)

A **cryptographic hash function** is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the **(cryptographic) hash value,** such that an accidental or intentional change to the data will change the hash value. The data to be encoded is often called the "message", and the hash value is sometimes called the **message digest** or simply **digest**.



A cryptographic hash function (specifically, SHA-1) at work. Note that even small changes in the source input (here in the word "over") drastically change the resulting output, by the so-called avalanche effect.

The ideal cryptographic hash function has four main properties:

- it is easy to compute the hash value for any given message,
- it is infeasible to find a message that has a given hash,
- it is infeasible to modify a message without changing its hash,
- it is infeasible to find two different messages with the same hash.

Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication. They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. Indeed, in information security contexts, cryptographic hash values are sometimes called **(digital) fingerprints, checksums,** or just **hash values,** even though all these terms stand for functions with rather different properties and purposes.

Contents

1 Properties
- 1.1 Meaning of "hard"

2 Applications

3 Hash functions based on block ciphers

4 Merkle-Damgård construction

5 Use in building other cryptographic primitives

6 Concatenation of cryptographic hash functions

7 Cryptographic hash algorithms

8 See also

9 References

10 Further reading

Mastercard, Ex1002, p. 583

Properties

Most cryptographic hash functions are designed to take a string of any length as input and produce a fixed-length hash value.

A cryptographic hash function must be able to withstand all known types of cryptanalytic attack. As a minimum, it must have the following properties:

- *Preimage resistance*: given a hash h it should be hard to find any message m such that $h = \text{hash}(m)$. This concept is related to that of one way function. Functions that lack this property are vulnerable to preimage attacks.
- *Second preimage resistance*: given an input m_1, it should be hard to find another input, m_2 (not equal to m_1) such that $\text{hash}(m_1) = \text{hash}(m_2)$. This property is sometimes referred to as *weak collision resistance*. Functions that lack this property are vulnerable to second preimage attacks.
- *Collision resistance*: it should be hard to find two different messages m_1 and m_2 such that $\text{hash}(m_1) = \text{hash}(m_2)$. Such a pair is called a (cryptographic) hash collision, and this property is sometimes referred to as *strong collision resistance*. It requires a hash value at least twice as long as what is required for preimage-resistance, otherwise collisions may be found by a birthday attack.

These properties imply that a malicious adversary cannot replace or modify the input data without changing its digest. Thus, if two strings have the same digest, one can be very confident that they are identical.

A function meeting these criteria may still have undesirable properties. Currently popular cryptographic hash functions are vulnerable to *length-extension* attacks: given $h(m)$ and $len(m)$ but not m, by choosing a suitable m' an attacker can calculate $h(m \,||\, m')$, where $||$ denotes concatenation. This property can be used to break naive authentication schemes based on hash functions. The HMAC construction works around these problems.

Ideally, one may wish for even stronger conditions. It should be impossible for an adversary to find two messages with substantially similar digests; or to infer any useful information about the data, given only its digest. Therefore, a cryptographic hash function should behave as much as possible like a random function while still being deterministic and efficiently computable.

Checksum algorithms, such as CRC32 and other cyclic redundancy checks, are designed to meet much weaker requirements, and are generally unsuitable as cryptographic hash functions. For example, a CRC was used for message integrity in the WEP encryption standard, but an attack was readily discovered which exploited the linearity of the checksum.

Meaning of "hard"

In cryptographic practice, "hard" generally means "almost certainly beyond the reach of any adversary who must be prevented from breaking the system for as long as the security of the system is deemed important." The meaning of the term is therefore somewhat dependent on the application, since the effort that a malicious agent may put into the task is usually proportional to his expected gain. However, since the needed effort usually grows very quickly with the digest length, even a thousand-fold advantage in processing power can be neutralized by adding a few dozen bits to the latter.

In some theoretical analyses "hard" has a specific mathematical meaning, such as *not solvable in asymptotic polynomial time*. Such interpretations of the word "hard" are important in the study of provably secure cryptographic hash functions but do not usually have a strong connection to practical security. For example, an exponential time algorithm can sometimes still be fast enough to make a feasible attack.

Applications

A typical use of a cryptographic hash would be as follows: Alice poses a tough math problem to Bob, and claims she has solved it. Bob would like to try it himself, but would yet like to be sure that Alice is not bluffing. Therefore, Alice writes down her solution, appends a random nonce, computes its hash and tells Bob the hash value (whilst keeping the solution and nonce secret). This way, when Bob comes up with the solution himself a few days later, Alice can prove that she had the solution earlier by revealing the nonce to Bob. (This is an example of a simple commitment scheme; in actual practice, Alice and Bob will often be computer programs, and the secret would be something less easily spoofed than a claimed puzzle solution).

Another important application of secure hashes is verification of message integrity. Determining whether any changes have been made to a message (or a file), for example, can be accomplished by comparing message digests calculated before, and after, transmission (or any other event).

A message digest can also serve as a means of reliably identifying a file; several source code management systems, including Git, Mercurial and Monotone, use the sha1sum of various types of content (file content, directory trees, ancestry information, etc) to uniquely identify them.

A related application is password verification. Passwords are usually not stored in cleartext, for obvious reasons, but instead in digest form. To authenticate a user, the password presented by the user is hashed and compared with the stored hash. This is sometimes referred to as one-way encryption.

For both security and performance reasons, most digital signature algorithms specify that only the digest of the message be "signed", not the entire message. Hash functions can also be used in the generation of pseudorandom bits.

Hashes are used to identify files on peer-to-peer filesharing networks. For example, in an ed2k link, an MD4-variant hash is combined with the file size, providing sufficient information for locating file sources, downloading the file and verifying its contents. Magnet links are another example. Such file hashes are often the top hash of a hash list or a hash tree which allows for additional benefits.

Hash functions based on block ciphers

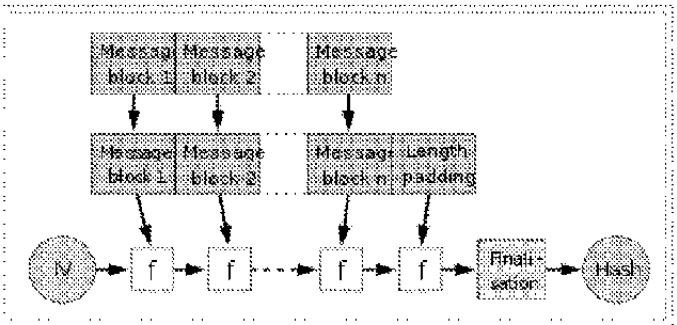
There are several methods to use a block cipher to build a cryptographic hash function, specifically a one-way compression function.

The methods resemble the block cipher modes of operation usually used for encryption. All well-known hash functions, including MD4, MD5, SHA-1 and SHA-2 are built from block-cipher-like components designed for the purpose, with feedback to ensure that the resulting function is not bijective.

A standard block cipher such as AES can be used in place of these custom block ciphers; this generally carries a cost in performance, but can be advantageous where a system needs to perform hashing and another cryptographic function such as encryption that might use a block cipher, but is constrained in the code size or hardware area it must fit into, such as in some embedded systems like smart cards.

Merkle-Damgård construction

A hash function must be able to process an arbitrary-length message into a fixed-length output. This can be achieved by breaking the input up into a series of equal-sized blocks, and operating on them in sequence using a one-way compression function. The compression function can either be specially designed for hashing or be built from a block cipher. A hash function built with the Merkle-Damgård construction is as resistant to collisions as is its compression function; any collision for the full hash function can be traced back to a collision in the compression function.



The Merkle-Damgård hash construction.

The last block processed should also be unambiguously length padded; this is crucial to the security of this construction. This construction is called the Merkle-Damgård construction. Most widely used hash functions, including SHA-1 and MD5, take this form.

The construction has certain inherent flaws, including length-extension and generate-and-paste attacks, and cannot be parallelized. As a result, many entrants in the current NIST hash function competition are built on different, sometimes novel, constructions.

Use in building other cryptographic primitives

Hash functions can be used to build other cryptographic primitives. For these other primitives to be cryptographically secure, care must be taken to build them correctly.

Message authentication codes (MACs) are often built from hash functions. HMAC is such a MAC.

Just as block ciphers can be used to build hash functions, hash functions can be used to build block ciphers. Luby-Rackoff constructions using hash functions can be provably secure if the underlying hash function is secure. Also, many hash functions (including the SHA hash functions) are built by using a special-purpose block cipher in a Davies-Meyer or other construction; that cipher can also be used in a conventional mode of operation, without the same security guarantees. See SHACAL, BEAR and LION.

Pseudorandom number generators (PRNGs) can be built using hash functions. This is done by combining a (secret) random seed with a counter and hashing it.

Some hash functions, such as Skein, Keccak, and RadioGatún output an arbitrarily long stream and can be used as a stream cipher; stream ciphers can also be built from fixed-length digest hash functions. Often this is done by first building a cryptographically secure pseudorandom number generator and then using its stream of random bytes as keystream. SEAL is a stream cipher that uses SHA-1 to generate internal tables, which are then used in a keystream generator more or less unrelated to the hash algorithm; SEAL is not guaranteed to be as strong (or weak) as SHA-1.

Concatenation of cryptographic hash functions

Concatenating outputs from multiple hash functions provides collision resistance at least as good as the strongest of the algorithms included in the concatenated result.[1] For example, SSL uses concatenated MD5 and SHA-1 sums; that ensures that a method to find collisions in in one of the functions doesn't allow forging traffic protected with both functions.

However, for Merkle-Damgård hash functions, the concatenated function is only *as strong* as the best component, not *stronger*.[2] Joux[3] noted that 2-collisions lead to n-collisions: if it is feasible to find two messages with the same MD5 hash, it is effectively no more difficult to find as many messages as the attacker desires with identical MD5 hashes. Among the n messages with the same MD5 hash, there is likely to be a collision in SHA-1. The additional work needed to find the SHA-1 collision (beyond the exponential birthday search) is polynomial. This argument is summarized by Finney (http://article.gmane.org/gmane.comp.encryption.general/5154).

Cryptographic hash algorithms

There is a long list of cryptographic hash functions, although many have been found to be vulnerable and should not be used. Even if a hash function has never been broken, a successful attack against a weakened variant thereof may undermine the experts' confidence and lead to its abandonment. For instance, in August 2004 weaknesses were found in a number of hash functions that were popular at the time, including SHA-0, RIPEMD, and MD5. This has called into question the long-term security of later algorithms which are derived from these hash functions — in particular, SHA-1 (a strengthened version of SHA-0), RIPEMD-128, and RIPEMD-160 (both strengthened versions of RIPEMD). Neither SHA-0 nor RIPEMD are widely used since they were replaced by their strengthened versions.

As of 2009, the two most commonly used cryptographic hash functions are MD5 and SHA-1. However, MD5 has been broken; an attack against it was used to break SSL in 2008.[4]

SHA-0 and SHA-1 are members of the SHA family of hash functions developed by the NSA. In February 2005, a successful attack on SHA-1 was reported, finding collisions in about 2^{69} hashing operations, rather than the 2^{80} expected for a 160-bit hash function. In August 2005, another successful attack on SHA-1 was reported, finding collisions in 2^{63} operations. Theoretical weaknesses of SHA-1 exist as well,[5][6] suggesting that it may be practical to break within years. New applications can avoid these problems by using more advanced members of the SHA family, such as SHA-2, or using techniques such as randomized hashing[7][8] that do not require collision resistance.

However, to ensure the long-term robustness of applications that use hash functions, there is a competition to design a replacement for SHA-2, which will be given the name SHA-3 and become a FIPS standard around 2012.[9]

Some of the following algorithms are known to be insecure; consult the article for each specific algorithm for more information on the status of each algorithm. Note that this list does not include candidates in the current NIST hash function competition. For additional hash functions see the box at the bottom of the page.

Algorithm	Output size (bits)	Internal state size	Block size	Length size	Word size	Collision attacks (complexity)	Preimage attacks (complexity)
GOST	256	256	256	256	32	No	
HAVAL	256/224/192/160/128	256	1024	64	32	Yes	
MD2	128	384	128	No	32	Almost	
MD4	128	128	512	64	32	Yes (2^8)[10]	With flaws (2^{102})[11]
MD5	128	128	512	64	32	Yes (2^{32})[12]	No
PANAMA	256	8736	256	No	32	Yes	
RadioGatún	Arbitrarily long	58 words	3 words	No	1-64	With flaws (2^{352} or 2^{704})[13]	
RIPEMD	128	128	512	64	32	Yes	
RIPEMD-128/256	128/256	128/256	512	64	32	No	
RIPEMD-160/320	160/320	160/320	512	64	32	No	
SHA-0	160	160	512	64	32	Yes (2^{39})[14]	
SHA-1	160	160	512	64	40	Proven (2^{63}), With flaws (2^{52})[15]	No
SHA-256/224	256/224	256	512	64	32	No	No
SHA-512/384	512/384	512	1024	128	64	No	No
Tiger(2)-192/160/128	192/160/128	192	512	64	64	"Pseudo-near collision"[16]	
WHIRLPOOL	512	512	512	256	8	No	

Note: The *internal state* here means the "internal hash sum" after each compression of a data block. Most hash algorithms also internally use some additional variables such as length of the data compressed so far since that is needed for the length padding in the end. See the Merkle-Damgård construction for details.

See also

- Avalanche effect
- Comparison of cryptographic hash functions
- MD5CRK
- Message authentication code
- Keyed-hash message authentication code
- UOWHF - Universal One Way Hash Functions.
- CRYPTREC and NESSIE - Projects which recommend hash functions.
- PGP word list
- Template:User committed identity for instructions on how to create a hash for Wikipedia.
- SHA-3
- Provably secure cryptographic hash function

References

1. If one has two plaintexts p1 and p2 such that (MD5(p1), SHA1(p1)) = (MD5(p2), SHA1(p2)), then MD5(p1)=MD5(p2) and SHA1(p1)=SHA1(p2), by the definition of concatenation. Finding p1 and p2 such that MD5(p1)=MD5(p2) is the definition of a successful collision attack on MD5, and finding p1 and p2 such that SHA1(p1)=SHA1(p2) is the definition of a successful collision attack against SHA1.
2. More generally, if an attack can produce a collision in one hash function's ***internal state***, attacking the combined construction is only as

difficult as a birthday attack against the other function(s). For the detailed argument, see the Joux and Finney references that follow.
3. Antoine Joux. *Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions*. LNCS 3152/2004, pages 306-316 Full text (http://www.springerlink.com/index/DWWVMQJU0N0A3UGJ.pdf).
4. Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger, MD5 considered harmful today: Creating a rogue CA certificate (http://www.win.tue.nl/hashclash/rogue-ca/), accessed March 29, 2009
5. Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu, Finding Collisions in the Full SHA-1 (http://people.csail.mit.edu/yiqun/SHA1AttackProceedingVersion.pdf)
6. Bruce Schneier, Cryptanalysis of SHA-1 (http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html) (summarizes Wang et al. results and their implications)
7. Shai Halevi, Hugo Krawczyk, Update on Randomized Hashing (http://csrc.nist.gov/groups/ST/hash/documents/HALEVI_UpdateonRandomizedHashing0824.pdf)
8. Shai Halevi and Hugo Krawczyk, Randomized Hashing and Digital Signatures (http://www.ee.technion.ac.il/~hugo/rhash/)
9. NIST.gov - Computer Security Division - Computer Security Resource Center (http://csrc.nist.gov/groups/ST/hash/sha-3/index.html)
10. http://www.infosec.sdu.edu.cn/uploadfile/papers/Cryptanalysis%20of%20the%20Hash%20Functions%20MD4%20and%20RIPEMD.pdf
11. http://www.nis-summer-school.eu/presentations/bart_preneel_lecture.pdf
12. http://www.win.tue.nl/hashclash/fastcoll.pdf
13. http://eprint.iacr.org/2008/515
14. http://www.infosec.sdu.edu.cn/paper/sha0-crypto-author-new.pdf
15. http://www.schneier.com/blog/archives/2009/06/ever_better_cry.html
16. http://dx.doi.org/10.1007%2F978-3-540-76900-2_33

Further reading

- Bruce Schneier. *Applied Cryptography*. John Wiley & Sons, 1996. ISBN 0471128457.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Cryptographic_hash_function&oldid=344034775"

Categories: Cryptography | Cryptographic primitives | Cryptographic hash functions | Hashing | Articles with Alice and Bob explanations

- This version of the page has been revised. Besides normal editing, the reason for revision may have been that this version contains factual inaccuracies, vandalism, or material not compatible with the Creative Commons Attribution-ShareAlike License.

Mastercard, Ex1002, p. 588

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13599647	YEAGER, C. DOUGLAS
	Examiner	Art Unit
	ASHA PUTTAIAH	3695

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor Search	9/27/2015	AP
East Search (please see attached)	9/29/2015	AP
East Search (please see attached)	6/10/2016	AP

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/ASHA PUTTAIAH/ Examiner.Art Unit 3695	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/599,647
				Filing Date	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	Puttaiah, Asha
Sheet	1	of	1	Attorney Docket Number	STAPP11100-5

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A21	US 20120317628	12-13-2012	Yeager	
	A22	US 20020026414	02-28-2002	Nakajima et al.	
	A23	US 20100153721	06-17-2010	Mellqvist	
	A24	US 20110099079	04-28-2011	White	
	A25	US 20090210308	08-20-2009	Toomer et al.	
	A26	US 20090143104	06-04-2009	Loh et al.	
	A27	US 20070156436	07-05-2007	Fisher et al.	
	A28	US 20090075592	03-19-2009	Nystrom et al.	
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
/A.P./	B1	WO 2001/008113	02-01-2001	Visa Int'l Service Assn	
/A.P./	B2	WO 2009/017754	02-05-2009	Ebay Inc.	

Examiner Signature		Date Considered	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.P./

Substitute Form PTO/SB/08b

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/599,647
				Filing Date	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	Puttaiah, Asha
Sheet	1	of	1	Atty Docket Number	STAPP1100-5

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
/A.P./	C1	International Search Report and Written Opinion for Int'l Application No. PCT/US2012/041670, mailed 08/17/2012, 15 pgs.	
/A.P./	C2	International Search Report and Written Opinion for Int'l Application No. PCT/US2012/053129, mailed 11/16/2012, 12 pgs.	
/A.P./	C3	International Preliminary Report on Patentability for Int'l Application No. PCT/US2012/041670, mailed 12/10/2013, 14 pgs.	
	C4	International Preliminary Report on Patentability for Int'l Application No. PCT/US2012/053129, mailed 12/10/2013, 11 pgs.	
/A.P./	C5	European Search Report for European Patent Application No. 12827026.1, dated 05/05/2015, 14 pgs.	
/A.P./	C6	Office Action for U.S. Patent Application No. 13/491,922, mailed 07/27/2015, 14 pgs.	

Examiner Signature	/Asha Puttaiah/	Date Considered	06/08/2016	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.P./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	20	("20040118914" | "20070266131" | "20070278291" | "20110140841" | "20060022033" | "20090124234" | "20100185545" | "20100274726" | "6199762" | "7774231" | "20100207742" | "20080046367" | "20070075133" | "20090006262" | "20110112918" | "20060224470" | "20030163708" | "20080238610" | "20090044012" | "20080219444").PN.	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:04
S2	84	"pos command"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:05
S3	2	"expected cryptogram"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:06
S4	0	"pos command" with (expected adj value adj cryptogram)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:07
S5	0	"pos command" same (expected adj value adj cryptogram)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:07
S6	0	"pos command" same (expected with value with cryptogram)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:07
S7	1	"pos command" same (cryptogram)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:07
S8	1	"pos command" and cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:07
S9	1	"unexpected cryptogram"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:08
S11	20	cryptogram same value same expected	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:09
S12	5	cryptogram same value same expected and (mobile with point)	US-PGPUB; USPAT;	AND	OFF	2015/09/24 22:09

			USOCR			
S13	20	cryptogram same (mobile with point)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:10
S14	6	S1 and calculat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:19
S15	123874	(cryptogram or authenticat$5) calculatS3	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:23
S16	20011	(cryptogram or authenticat$5) same calculat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:24
S17	11595	(cryptogram or authenticat$5) with calculat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:24
S18	101	(cryptogram or authenticat$5) with calculat$3 and (permanent near4 key)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:25
S19	96	(cryptogram or authenticat$5) with calculat$3 and (permanent near3 key)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:25
S20	1	(cryptogram or authenticat$5) with calculat$3 and (remote with permanent near3 key)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:26
S21	1	(cryptogram or authenticat$5) with calculat$3 and (remote same (permanent near3 key))	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:27
S22	56	(remote same (permanent near3 key))	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:27
S23	56	(remote same (permanent near3 key))	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:28
S24	5	"pos command" and "unpredictable"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 13:26
S25	458	"unpredictable data"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 13:27
S26	0	"unpredictable data" and crytogra,	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 13:27
S27	0	"unpredictable data" and crytogram	US-	AND	OFF	2015/09/28

			PGPUB; USPAT; USOCR			13:27
S28	7	"unpredictable data" and cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 13:27
S29	29	$2expected with cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 13:29
S30	72	ISO7816-4	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 13:58
S31	4	ISO7816-4 and POS	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 14:01
S32	20	("2008/0040285").URPN.	USPAT	AND	OFF	2015/09/28 20:08
S33	143	transaction adj PIN	USPAT	AND	OFF	2015/09/28 20:12
S34	18	transaction adj PIN with amount	USPAT	AND	OFF	2015/09/28 20:12
S35	51	transaction adj PIN with amount	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:12
S36	84	"pos command"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:14
S37	0	S35 and S36	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:14
S38	0	S35 and S36	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:14
S39	18	S35 and S34	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:14
S40	0	transaction adj PIN with amount and "unpredictable data"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:15
S41	0	(transaction adj PIN with amount) and "unpredictable data"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:16
S42	0	(transaction adj PIN with amount) and "unpredictable"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:16
S43	20	("20040118914" | "20070266131" |	US-	AND	OFF	2015/09/28

		"20070278291" | "20110140841" | "20060022033" | "20090124234" | "20100185545" | "20100274726" | "6199762" | "7774231" | "20100207742" | "20080046367" | "20070075133" | "20090006262" | "20110112918" | "20060224470" | "20030163708" | "20080238610" | "20090044012" | "20080219444").PN.	PGPUB; USPAT; USOCR			20:44
S44	0	S34 and S43	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:44
S45	4	S43 and cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:44
S46	20	("20040118914" | "20070266131" | "20070278291" | "20110140841" | "20060022033" | "20090124234" | "20100185545" | "20100274726" | "6199762" | "7774231" | "20100207742" | "20080046367" | "20070075133" | "20090006262" | "20110112918" | "20060224470" | "20030163708" | "20080238610" | "20090044012" | "20080219444").PN.	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/29 11:08
S47	84	"pos command"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/29 11:08
S48	600	cryptogram same value	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/29 11:08
S49	33585	key with cryptographic	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:02
S50	7656	key with cryptographic with device	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:02
S51	183	(key adj cryptographic) same (device with stor$4) and "transaction"	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:14
S52	18	(key adj cryptographic) same (mobile with device with stor$4) and "transaction"	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:15
S53	88	(key adj cryptographic) same (mobile with device with stor$4) and authori$5	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:17
S54	0	(key adj cryptographic adj local) same (mobile with device with stor$4) and authori$5	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:19
S55	0	(key adj cryptographic adj local) same	US-	AND	OFF	2016/06/06

		(mobile with device with stor$4)	PGPUB; USPAT; USOCR			17:19
S56	0	(key adj cryptographic adj local) same (mobile with device)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:19
S57	571	key with cryptographic with local	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:25
S58	2	key with cryptographic with local with replac$5	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:25
S59	9	key with cryptographic with local same replac$5	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:39
S60	9	(key with cryptographic with local) same replac$5	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:39
S61	20	(key with cryptographic with (local or internal)) same replac$5	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:40
S62	1	"20100185545"	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 20:18
S63	8	("20020026414" | "20070156436" | "20090075592" | "20090143104" | "20090210308" | "20100153721" | "20110099079" | "20120317628").PN.	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/08 18:07
S64	14	(US-20100317318-$ or US-20070254712-$ or US-20050190769-$ or US-20080040285-$ or US-20120109764-$ or US-20140188738-$ or US-20100185545-$ or US-20070156436-$ or US-20110099079-$).did. or (US-5636280-$ or US-3842629-$ or US-5196840-$ or US-7890997-$ or US-8996869-$).did.	US-PGPUB; USPAT	AND	OFF	2016/06/09 14:43
S65	0	S64 and rekey	US-PGPUB; USPAT	AND	OFF	2016/06/09 14:43
S66	5	S64 and re -key	US-PGPUB; USPAT	AND	OFF	2016/06/09 14:43
S67	0	S64 and re-key	US-PGPUB; USPAT	AND	OFF	2016/06/09 14:43
S68	21	(mobile adj device) same cryptogram same POS	US-PGPUB; USPAT	AND	OFF	2016/06/09 14:45
S69	21	(mobile adj device) same cryptogram same POS	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:45

S70	0	rekey with cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:47
S71	97	(rekey$3 or updat$3) with cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:48
S72	1	(rekey$3 or updat$3) with cryptogram same (dynamic or temporary or non-permanent)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:51
S73	51	(rekey$3 or updat$3) with cryptogram and (mobile with device)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:51
S74	51	((rekey$3 or updat$3) with cryptogram) and (mobile with device)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:52
S75	2	((rekey$3 or updat$3) with cryptogram) same (mobile with device)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:52
S76	11	((rekey$3 or updat$3) with cryptogram) and ((mobile with device) same key)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:54
S77	2363	((mobile with device) same key same (rekey$3 or updat$3))	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:56
S78	18	((mobile with device) same key same (rekey$3 or updat$3)) and cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:56
S79	6	((mobile with device) same key same (rekey$3 or updat$3)) same cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:57
S80	0	((mobile with device) same (key with (rekey$3 or updat$3))) same cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:58
S81	7	((mobile with device) same (key with (rekey$3 or updat$3))) and cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:58
S82	4	S64 and updat$3	US-PGPUB; USPAT	AND	OFF	2016/06/09 15:09
S83	49711	((mobile with device) same (cryptographic with rekey$3 or updat$3))	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 15:11
S84	28348	((mobile with device) with (cryptographic with rekey$3 or updat$3))	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 15:12

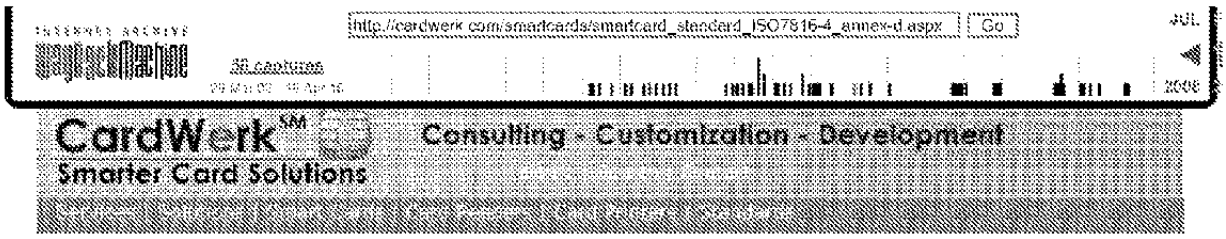
S85	15	cryptogram with key with updat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 15:39
S86	1	(cryptogram with key with updat$3) same card	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 15:39
S87	4439	encryption with key with updat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 15:42
S88	2445	(encryption adj key) with updat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 15:42
S89	90	(card with (encryption adj key)) with updat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 15:42
S90	0	(card with (local near3 (encryption adj key))) with updat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 15:45
S91	15	((local or stored) with card with (encryption adj key)) with updat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 15:45
S92	33	"BER-TLV"	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 16:25
S93	15	(US-20100317318-$ or US-20070254712-$ or US-20050190769-$ or US-20080040285-$ or US-20120109764-$ or US-20140188738-$ or US-20100185545-$ or US-20070156436-$ or US-20110099079-$).did. or (US-5636280-$ or US-3842629-S or US-5196840-$ or US-7890997-$ or US-8996869-$ or US-5737423-$).did.	US-PGPUB; USPAT	AND	OFF	2016/06/09 16:41
S94	3	S93 and hash	US-PGPUB; USPAT	AND	OFF	2016/06/09 16:41
S95	199	(offline with transaction) same encryption	US-PGPUB; USPAT	AND	OFF	2016/06/09 18:04
S96	96	(offline with transaction) same (encryption with key)	US-PGPUB; USPAT	AND	OFF	2016/06/09 18:04
S97	0	(offline with transaction) same (encryption with key) same cryptogram	US-PGPUB; USPAT	AND	OFF	2016/06/09 18:04
S98	0	(offline with transaction) same (encryption with key) same hash	US-PGPUB; USPAT	AND	OFF	2016/06/09 18:04
S99	0	(offline with transaction) same (encryption with key) and (cryptogram)	US-PGPUB; USPAT	AND	OFF	2016/06/09 18:05

S100	6	(offline with transaction) same (encryption with key) and (hash)	US-PGPUB; USPAT	AND	OFF	2016/06/09 18:05
S101	6	(offline with transaction) same (encryption with key) and (hash)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 18:05
S102	2	(offline with transaction) same (encryption with key) and ((hash) same response)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 18:05
S103	2593	(encryption with key) and (hash with response)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 18:17
S104	357	(encryption with key) same (hash with response)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 18:19
S105	76	(encryption with key) same (hash with response) and transactions	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 18:19
S106	20	(encryption with key) same (hash with response) and (offline with transactions)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 18:27
S107	0	("l30andoffline").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2016/06/09 19:42
S108	44	"l30" and offline	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 19:42
S109	44	"l30" and offline	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 19:42
S110	43	"l30" and offline	US-PGPUB; USPAT	AND	OFF	2016/06/09 19:43
S111	15	(US-20100317318-$ or US-20070254712-$ or US-20050190769-$ or US-20080040285-$ or US-20120109764-$ or US-20140188738-$ or US-20100185545-$ or US-20070156436-$ or US-20110099079-$).did. or (US-5636280-$ or US-3842629-S or US-5196840-$ or US-7890997-$ or US-8996869-$ or US-5737423-$).did.	US-PGPUB; USPAT	AND	OFF	2016/06/09 19:43
S112	1	S111 and offline	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 19:43
S113	15	(US-20100317318-$ or US-20070254712-$ or US-20050190769-$ or US-20080040285-$ or US-20120109764-$ or US-20140188738-$ or US-20100185545-$ or US-20070156436-$ or US-20110099079-	US-PGPUB; USPAT	AND	OFF	2016/06/10 15:35

		$).did. or (US-5636280-$ or US-3842629-S or US-5196840-$ or US-7890997-$ or US-8996869-$ or US-5737423-$).did.				
S114	0	S113 and "TLV"	US-PGPUB; USPAT	AND	OFF	2016/06/10 15:35
S115	8137	"TLV"	US-PGPUB; USPAT	AND	OFF	2016/06/10 15:35

6/ 10/ 2016 5:08:21 PM
C:\ Users\ aputtaiah1\ Documents\ EAST\ Workspaces\ 13599647.wsp

Mastercard, Ex1002, p. 600



ISO 7816-4: Interindustry Commands for Interchange
Annex D: Use of Basic Encoding Rules ASN.1

ISO 7816 [part 1] [part 2] [part 3] [part4] [section..1 2 3 4 5 6 7 8 9 annex.. A B C D E F]

Annex D: Use of Basic Encoding Rules ASN.1

- Annex D.1 BER-TLV data object
- Annex D.2 Tag field
- Annex D.3 Length field
- Annex D.4 Value field

ISO 7816 Annex D.1: BER-TLV data object

Each BER-TLV data object (see ISO/IEC 8825) shall consist of 2 or 3 consecutive fields :

- The tag field T consists of one or more consecutive bytes. It encodes a class, a type and a number.
- The length field consists of one or more consecutive bytes. It encodes an integer L.
- If L is not null, then the value field V consists of L consecutive bytes. If L is null, then the data object is empty: there is no value field.

ISO/IEC 7816 uses neither '00' nor 'FF' as tag value.

NOTE - Before, between or after BER-TLV data objects, '00' or 'FF' bytes without any meaning may occur (e.g. due to erased or modified TLV-coded data objects).

ISO 7816-4 Annex D.2: Tag field

The bits B8 and B7 of the leading byte of tag field shall encode the tag class, i.e. the class of the data object.

- B8-7='00' introduces a tag of universal class
- B8-7='01' introduces a tag of application class
- B8-7='10' introduces a tag of context-specific clas
- B8-7='11' introduces a tag of private class

The bit B6 of the leading byte of the tag field shall encode the tag type, i.e. the type of the data object.

- B6–0 introduces a primitive data object
- B6–1 introduces a constructed data object

If the bits B5-B1 of the leading byte are not all set to 1, then may they shall encode an integer equal to the tag number which therefore lies in the range from 0 to 30. Then the tag field consists of a single byte.

Otherwise (B5-B1 set to 1 in the leading byte), the tag field shall continue on one or more subsequent bytes.

- The bit B8 of each subsequent byte shall be set to 1, unless it is the last subsequent byte
- The bits B7-B1 of the first subsequent byte shall not be all set to 0
- The bits B7-B1 of the first subsequent byte, folowed by the bits B7 to B1 of each further subsequent byte, up to and including the bits B7-B1 of the last subsequent byte, shall encode an integer equal to the tag number (thus strictly positive).

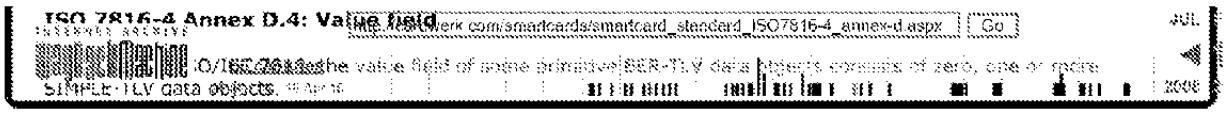
ISO 7816-4 Annex D.3: Length field

In short form, the length field consists of a single byte where the bit B8 shall be set to 0 and the bits B7-B1 shall encode an integer equal to the number of bytes in the value field. Any length from 0-127 can thus be encoded by 1 byte.

In long form, the length field consists of a leading byte where the bit B8 shall be set to 1 and the B7-B1 shall not be all equal, thus encoding a positive integer equal to the number of subsequent bytes in the length field. Those subsequent bytes shall encode an integer equal to the number of bytes in the value field. Any length within the APDU limit (up to 65535) can thus be encoded by 3 bytes.

NOTE - ISO/IEC 7816 does not use the indefinite lengths specified by the basic encoding rules of ASN.1 (see ISO/IEC 8825).

Mastercard, Ex1002, p. 601



ISO/IEC 7816 defines the value field of every primitive BER-TLV data object consists of zero, one or more SIMPLE-TLV data objects.

The value field of any other primitive BER-TLV data object consists of zero, one or more data elements fixed by the specifications of the data objects.

The value field of each constructed BER-TLV data object consists of zero, one or more BER-TLV data objects.

Smart Card Software Engineering Services
HOME | CONTACT | RESOURCES | SITE MAP
SMART CARDS | SMART CARD READERS | SMART CARD PRINTERS | TOOLS
Solutions: Loyalty Cards | Logical Access Control | Physical Access Control | Smart Card Personalization

© Copyright 1999-2008 Incoded Computing, Inc.
All rights reserved. Legal disclaimer Last modified September 21, 2008

Mastercard, Ex1002, p. 602

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13599647	YEAGER, C. DOUGLAS
	Examiner	Art Unit
	ASHA PUTTAIAH	3695

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	09/29/2015	06/10/2016							
	1	✓	-							
	2	✓	-							
	3	✓	-							
	4	✓	-							
	5	✓	-							
	6	✓	-							
	7	✓	-							
	8	✓	-							
	9	✓	-							
	10	✓	-							
	11	✓	-							
	12	✓	-							
	13	✓	-							
	14	✓	-							
	15	✓	-							
	16	✓	-							
	17	✓	-							
	18	✓	-							
	19	✓	-							
	20	✓	-							
	21	✓	-							
	22	✓	-							
	23	✓	-							
	24	✓	-							
	25	✓	-							
	26	✓	-							
	27	✓	-							
	28	✓	-							
	29		-							
	30		✓							
	31		✓							
	32		✓							
	33		✓							
	34		✓							
	35		✓							
	36		✓							

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13599647	YEAGER, C. DOUGLAS
	Examiner	Art Unit
	ASHA PUTTAIAH	3695

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	09/29/2015	06/10/2016							
	37		✓							
	38		✓							
	39		✓							
	40		✓							
	41		✓							
	42		✓							
	43		✓							
	44		✓							
	45		✓							
	46		✓							
	47		✓							
	48		✓							
	49		✓							
	50		✓							
	51		✓							
	52		✓							
	53		✓							
	54		✓							
	55		✓							
	56		✓							
	57		✓							
	58		✓							

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (07-14)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	13/599,647	Filing Date	2012-08-30	Docket Number (if applicable)	STAPP1100-5	Art Unit	3695
First Named Inventor	C. Douglas Yeager			Examiner Name	Puttaiah, Asha		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, to any international application that does not comply with the requirements of 35 U.S.C. 371, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV.

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

☐ Other _____

☒ Enclosed

☒ Amendment/Reply

☒ Information Disclosure Statement (IDS)

☐ Affidavit(s)/ Declaration(s)

☒ Other Notification of Extension of Time

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____ (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

☒ The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 503183

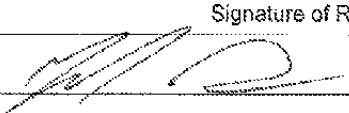
SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

PTO/SB/30EFS (07-14)
Approved for use through 07/31/2016, OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature		Date (YYYY-MM-DD)	2016-12-14
Name	John L. Adair	Registration Number	48828

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
REPLY TO OFFICE ACTION DATED 06/14/2016	Atty. Docket No. **STAPP1100-5**

First Named Inventor **C. Douglas Yeager**	
Application Number **13/599,647**	Date Filed **August 30, 2012**
Title **SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE (As Amended)**	
Group Art Unit **3695**	Examiner **Puttaiah, Asha**
Confirmation Number: **1919**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Certificate of Transmission Under 37 C.F.R. § 1.8

I hereby certify that this correspondence is being deposited electronically with the U.S. Patent and Trademark Office using the United States Patent and Trademark Office's EFS-Web system on **December 14, 2016.**

Shenise Ramdeen

This paper is submitted in response to the Official Action mailed on June 14, 2016. Please reconsider the above-identified application in view of the following amendments and remarks.

A Claim Listing begins on page 2 of this paper.

Remarks/Arguments begin on page 9 of this paper.

CLAIM LISTING:

1-29. Cancelled.

30. (Previously Presented) A method for secure application-based participation in a payment card transaction authorization process by a mobile device, the method comprising:

receiving over a wireless network at a mobile device a first non-permanent cryptographic key associated with an account having a corresponding digital credential, wherein the mobile device comprises an operating system and an application executable in the operating system, the application interrogable for digital credential data corresponding to the account, wherein the application does not access a permanent cryptographic key associated with the account during interrogations;

locally storing a first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;

participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device comprising:

receiving at least one POS command communication sent by the POS terminal over a communications channel, wherein the at least one POS command communication comprises a request for digital credential data to authorize a transaction against the account;

generating a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram; and

responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to an electronic reader through the communication channel, the at least one device response communication comprising at least a portion of the digital credential data, wherein the at least a portion of the digital credential data comprises the response cryptogram and an account identifier for the account;

receiving a second non-permanent cryptographic key at the mobile device, wherein the second non-permanent cryptographic key is associated with the account; and

replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key as the local cryptographic key associated with the account prior to the application participating in a subsequent interrogation.

31. (Previously Presented) The method of Claim 30, wherein the mobile device is an NFC emulating device.

32. (Previously Presented) The method of Claim 30, wherein the response cryptogram is a hash.

33. (Previously Presented) The method of Claim 30, wherein the interrogation conforms to a card specification, the set of inputs is specified by the card specification and the at least one device response is formulated according to the card specification.

34. (Previously Presented) The method of Claim 33, wherein the request for digital credential data comprises a request for a first cryptogram according to the card specification and the at least one device response communication comprises a second cryptogram, wherein the second cryptogram is the response cryptogram.

35. (Currently Amended) The method of Claim 30, wherein generating the response cryptogram comprises encrypting the set of inputs using the local cryptographic key according to a digital encryption standard (DES) calculation to generate an output, wherein the ~~reponse~~ response cryptogram includes a portion, but not all, of the output.

36. (Previously Presented) The method of Claim 30, wherein the mobile device does not have connectivity to the wireless network during the interrogation.

37. (Previously Presented) The method of Claim 30, further comprising, at a remote system:

prior to the interrogation, generating at a remote system the first non-permanent cryptographic key, associating the first non-permanent cryptographic key with the account, and sending the first non-permanent cryptographic key and the account identifier to the mobile device over the wireless network; and

after the interrogation generating at the remote system, the second non-permanent cryptographic key, associating the second non-permanent cryptographic key with the account and sending the second non-permanent cryptographic key and the account identifier to the mobile device over the wireless network.

38. (Previously Presented) The method of Claim 37, wherein the digital credential comprises a secure element representation maintained at the remote system.

39. (Previously Presented) The method of Claim 30, further comprising, at a remote system performing an authorization process comprising:

receiving an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the response cryptogram and the account identifier;

determining a current non-permanent cryptographic key associated with the account using the account identifier;

calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account;

verifying a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram; and

sending an authorization response to the POS terminal, wherein the data contained in the authorization response is determined, at least in part, by the verifying the correctness of the response cryptogram.

40. (Previously Presented) The method of Claim 39, wherein:

the set of inputs comprises unpredictable data;

the authorization data comprises the unpredictable data; and

the calculated cryptogram is calculated using the unpredictable data.

41. (Previously Presented) The method of Claim 40, wherein the POS command communications comprise the unpredictable data.

42. (Previously Presented) The method of Claim 41, wherein the authorization data further comprises values from the transaction and wherein the POS terminal communicates the

values from the transaction, the response cryptogram and the account identifier to the remote system in track 2 format.

43. (Previously Presented) The method of Claim 41, wherein the authorization data further comprises values from the transaction and wherein the POS terminal communicates values from the transaction, the response cryptogram and the account identifier in BER-TLV format.

44. (Previously Presented) A system for secure application-based participation by a mobile device in point-of-sale interrogations, the system comprising:

a mobile device comprising:

a controller configured to route communications received over a communication channel from an electronic reader;

a wireless interface to connect to a wireless network;

a processor;

a computer readable storage medium accessible by the processor storing an application interrogable for digital credential data to authorize transactions against an account having a digital credential, the application executable in an operating system of the mobile device to participate in interrogations, wherein the application is executable to:

during an interrogation:

receive at least one point-of-sale (POS) command communication sent by a POS terminal to the mobile device over the communications channel, wherein the at least one POS command communication comprises a request for digital credential data;

access a locally stored cryptographic key associated with the account, wherein the mobile device does not have access to a permanent cryptographic key associated with the account and the locally stored cryptographic key associated with the account is a non-permanent cryptographic key that does not last a life of a digital credential for an account;

generate a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key

associated with the account used to generate the response cryptogram; and

respond to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response to the electronic reader through the communication channel, the at least one device response communication comprising at least a portion of the digital credential data, wherein the at least a portion of the digital credential data comprises the response cryptogram and an account identifier for the account;

receive non-permanent cryptographic keys associated with the account transmitted to the mobile device over the wireless network by a remote source; and

store the received non-permanent cryptographic keys as the locally stored cryptographic key associated with the account to change the locally stored cryptographic key associated with the account between at least two interrogations.

45. (Previously Presented) The system of Claim 44, wherein the mobile device is an NFC emulating device.

46. (Previously Presented) The system of Claim 44, wherein the response cryptogram is a hash.

47. (Previously Presented) The system of Claim 44, wherein the interrogations conform to a card specification, the set of inputs is specified by the card specification and the at least one device response is formulated according to the card specification.

48. (Previously Presented) The system of Claim 47, wherein the request for digital credential data requests digital credential data comprising a first cryptogram and the at least one device response communication comprises a second cryptogram, wherein the second cryptogram is the response cryptogram.

49. (Previously Presented) The system of Claim 44, wherein generating the response cryptogram comprises encrypting the set of inputs using the local cryptographic key according to a digital encryption standard (DES) calculation to generate an output, wherein the response cryptogram includes a portion, but not all, of the output.

50. (Previously Presented) The system of Claim 44, wherein the mobile device does not have connectivity to the wireless network during the interrogation.

51. (Previously Presented) The system of Claim 44, wherein the mobile device is programmed to request a new non-permanent cryptographic key after the interrogation.

52. (Previously Presented) The system of Claim 44, further comprising a remote computer system configured to generate the non-permanent cryptographic keys associated with the account and send each of the non-permanent cryptographic keys and the account identifier to the mobile device over the wireless network.

53. (Previously Presented) The system of Claim 52, wherein the remote computer system is configured to maintain a secure element representation for the account, wherein the digital credential comprises the secure element representation.

54. (Previously Presented) The system of Claim 44, further comprising, a remote computer system programmed to:

receive an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the response cryptogram and the account identifier;

determine a current non-permanent cryptographic key associated with the account using the account identifier;

calculate a calculated cryptogram using the current non-permanent cryptographic key associated with the account;

verify a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram; and

send an authorization response to the POS terminal, wherein the data contained in the authorization response is determined, at least in part, by the verifying the correctness of the response cryptogram.

55. (Previously Presented) The system of Claim 54, wherein:
the set of inputs comprises unpredictable data;
the authorization data comprises the unpredictable data; and
the calculated cryptogram is calculated using the unpredictable data.

56. (Previously Presented) The system of Claim 55, wherein the POS command communications comprise the unpredictable data.

57. (Previously Presented) The system of Claim 55, wherein the authorization data further comprises values from the transaction and wherein the POS terminal communicates the values from the transaction, the response cryptogram and the account identifier to the remote system in track 2 format.

58. (Previously Presented) The system of Claim 55, wherein the authorization data further comprises values from the transaction and wherein the POS terminal communicates the values from the transaction, the response cryptogram and the account identifier to the remote system in BER-TLV format.

REMARKS

Applicant appreciates the time taken by the Examiner to review Applicant's present application. Applicant respectfully requests reconsideration and favorable action in this case.

Rejections under 35 U.S.C. § 112

Claims 36, 42, 43, 50, 57 and 58 stand rejected under 35 U.S.C. § 112, second paragraph. Applicant traverses these rejections.

Claims 36 and 50

With respect to Claims 36 and 50, the Office Action states that "[i]t is unclear what is meant by ['wherein the mobile device does not have connectivity to the wireless network during the interrogation . . .'] as the 'mobile device' must be 'connected to the wireless' system in order to transmit data to the POS during the interrogation." Using Claim 36 as the example, Claim 30 from which Claim 36 depends, recites "a wireless network" and "a communications channel." The mobile device communicates with the POS over the "communications channel" (e.g., NFC) and may also, for example, connect to remote systems via a wireless network (e.g., such as a cellular data network). However, unlike some other solutions, the mobile device of Claim 36 does not require data network access to a remote repository and SE during interrogation and can be disconnected from the wireless network while still participating in the interrogation over the "communications channel." Applicant submits that Claims 36 and 50 are clear and respectfully requests withdrawal of the rejection.

Claims 42, 43, 57, 58

The Examiner objects to Claims 42, 57, 43 and 58 as being indefinite for specifying "an industry standard [which] can change upon updates." Office Action at 5-6. The Patent Trial and Appeal Board ("PTAB" or "Board"), however, has found such rejections insufficient. In *Ex Parte Honeck*, for example, the examiner rejected the claims as being indefinite for referring to "International Organization for Standardization documents that are continuously updated." *See Ex Parte Honeck*, Appeal 2011-010512, *Decision* on Appeal at 9 (PTAB Sept. 27, 2013). The Board reversed the rejection because *inter alia* the examiner did not "establish that a person of ordinary skill in the art, aware of the filing date of the application, and thus, the standard in place at the time, would be uncertain of the meaning of these terms." *Id.* As such, Applicant requests that the similar rejections in the present matter be withdrawn.

Rejections under 35 U.S.C. § 101

Claims **30-58** stand rejected under 35 U.S.C. § 101. Subsequent to the issuance of the present rejection, the Court of Appeals for the Federal Circuit ("Fed. Cir.") entered several precedential opinions on subject matter eligibility under 35 U.S.C. § 101 and the Office issued an updated memorandum, "Recent Subject Matter Eligibility Decisions" (the Nov. 2 Memorandum), further clarifying the subject matter eligibility framework. Applicant respectfully submits that, in light of these decisions and further guidelines, the present rejection should be withdrawn.

As stated in the Nov. 2 Memorandum, "an examiner should consider in Step 2A of the eligibility analysis whether the claim is directed to an improvement in computer related technology or a specific way of achieving a desired outcome or end result." *Id.* at 4. An indication that a claim is directed to an improvement in computer related technology may include "a teaching in the specification about how the claimed invention improves a computer or other technology." *Id.* at 2. The "improvement to computer-related technology" is not limited to "improvements in the operation of a computer or computer network *per se*." *Id.* at 2.

The Specification clearly shows that the present application improves mobile device payment technology. As described in the Specification, conventional secure element payment systems require that the user have physical possession of a "card" (e.g., card or mobile device with a secure element microchip) that matches the authorization capabilities of a merchant's system where a purchase is made. *See, Application* at ¶ 5. In a typical interrogation, a POS terminal sends at least one command communication to a secure element requesting a cryptogram and the SE generates a responsive cryptogram using a permanent cryptographic key for the SE. *See, id.* at ¶ 165.

Many mobile devices, however, do not have a secure element microchip for electronic payment or, if they do, the secure element microchip may be limited to a single or limited number of card specifications and accounts. Mobile device applications, however, may not be secure. *See, id.* at ¶ 194. One solution to this problem, as described in the Specification, is to use remotely hosted secure elements in which the secure element resides at a remote server and the mobile application contacts the secure element during an integration. *See, id.* at ¶ 160. However, this leads to another problem. "Many payment applications that communicate with an SE may require a plurality of commands and responses to the SE for each transaction." *See, id.* at ¶ 83. When the SE is a remote SE, "[e]ach or some of these command and responses to the SE may be subject to network delays and latency." *See, id.* See also, *id.* at ¶ 84 ("The remote SE took ~400ms longer in the above example due to network latency and delay during the SE interrogation.")

Claim 30 addresses the problem of allowing an application running in the operating system of a mobile device to securely participate in interrogations with a POS terminal for digital credential data while retaining low latency. According to Claim 30, "the [interrogable] application [executable in the operating system of the mobile device] does not access a permanent cryptographic key associated with the account during interrogations." Instead, as shown be the emphasized portions of Claim 30 below, the application generates response cryptograms during interrogations based on a non-permanent key that changes between at least two interrogations.

30. A method for secure application-based participation in a payment card transaction authorization process by a mobile device, the method comprising:

receiving over a wireless network at a mobile device a first non-permanent cryptographic key associated with an account having a corresponding digital credential, wherein the mobile device comprises an operating system and an application executable in the operating system, the application interrogable for digital credential data corresponding to the account, wherein the application does not access a permanent cryptographic key associated with the account during interrogations;

locally storing a first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;

participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device comprising:

receiving at least one POS command communication sent by the POS terminal over a communications channel, wherein the at least one POS command communication comprises a request for digital credential data to authorize a transaction against the account;

generating a response cryptogram based on a set of inputs and **the local cryptographic key associated with the account**, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram; and

responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to the electronic reader through the communication channel, the at least one device response communication comprising at least a portion of the digital credential data, wherein the at least a portion of the digital credential data comprises the response cryptogram and an account identifier for the account;

receiving a second non-permanent cryptographic key at the mobile device, wherein the second non-permanent cryptographic key is associated with the account; and

replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key as the local cryptographic key associated with the account prior to the application participating in a subsequent interrogation.

Claim 30 thus claims a solution that helps address security issues that arise from using an interrogable application executable in the operating system of the mobile device to respond to interrogations at least because the key used to generate response cryptograms changes, limiting the key's usefulness if stolen by other code running in the operating system of the mobile device.

Moreover, Claim 30 provides this security while reducing latency and network delays experienced by other solutions. In particular, cryptogram generation is done at the mobile device reducing/eliminating the commands/requests that the mobile device sends between a POS and remote secure element. For example, the Specification describes that:

> Also, sharing a temporary cryptographic key with the mobile device wherein the mobile device calculates an unpredictable cryptogram would be an alternative using a predetermined cryptogram to achieve a similar system performance result with the context of 100% transaction caching.

Application at ¶ 152.

The present claims are thus clearly drawn to addressing security and latency/network delay issues computer-related mobile device payment technology and are patent eligible under Step 2A.

Furthermore, "an indication that a claim is directed to an improvement in computer-related technology may include (2) a particular solution or a particular way to achieve a desired outcome defined by the claimed invention, as opposed to merely claiming the idea of a solution or outcome." Nov. 2 Memorandum at 2. Here, Claim 30 includes a specific series of steps that achieve the desired security while reducing latency and network delays. Thus, both indicators of subject matter eligibility set forth in the Nov. 2 Memorandum indicate the claims are not abstract but are, instead, directed to patent eligible subject matter.

In addition, under Step 2B "the examiner should consider the additional elements in combination, as well as individually." Nov. 2 Memorandum at 2. In *Bascom Global Internet Services v. AT&T Mobility LLC* 827 F.3d 1341, for example, the Federal Circuit agreed with the district court that the additional claim elements were generic computer, network, and Internet components that did not amount to significantly more when considered individually, but explained that the district court erred by failing to recognized that when combined, an inventive concept may be found in the non-conventional and non-generic arrangement of additional elements. Nov. 2 Memorandum at 3.

The *Bascom* court recognized that "prior art filters were either susceptible to hacking and dependent on local hardware and software or confined to an inflexible one-size-fits all-scheme." However, the court found that "[b]y taking a prior art filter solution . . . and making it more

dynamic and efficient . . . the claimed invention represents a 'software-based invention[] that improve[s] the performance of the computer system itself." *Bascom*, 827 F.3d at 1350-51. Here, the present application recognizes that there is a lack of flexibility or security at mobile devices but that remote hosted SEs can introduce latency and network delays, particularly if the payment application "require(s) a plurality of commands and responses to the SE for each transaction." Claim 30 provides a specific solution that improves the computer system itself by providing security while making the system more efficient. Like the claims at issue in *Bascom*, Claim 30 provides a technical solution to a technical problem and should be patent-eligible under Step 2B.

Applicant further submits that Claim 44 recites patent-eligible subject matter under Steps 2A and 2B.

Rejections under 35 U.S.C. § 103

Claims 30, 31, 33, 34, 35, 37, 38, 39, 40, 41, 42, 44, 45, 47, 48, 49, 51, 52, 53, 54, 55, 56 and 57 stand rejected as obvious over U.S. Patent Publication No. 2010/0185545 ("Royyuru") in view of U.S. Patent No. 5,737,423 ("Manduley").

The Examiner cites "Royyuru, pg. 9, Table, Card-Key, CK, random CK can be system generated" as allegedly showing "locally storing a first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account." Office Action at page 13. According Royyuru, the "Card Key" is system generated "when an institution requests that a card be added to the service." Royyuru, pg. 9, Table. The Card Key is a conventional permanent cryptographic key that is issued when a card is initially added to a system.

The Office Action goes on to assert that Manduley teaches "receiving a second non-permanent cryptographic key at the mobile device, wherein the second non-permanent cryptographic key is associated with the account . . . and replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key as the local cryptographic key associated with the account prior to the application participating in a subsequent interrogation." Office Action at 15-16, citing Manduley at 2:29-41.

Applicant respectfully submits that the reliance on Manduley is misplaced. Manduley teaches a smart card that "[w]hen connected to an appropriate card reader . . . can be used for secure information exchange transactions. In particular, it has frequently been suggested that a smart card can be used as an 'electronic purse'." Manduely at 1:17-18. Manduley explicitly does not change the underlying information transactions, stating "information transaction between smart cards and external devices are well known, and indeed are the reason such cards exist, and details of particular type of transactions **form no part per se of the subject invention**." *Id.*

would not change the underlying payment transaction process, which in Royyuru, uses a permanent Card Key to generate a DTC cryptogram.

Instead, Manduley provides a mechanism that is completely tangential to the information exchange transaction between a smart card and a card reader. The mechanism of Manduley allows an issuing authority to remotely inspect a card to ensure, for example, that the card is still in the possession of the card owner. *Id.* at 1:52-56.

As described in Manduely:

> At 50 the issuing authority transmits a Response Request addressed to card 10, and at 52 tests to determine if a response has been received. The response may be returned in any convenient manner, but preferably will be transmitted over the telephone network by means of tone signals in a conventional manner by a person in possession of card 10 . . .
>
> If the response is valid, then at 60 a Response Confirmation message is sent to card 10, completing the inspection. Preferably, the Response Confirmation message will update an encryption key used to encrypt the response so that each encrypted response received will differ from previous responses, thus assuring that the response is provided by a person actually in possession of the card.

Id. at 4:1-6, 21-27 (emphasis added). As can be seen, the portions of Manduley cited in the Office Action describe updating the encryption key used to encrypt responses to remote card inspections by the issuing authority. Again, however, Manduley does not change anything about the encryption used by the smart card in transactions with card readers.

For at least the foregoing reasons, Applicant submits that Royyuru and Manduley, alone or in combination, do not teach Claim 30. For similar reasons, Applicant respectfully submits that the cited reference fail to teach Claim 44. As such, Applicant respectfully requests withdrawal of the rejection and allowance of the claims.

Conclusion

Applicant has now made an earnest attempt to place this case in condition for allowance. Other than as explicitly set forth above, this reply does not include an acquiescence to statements, assertions, assumptions, conclusions, or any combination thereof in the Office Action. For the foregoing reasons and for other reasons clearly apparent, Applicant respectfully requests full allowance of Claims 30-58. The Examiner is invited to telephone the undersigned at the number listed below for prompt action in the event any issues remain.

An extension of three (3) months is requested and a Notification of Extension of Time Under 37 C.F.R. § 1.136 with the appropriate fee is enclosed herewith.

The Director of the U.S. Patent and Trademark Office is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

Sprinkle IP Law Group
Attorneys for Applicant

John L. Adair
Reg. No. 48,828

Date: Dec. 14, 2016

1301 W. 25th Street, Suite 408
Austin, TX 78705
Tel. (512) 637-9220
Fax. (512) 371-9088

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. (Opt.) **STAPP1100-5**

First Named Inventor **C. Douglas Yeager**	
Application Number **13/599,647**	Date Filed **August 30, 2012**
Title **SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE (as amended)**	
Group Art Unit **3695**	Examiner **Puttaiah, Asha**
Confirmation Number **1919**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certification of Transmission Under 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on **December 14 2016.**

Shenise Ramdeen

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. A copy of foreign patent documents as well as the information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

☐ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☐ This Information Disclosure Statement is being submitted before the mailing of a first Office action on the merits; or

☒ This Information Disclosure Statement is being submitted before the mailing of a first Office action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

Furthermore, pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application.

Applicant does not believe any fees are due and owing at this time. If Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

SPRINKLE IP LAW GROUP
Attorneys for Applicant

John L. Adair
Reg. No. 48,828

Dated: December 11, 2016

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 317-9088

Substitute Form PTO/SB/08b

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/599,647
				Filing Date	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	Puttaiah, Asha
Sheet	1	of	1	Atty Docket Number	STAPP1100-5

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C4	International Preliminary Report on Patentability for Int'l Application No. PCT/US2012/053129, mailed 12/10/2013, 11 pgs.	

Examiner Signature		Date Considered	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
NOTIFICATION OF EXTENSION OF TIME UNDER 37 C.F.R § 1.136	Atty. Docket No. **STAPP1100-5**

First Named Inventor **C. Douglas Yeager**	
Application Number **13/599,647**	Filed **August 30, 2012**
Title **SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE (As Amended)**	
Group Art Unit **3695**	Examiner **Puttaiah, Asha**
Confirmation No. **1919**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certification Under 37 C.F.R. §1.8

I hereby certify that this document is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22312-1450 on December 14, 2016.

Shenise Ramdeen

Dear Sir:

Applicant hereby takes an Extension of Time for responding to the **Office Action** mailed **June 14, 2016** for a period of **three** (3) month(s).

		Small Entity	*Large Entity*
	First Month	$ 100.00	$ 200.00
	Second Month	$ 300.00	$ 600.00
X	Third Month	$ 700.00	$ 1,400.00
	Fourth Month	$ 1,100.00	$ 2,200.00
	Fifth Month	$ 1,500.00	$ 3,000.00
	TOTAL	**$ 700.00**	

The Commissioner is hereby authorized to deduct the above-noted fee from Deposit Account 50-3183 of Sprinkle IP Law Group. If any fees are inadvertently omitted, additional fees are required, or if any amounts have been overpaid, please appropriately charge or credit those fees to Deposit Account No. 50-3183 of SPRINKLE IP LAW GROUP.

Respectfully submitted,

SPRINKLE IP LAW GROUP

John L. Adair
Reg. No. 48,828

Date: December 14, 2016
1301 W. 25th Street, Suite 408
Austin, Texas 78705
(512) 637.9220 - Telephone
(512) 371.9088 - Facsimile

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 67979.W2	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2012/053129	International filing date *(day/month/year)* 30 August 2012 (30.08.2012)	Priority date *(day/month/year)* 30 August 2011 (30.08.2011)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant YEAGER, C., Douglas		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 11 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 04 March 2014 (04.03.2014)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Nora Lindner e-mail: pt05.pct@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: JAMES PALMER
LUEDEKA NEELY GROUP, P.C.
P.O. BOX 1871
KNOXVILLE, TN 37901-1871

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	16 NOV 2012
Applicant's or agent's file reference 67979.W2	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2012/053129	30 August 2012	30 August 2011

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - G06Q 20/00 (2012.01)
USPC - 705/64

Applicant YEAGER, C.

1. This opinion contains indications relating to the following items:

- [x] Box No. I Basis of the opinion
- [ ] Box No. II Priority
- [ ] Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- [ ] Box No. IV Lack of unity of invention
- [x] Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- [ ] Box No. VI Certain documents cited
- [ ] Box No. VII Certain defects in the international application
- [ ] Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	24 October 2012	Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (July 2011)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	2-29	YES
	Claims	1	NO
Inventive step (IS)	Claims	8-11, 15-16, 19-23, 28-29	YES
	Claims	1-7, 12-14, 17-18, 24-27	NO
Industrial applicability (IA)	Claims	1-29	YES
	Claims	None	NO

2. Citations and explanations:

Claim 1 lacks novelty under PCT Article 33(2) as being anticipated by Yeager (US 2007/0075133 A1).

Regarding claim 1, Yeager discloses a method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction (method, system and computer-readable medium for radio frequency identification device, title; the adapter is connected to a host device like a mobile phone to construct a mobile device capable of financial transactions, Fig. 3 and [0027]-[0029], in which the mobile device communicates with a terminal such as the Mastercard PayPass system, Fig. 5 and [0030]) comprising:
using a remote permanent cryptographic key to calculate an expected cryptogram that is expected to comprise at least a portion of the digital credential data (a secret key on a remote server, Fig. 6 and [0031]-[0032], which is a remote permanent cryptographic key, is used to calculate an expected cryptogram that comprises, and hence encrypts, digital credential data such as credit card information, [0022]), wherein the remote permanent cryptographic key is persistently stored at a remote source that is remote from the mobile device (the secret key is stored in a remote location that is remote from the mobile device/host, Fig. 6 and [0031]-[0032]) and wherein the mobile device does not access a duplicate local permanent cryptographic key persistently stored locally to the mobile device (the mobile device/host also shares the secret key, Fig. 6 and [0031]-[0032], and the mobile device/host does not access the secret key; only the server and the adapter have access to the secret key, because they're the only two entities that know the key, [0031]-[0032]);performing an interrogation between the point-of-sale terminal and the mobile device (the adapter is connected to a host device like a mobile phone to construct a mobile device capable of financial transactions, Fig. 3 and [0027]-[0029], in which the mobile device communicates with a terminal such as the Mastercard PayPass system, Fig. 5 and [0030]) comprising: sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device requesting the digital credential data (the digital credential data is credit card information, [0022], and is requested by the terminal to the mobile device in order to facilitate a transaction, Fig. 9 and [0036]); and
sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal comprising the expected cryptogram as the at least a portion of the digital credential data (credenttial data is sent to a server via the terminal, Fig. 9 and [0036], in which the credential data is encrypted using the encryption key for the purpose of communication between an adapter and server, [0031]-[0032], and hence the encrypted credential data is the expected cryptogram comprising at least a portion of the digital credential data); wherein the financial transaction is authorized (the transaction is determined to be successful or not, hence authorized, and then the user account may then be updated by deducting the transaction amount, Fig. 9 and [0036]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Claim 2 lacks an inventive step under PCT Article 33(3) as being obvious over Yeager (US 2007/0075133 A1) and further in view of Smets et al (US 2006/0022033 A1), hereinafter referred to as Smets.

Regarding claim 2 of claim 1, Yeager further discloses a further step that precedes the performing the interrogation step, the further step comprising:
sending the remote permanent cryptographic key to the mobile device from the remote source (the secret key is chosen by the server sent from a server to the mobile host, [0031]-[0032]); and transiently caching the remote permanent cryptographic key in the mobile device as a cached transient permanent cryptographic key (the server may change the secret key after each transaction, [0031]-[0032], and hence the secret key is actually a temporary session key or cached transient permanent cryptographic key, [0031]-[0032]), sending the expected cryptogram calculated, at least in part, from the cached transient cryptographic key (communications is encrypted with the session key, and hence results in an expected cryptogram, [0031]-[0032]).
Yeager does not adequately disclose:
the step of sending through the communication channel the at least one POS command communication comprises sending unpredictable data; the step of sending through the communication channel the at least one POS command communication comprises sending a request for an expected cryptogram that is expected to be calculated by the mobile device, at least in part, from the unpredictable data; and the step of sending through the communication channel the at least one device response communication from the mobile device to the point-of-sale terminal comprises sending the expected cryptogram calculated, at least in part, from the unpredictable data. However, Smets is also in the field of electronic payment systems (abstract) and further teaches:
the step of sending through the communication channel the at least one POS command communication comprises sending unpredictable data (an unpredicatable number UN, which is unpredictable data, is sent from the POS terminal, Fig. 5 and [0026]); the step of sending through the communication channel the at least one POS command communication comprises sending a request for an expected cryptogram that is expected to be calculated by the mobile device, at least in part, from the unpredictable data (using the unpredictable number, a mobile device, such as the card, calculates a CVC3 number based on a portion of the unpredictable number and transmits the result to the terminal, Fig. 5 and [0026]); and the step of sending through the communication channel the at least one device response communication from the mobile device to the point-of-sale terminal comprises sending the expected cryptogram calculated, at least in part, from the unpredictable data (the resulting cryptogram CVC3 is calculated in part from the unpredictable number and transmitted to the terminal, Fig. 5 and [0026]). Therefore, it would have been obvious to a person having ordinary skill in the art wherein: the step of sending through the communication channel the at least one POS command communication comprises sending unpredictable data; the step of sending through the communication channel the at least one POS command communication comprises sending a request for an expected cryptogram that is expected to be calculated by the mobile device, at least in part, from the unpredictable data; and the step of sending through the communication channel the at least one device response communication from the mobile device to the point-of-sale terminal comprises sending the expected cryptogram calculated, at least in part, from the unpredictable data, as taught by Smets, in which the mobile device may also comprise a mobile card device for an electronic payment system of Royyuru. This combination increase the security of the electronic payment system in the event that an unauthorized person obtains the CVC3 number for a particular transaction (Smets [0010]).

Claims 3-6, 24, 26 lack an inventive step under PCT Article 33(3) as being obvious over Royyuru et al (US 2010/0185545 A1), hereinafter referred to as Royyuru and further in view of Brown et al (US 2009/0006262 A1), hereinafter referred to as Brown.

Regarding claim 3, Royyuru discloses a method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction (dynamic primary account number and unique key per card, title; financial transaction authorization, abstract, Fig. 3) comprising:
performing an interrogation between the point-of-sale terminal and the mobile device (in NFC technology, a mobile device is in communication with a point-of-sale POS terminal, [0022]) comprising: sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device (commands and responses are communicated between a terminal and mobile device in order to perform a financial transaction, [0057]), the at least one POS command communication comprising (a) a request for the digital credential data that is expected to comprise an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data, and, at least in part, from a permanent cryptographic key (transaction requests comprise credit card numbers, which is digital credential data, and is calculated from a unpredictable number, which is unpredictable data, and the message is encrypted with a key, [0049]-[0051]) and (b) the unpredictable data (an unpredictable number UN, which is unpredictable data, is generated by the NFC terminal and transmitted to the device, [0057]); and sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal (commands and responses are communicated between a terminal and mobile device in order to perform a financial transaction, [0057]), the at least one device response communication comprising at least a portion of the digital credential data that comprises an unexpected cryptogram (encrypting the credit card numbers with an unpredictable number will result in a dynamic PAN, which is an unexpected cryptogram, [0049]-[0051]), wherein the financial transaction is authorized (the financial transaction may be authorized or denied, [0050]).
Royyuru may not adequately describe that an unexpected cryptogram is substituted in place of the expected cryptogram. However, Brown is also in the field of financial transactions (abstract) and further teaches cryptogram substitution of one cryptogram for another cryptogram ([0134]-[0141]; Once the data format is known, it is effectively a template, like an invoice sheet, in which there is a location where information like a price of an item is shown. This is similar to substituting one value for another value given that the data is of the same type, like price). Therefore, it would have been obvious to a person having ordinary skill in the art that: an unexpected cryptogram is substituted in place of the expected cryptogram, as taught by Brown, in a financial transaction system of Royyuru. This combination allows for a a less expensive microcontroller to be required (Brown [0134]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Regarding claim 4 of Claim 3, Royyuru further discloses wherein the unpredictable data comprises an unpredictable number (unpredictable number UN, [0049]-[0051] and [0057]).

Regarding claim 5 of Claim 3, Royyuru discloses that the unpredictable data may be any number, such as a random number, a time of day, or another number generated or received by the presentation instrument ([0051]). Royyuru does not specifically state wherein the unpredictable data comprises a transaction amount. However, it is notoriously well known that a transaction amount is a number. A transaction amount is also unpredictable in the sense that the number is not known as opposed to a credit card number which is already predetermined. Therefore, it would have been obvious to a person having ordinary skill in the art for the unpredictable data of Royyuru to comprise any number, such that the number may be a transaction amount, because a transaction amount is a number that is unpredictable and changes with each transaction.

Regarding claim 6 of Claim 3, Royyuru further discloses a mobile device preparation step that precedes the performing an interrogation step, the mobile device preparation step comprising sending critical data from a remote source to a mobile device, wherein the critical data comprises data used to formulate at least a portion of the digital credential data as a local portion of the digital credential data (before a financial transaction may occur, the mobile device needs to be programmed with a key and information regarding a primary account number PAN that can be mapped to a dynamic PAN, [0004]-[0006] and [0047]-[0048]).

Regarding claim 24 of Claim 3, Royyuru further discloses an authorizing step that follows the step of performing an interrogation, the authorizing step comprising sending the unpredictable data from the mobile device to a remote application system (the mobile device may send the unpredictable number to a remote system as Track-1 data, because the unpredictable number is contained in the Track-1 data format, [0049]-[0051]).

Regarding claim 26 of Claim 3, Royyuru further discloses wherein the communication channel comprises a near-field communication channel (communication via NFC technology is used, [0002]-[0003] and [0022]).

Claims 7, 17 lack an inventive step under PCT Article 33(3) as being obvious over Royyuru et al (US 2010/0185545 A1), hereinafter referred to as Royyuru and further in view of Brown et al (US 2009/0006262 A1), hereinafter referred to as Brown, and further in view of Smets et al (US 2006/0022033 A1), hereinafter referred to as Smets.

Regarding claim 7 of Claim 6, Royyuru may not specifically state: wherein the local portion of the digital credential data comprises a predetermined cryptogram, which is calculated without the use of the unpredictable data, as the unexpected cryptogram. However, Smets is also in the field of electronic payment systems (abstract) and further teaches: wherein the local portion of the digital credential data comprises a predetermined cryptogram (a bitmap is created which serves as a type of template that defines data that is used or unused/discretionary, [0013]-[0014], and hence the bitmap creates a cryptogram that is predetermined and as-of-yet unexpected), which is calculated without the use of the unpredictable data, as the unexpected cryptogram (the unpredictable number is not placed in the bitmap yet, because it is considered to be discretionary, [0026] and [0031]-[0033]). Therefore, it would have been obvious to a person having ordinary skill in the art: wherein the local portion of the digital credential data comprises a predetermined cryptogram, which is calculated without the use of the unpredictable data, as the unexpected cryptogram, as taught by Smets, in an electronic payment system of Royyuru. This combination allows for financial transaction data to be standardized (Smets [0013]-[0014]).

Regarding claim 17 of Claim 3, Royyuru may not specifically state: creating a predetermined cryptogram on the mobile device as the unexpected cryptogram; wherein the predetermined cryptogram is calculated without the use of the unpredictable data; and sending at least a portion of the predetermined cryptogram from the mobile device to a remote application system. However, Smets is also in the field of electronic payment systems (abstract) and further teaches: creating a predetermined cryptogram on the mobile device as the unexpected cryptogram (a bitmap is created which serves as a type of template that defines data that is used or unused/discretionary, [0013]-[0014], and hence the bitmap creates a cryptogram that is predetermined and as-of-yet unexpected); wherein the predetermined cryptogram is calculated without the use of the unpredictable data (the unpredictable number is not placed in the bitmap yet, because it is considered to be discretionary, [0026] and [0031]-[0033]); and sending at least a portion of the predetermined cryptogram from the mobile device to a remote application system (at least a portion of the cryptogram is sent from the mobile device to a remote system for authorization of the transaction, Fig. 5 and [0026]). Therefore, it would have been obvious to a person having ordinary skill in the art for: creating a predetermined cryptogram on the mobile device as the unexpected cryptogram; wherein the predetermined cryptogram is calculated without the use of the unpredictable data; and sending at least a portion of the predetermined cryptogram from the mobile device to a remote application system, as taught by Smets, in an electronic payment system of Royyuru. This combination allows for financial transaction data to be standardized (Smets [0013]-[0014]).

Claims 12-14, 18 lack an inventive step under PCT Article 33(3) as being obvious over Royyuru et al (US 2010/0185545 A1), hereinafter referred to as Royyuru and further in view of Brown et al (US 2009/0006262 A1), hereinafter referred to as Brown, and further in view of Fisher et al (US 2009/0124234 A1), hereinafter referred to as Fisher.

Regarding claim 12 of Claim 6, Royyuru may not adequately disclose: wherein the mobile device preparation step further comprises transiently storing at least a portion of the critical data on the mobile device, wherein the mobile device does not persistently store the at least a portion of critical data. However, Fisher is also in the field of payment transactions ([0011]) and further teaches: wherein the mobile device preparation step further comprises transiently storing at least a portion of the critical data on the mobile device (critical data like a cryptographic key, is transiently stored in the mobile device, because it is only valid for the duration the session, Fig. 4 and [[0016]]), wherein the mobile device does not persistently store the at least a portion of critical data (the cached key data may be flushed, and hence the mobile device does not persistently store the key, Fig.4 and [0017]-[0018]). Therefore, it would have been obvious to a person having ordinary skill in the art: wherein the mobile device preparation step further comprises transiently storing at least a portion of the critical data on the mobile device, wherein the mobile device does not persistently store the at least a portion of critical data, as taught by Fisher, in a payment transaction system of Royyuru. This combination allows for a financial transaction system that is more secure in the event that the mobile device is lost or stolen (Fisher [0013]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding claim 13 of Claim 6, Royyuru further discloses wherein the local portion of the digital credential data comprises an unpredictable cryptogram as the unexpected cryptogram (the Primary Account Number PAN, which is digital credential data, is not sent to the remote system; instead a dynamic PAN is generated and sent as the unpredictable, unexpected cryptogram, Fig. 4 and [0051]-[0055]).
Royyuru may not best disclose: wherein the unpredictable cryptogram is calculated, at least in part, using a temporary cryptographic key.
However, Fisher is also in the field of payment transactions ([0011]) and further teaches: wherein the unpredictable cryptogram is calculated, at least in part, using a temporary cryptographic key (a session key, which is a temporary cryptographic key, is created for the mobile device, Fig. 3 and [0016], and the session key is used to encrypt data for the session, [0016]). Therefore, it would have been obvious to a person having ordinary skill in the art: wherein the unpredictable cryptogram is calculated, at least in part, using a temporary cryptographic key, as taught by Fisher, in a payment transaction system of Royyuru. This combination allows for a financial transaction system that is more secure in the event that the mobile device is lost or stolen (Fisher [0013]).

Regarding claim 14 of Claim 6, Royyuru further discloses wherein the mobile device preparation step further comprises:
Royyuru further discloses wherein the local portion of the digital credential data comprises an unpredictable cryptogram as the unexpected cryptogram (the Primary Account Number PAN, which is digital credential data, is not sent to the remote system; instead a dynamic PAN is generated and sent as the unpredictable, unexpected cryptogram, Fig. 4 and [0051]-[0055]).
Royyuru may not best disclose: creating a temporary cryptographic key in a remote application system wherein the remote application system is the remote source; sending at least a portion of the temporary cryptographic key from the remote application system to the mobile device as a portion of the critical data; and wherein the unpredictable cryptogram is calculated, at least in part, using the temporary cryptographic key. However, Fisher is also in the field of payment transactions ([0011]) and further teaches:
creating a temporary cryptographic key in a remote application system wherein the remote application system is the remote source (a session key, which is a temporary cryptographic key, is server-generated and created for the mobile device, Fig. 3 and [0016]); sending at least a portion of the temporary cryptographic key from the remote application system to the mobile device as a portion of the critical data (at least a portion of session key is sent from the server to the mobile device, because the session key is server generated, Fig. 3 and [0016]); and wherein the unpredictable cryptogram is calculated, at least in part, using the temporary cryptographic key (the session key is used to encrypt data for the session including cryptograms communicated during the session, [0016]). Therefore it would have been obvious to a person having ordinary skill in the art for: creating a temporary cryptographic key in a remote application system wherein the remote application system is the remote source; sending at least a portion of the temporary cryptographic key from the remote application system to the mobile device as a portion of the critical data; and wherein the unpredictable cryptogram is calculated, at least in part, using the temporary cryptographic key, as taught by Fisher, in a payment transaction system of Royyuru. This combination allows for a financial transaction system that is more secure in the event that the mobile device is lost or stolen (Fisher [0013]).

Regarding claim 18 of Claim 3, Royyuru may not adequately disclose: creating a temporary cryptographic key on the mobile device; wherein the temporary cryptographic key is used to calculate, at least in part, an unpredictable cryptogram as the unexpected cryptogram; sending at least a portion of the unpredictable cryptogram from the mobile device to a remote application system. However, Fisher is also in the field of payment transactions ([0011]) and further teaches: creating a temporary cryptographic key on the mobile device (a session key, which is a temporary cryptographic key, is created for the mobile device, Fig. 3 and [0016]); wherein the temporary cryptographic key is used to calculate, at least in part, an unpredictable cryptogram as the unexpected cryptogram (the session key is used to encrypt data for the session, [0016], and hence constitutes an unpredictable cryptogram calculated at least in part with a temporary session key); sending at least a portion of the unpredictable cryptogram from the mobile device to a remote application system (at least a portion of the cryptogram is sent to a remote server in order to conduct payment transactions, Fig. 1 and [0011]-[0013]). Therefore it would have been obvious to a person having ordinary skill in the art for: creating a temporary cryptographic key on the mobile device; wherein the temporary cryptographic key is used to calculate, at least in part, an unpredictable cryptogram as the unexpected cryptogram; sending at least a portion of the unpredictable cryptogram from the mobile device to a remote application system, as taught by Fisher, in a payment transaction system of Royyuru. This combination allows for a financial transaction system that is more secure in the event that the mobile device is lost or stolen (Fisher [0013]).

Claim 25 lacks an inventive step under PCT Article 33(3) as being obvious over Royyuru et al (US 2010/0185545 A1), hereinafter referred to as Royyuru and further in view of Brown et al (US 2009/0006262 A1), hereinafter referred to as Brown, and further in view of Buhot et al (US 2010/0207742 A1), hereinafter referred to as Buhot.

Regarding claim 25 of Claim 3, Royyuru further discloses that the POS command communication conforms to a data protocol and the device response communication conforms to a data protocol (in order to communicate, [0057] and [0037]). Royyuru lacks wherein the data protocol is the ISO 7816-4 protocol. However, Buhot is also in the field of near field communications (abstract) and further teaches the ISO 7816-4 data protocol ([0052] and [0085]). Therefore, it would have been obvious to a person having ordinary skill in the art to substitute a data protocol for the ISO 7816-4 protocol of Buhot wherein the POS command communication conforms to a data protocol and the device response communication conforms to a data protocol of Royyuru. This combination allows for an electronic payment system using NFC technology (Buhot [0018]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Claim 27 lacks an inventive step under PCT Article 33(3) as being obvious over Royyuru et al (US 2010/0185545 A1), hereinafter referred to as Royyuru and further in view of Brown et al (US 2009/0006262 A1), hereinafter referred to as Brown, and further in view of Yeager (US 2007/0075133 A1).

Regarding claim 27 of Claim 3, Royyuru does not specifically state: wherein the mobile device does not access a local persistently stored permanent cryptographic key that is expected to be used to calculate the expected cryptogram wherein the expected cryptogram is expected to be contained within the at least a portion of the digital credential. However, Yeager is also in the field of NFC devices ([0003]) and further teaches: wherein the mobile device does not access a local persistently stored permanent cryptographic key that is expected to be used to calculate the expected cryptogram wherein the expected cryptogram is expected to be contained within the at least a portion of the digital credential (a mobile device, like a mobile phone, [0027], does not actually access the keys, because the keys for encrypting the credential data are only shared between the server and adapter, Fig. 6 and [0031]-[0032]). Therefore, it would have been obvious to a person having ordinary skill in the art: wherein the mobile device does not access a local persistently stored permanent cryptographic key that is expected to be used to calculate the expected cryptogram wherein the expected cryptogram is expected to be contained within the at least a portion of the digital credential, as taught by Yeager, in a financial transaction system of Royyuru. This combination better ensures the confidentiality and security of the keys (Yeager [0031]).

Claims 8-11, 15-16, 19-23 meet the criteria set out in PCT Article 33(2)-(3), because the prior art does not teach or fairly suggest:

Regarding claim 8 creating remote unpredictable data in a remote application system wherein the remote application system is the remote source; sending the remote unpredictable data from application system to an HSM; calculating a predetermined cryptogram in the HSM; sending the predetermined cryptogram from the HSM to the remote application system; sending at least a portion of the predetermined cryptogram from the remote application system to the mobile device as a portion of the critical data; and wherein the local portion of the digital credential data comprises the predetermined cryptogram as the unexpected cryptogram.

Regarding claim 9 creating a predetermined cryptogram, which is calculated without the use of the unpredictable data, in a remote application system wherein the remote application system as the remote source; sending at least a portion the predetermined cryptogram from the remote application system to the mobile device as a portion of the critical data; and wherein the local portion of the digital credential data comprises the predetermined cryptogram as the unexpected cryptogram.

Regarding claim 10 wherein the critical data comprises a set of possible predetermined cryptograms; and the method further comprises a logical step of logically determining, in the mobile device, which of the possible predetermined cryptograms within the set of predetermined cryptograms to designate as the unexpected cryptogram; wherein the logical step is based, at least in part, on the unpredictable data; and wherein the local portion of the digital credential data comprises the designated predetermined cryptogram as the unexpected cryptogram.

Regarding claim 11: wherein the critical data comprises a set of possible predetermined cryptograms and card risk management data; and the method further comprises a logical step of logically determining, in the mobile device, which of the possible predetermined cryptograms within the set of possible predetermined cryptograms to designate as the unexpected cryptogram; wherein the logical step of is based, at least in part, on the unpredictable data or based, at least in part, on the card risk management data; and wherein the local portion of the digital credential data comprises the designated predetermined cryptogram as the unexpected cryptogram.

Regarding claim 15 wherein the critical data comprises a temporary cryptographic key; and the method further comprises a step of calculating at least one local unpredictable cryptogram that is calculated, in at least part, using the temporary cryptographic key, and, in at least part, using a calculation formula determined from a set of calculation formulas; and the method further comprises a logical step of logically determining, in the mobile device, which local unpredictable cryptogram to designate as the unpredictable cryptogram; wherein the step of logically determining a decision is made based, at least in part, on the unpredictable data; and wherein the local portion of the digital credential data comprises the designated local unpredictable cryptogram as the unexpected cryptogram.

Regarding claim 16 wherein the critical data comprises a temporary cryptographic key and card risk management data; and the method further comprises a step of calculating at least one local unpredictable cryptogram that is calculated, in at least part, using the temporary cryptographic key, and, in at least part, using a calculation formula determined from a set of calculation formulas; and the method further comprises a logical step of logically determining, in the mobile device, which local unpredictable cryptogram to designate as the unpredictable cryptogram;
wherein the logical step is made based, at least in part, on the unpredictable data or based, at least in part, on the card risk management data; and wherein the local portion of the digital credential data comprises the designated local unpredictable cryptogram as the unexpected cryptogram.

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Regarding claim 19: an authorizing step that follows the step of performing the interrogation, the authorizing step comprising: sending an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system, wherein the unexpected cryptogram comprises a predetermined cryptogram; verifying a correctness of the predetermined cryptogram by the application system
(a) by comparing the predetermined cryptogram with a previously stored reference predetermined cryptogram and
(b) without reference to the unpredictable data from the point-of-sale terminal; and sending an authorization response from the remote application system to the point-of-sale wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the predetermined cryptogram.

Regarding claim 20 an authorizing step that follows the step of performing the interrogation, the authorizing step comprising: sending an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system, wherein the unexpected cryptogram comprises an unpredictable cryptogram: verifying a correctness of the unpredictable cryptogram by the application system wherein the unpredictable cryptogram is compared with a result of an unpredictable cryptogram calculation; wherein the unpredictable cryptogram calculation is calculated using, at least in part, a temporary cryptographic key; and sending an authorization response from the remote application system to the point-of-sale wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable cryptogram.

Regarding claim 21 a corroborative authorizing step that follows the step of performing the interrogation, the corroborative authorizing step comprising: sending through a second communication channel an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system; sending through a third communication channel the unpredictable data from the mobile device to the remote application system; verifying a correctness of the unexpected cryptogram in the remote application system;
verifying a correctness of the unpredictable data in the remote application system by comparing the unpredictable data sent through the second communication channel with the unpredictable data sent through the third communication channel; sending through the second communication channel an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable data and, at least in part, by the verifying of the correctness of the unexpected cryptogram.

Regarding claim 22 a verifying a transaction amount step that follows the step of performing an interrogation and precedes the corroborative
authorizing step, the verifying a transaction amount step comprising: displaying transaction amount data to a display on the mobile device wherein the transaction amount data is at least a portion of the unpredictable data; requesting verification of the transaction amount data from a card holder by the mobile device display screen; sending the result of the requesting verification of the transaction amount data to a remote application system as input transaction amount data; and wherein the corroborative authorizing step comprises determining, at least in part, an accuracy of the result of the verification step by using the input of the transaction amount data.

Regarding claim 23 an authorizing step that follows the step of performing an interrogation, the authorizing step comprising: sending an authorization request comprising the unpredictable data and the unexpected cryptogram from the point-of-sale terminal to a remote application system, wherein the unexpected cryptogram comprises a predetermined cryptogram; verifying a correctness of the predetermined cryptogram wherein the unpredictable data from the point-of sale (a) is substituted by the application system with a previously created unpredictable data that was previously used to calculate the predetermined cryptogram; and subsequently (b) is sent with the predetermined cryptogram to the HSM for cryptogram correctness verification; and sending an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the predetermined cryptogram.

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding claim 28: A method for acquiring digital credential data by a point-of-sale terminal from a secure mobile device for authorization of a financial transaction comprising: performing an interrogation between the point-of-sale terminal and the secure mobile device comprising: sending through a communication channel at least one POS command communication from the point-of-sale terminal to the secure mobile device,
the at least one POS command communication comprising (a) a request for the digital credential data that is expected to comprise an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data, and, at least in part, from a permanent cryptographic key and (b) the unpredictable data; and sending through the communication channel at least one device response communication from the secure mobile device to the point-of-sale terminal, the at least one device response communication comprising at least a portion of the digital credential data that comprises the expected cryptogram; in a step that follows the step of performing an interrogation, a secure mobile device transmitting step comprising sending over a second communication channel the unpredictable data from the secure mobile device to a remote application system; in a step that follows the step of performing an interrogation, a point-of-sale terminal transmitting step comprising sending over a third communication channel an authorization request from the point of sale terminal to the remote application system, the authorization request comprising the expected cryptogram and the unpredictable data; in a step that follows the secure mobile device transmitting step and the point-of-sale terminal transmitting step, a corroborative authorizing step comprising: verifying a correctness of the expected cryptogram by the application system; verifying a correctness of the unpredictable data by the application system by comparing the unpredictable data sent over the second communication channel with the unpredictable data sent over the third communication channel; and sending through the third communication channel an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable data and at least in part by the verifying of the correctness of the expected cryptogram; wherein the financial transaction is authorized.

Claim 29 meets the criteria due to their dependence on novel claim 28.

The prior art, as shown below, details some of the aspects of the invention, however none of the prior art teaches all the missing limitations either alone or in combination as specified:

Royyuru et al (US 2010/0185545 A1), discloses a method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction (dynamic primary account number and unique key per card, title: financial transaction authorization, abstract, Fig. 3) comprising:
performing an interrogation between the point-of-sale terminal and the mobile device (in NFC technology, a mobile device is in communication with a point-of-sale POS terminal, [0022]) comprising: sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device (commands and responses are communicated between a terminal and mobile device in order to perform a financial transaction, [0057]), the at least one POS command communication comprising (a) a request for the digital credential data that is expected to comprise an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data, and, at least in part, from a permanent cryptographic key (transaction requests comprise credit card numbers, which is digital credential data, and is calculated from a unpredictable number, which is unpredictable data, and the message is encrypted with a key, [0049]-[0051]) and (b) the unpredictable data (an unpredictable number UN, which is unpredictable data, is generated by the NFC terminal and transmitted to the device, [0057]); and sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal (commands and responses are communicated between a terminal and mobile device in order to perform a financial transaction, [0057]), the at least one device response communication comprising at least a portion of the digital credential data that comprises an unexpected cryptogram (encrypting the credit card numbers with an unpredictable number will result in a dynamic PAN, which is an unexpected cryptogram, [0049]-[0051]), wherein the financial transaction is authorized (the financial transaction may be authorized or denied, [0050]).Royyuru may not adequately describe that an unexpected cryptogram is substituted in place of the expected cryptogram, or the verifying correctness features.

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2012/053129

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Yeager discloses a method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction (method, system and computer-readable medium for radio frequency identification device, title; the adapter is connected to a host device like a mobile phone to construct a mobile device capable of financial transactions, Fig. 3 and [0027]-[0029], in which the mobile device communicates with a terminal such as the Mastercard PayPass system, Fig. 5 and [0030]) comprising: using a remote permanent cryptographic key to calculate an expected cryptogram that is expected to comprise at least a portion of the digital credential data (a secret key on a remote server, Fig. 6 and [0031]-[0032], which is a remote permanent cryptographic key, is used to calculate an expected cryptogram that comprises, and hence encrypts, digital credential data such as credit card information, [0022]). Yeager does not disclose the unpredictable data; and sending through the communication channel at least one device response communication from the secure mobile device to the point-of-sale terminal, the at least one device response communication comprising at least a portion of the digital credential data that comprises the expected cryptogram; in a step that follows the step of performing an interrogation, a secure mobile device transmitting step comprising sending over a second communication channel the unpredictable data from the secure mobile device to a remote application system; in a step that follows the step of performing an interrogation, a point-of-sale terminal transmitting step comprising sending over a third communication channel an authorization request from the point of sale terminal to the remote application system, the authorization request comprising the expected cryptogram and the unpredictable data; in a step that follows the secure mobile device transmitting step and the point-of-sale terminal transmitting step, a corroborative authorizing step comprising: verifying a correctness of the expected cryptogram by the application system; verifying a correctness of the unpredictable data by the application system by comparing the unpredictable data sent over the second communication channel with the unpredictable data sent over the third communication channel; and sending through the third communication channel an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the unpredictable data and at least in part by the verifying of the correctness of the expected cryptogram; wherein the financial transaction is authorized.

Claims 1-29 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.

Electronic Patent Application Fee Transmittal

Application Number:	13599647
Filing Date:	30-Aug-2012
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Filer:	John L. Adair/Shenise Ramdeen
Attorney Docket Number:	STAPP1100-5

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	2253	1	700	700
Miscellaneous:				
RCE- 1st Request	2801	1	600	600
		Total in USD ($)		**1300**

Electronic Acknowledgement Receipt	
EFS ID:	27792964
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Customer Number:	44654
Filer:	John L. Adair/Shenise Ramdeen
Filer Authorized By:	John L. Adair
Attorney Docket Number:	STAPP1100-5
Receipt Date:	14-DEC-2016
Filing Date:	30-AUG-2012
Time Stamp:	14:57:12
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1300
RAM confirmation Number	121516INTEFSW00001466503183
Deposit Account	503183
Authorized User	Shenise Ramdeen
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	STAPP1100-5_RCE12-14-16.pdf	432483 cc77a456ccnee9e25322e5ef6a09eb5fb57d23f49	no	2
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
2	Amendment Submitted/Entered with Filing of CPA/RCE	STAPP1100-5_ROA12-14-16.pdf	1088877 6f38715ee0d55f250e53c977b0e9a089d289a225	no	15
Warnings:					
Information:					
3		STAPP1100-5_IDS12-14-16.pdf	427303 55ac3435a4668ea746e1a1ddbc4fbea39fa065e	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Information Disclosure Statement (IDS) Form (SB08)	1	2
	Non Patent Literature	3	3

Warnings:					
Information:					
4	Extension of Time	STAPP1100-5_EOT12-14-16.pdf	621094 268c858f943cad8193cba43a33cd0455256729c	no	1
Warnings:					
Information:					
5	Non Patent Literature	STAPP1100_Ref_C4.pdf	790485 d33ede93229e40d0891383e8b6504d6241b276	no	11
Warnings:					

Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	32580 b6b1c3225d173afc310cdda12fc161a66b9fb18ec3	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	3392822	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/599,647	Filing Date 08/30/2012	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	12/14/2016	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 29	Minus	** 29	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $210 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
TARA WASHINGTON

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/599,647
				Filing Date	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	Puttaiah, Asha
Sheet	1	of	1	Attorney Docket Number	STAPP1100-5

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	B3	CN101048794	10-03-2007	Mastercard International Inc.	

Examiner Signature		Date Considered	

Substitute Form PTO/SB/08b

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/599,647
				Filing Date	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	Puttaiah, Asha
Sheet	1	of	1	Atty Docket Number	STAPP1100-5

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C8	Patent Examination Report for Australian Patent Application No. 2012301897, issued on November 22, 2016, 4 pages.	
	C9	Office Action for Chinese Patent Application No. 201280053080.6, issued on June 22, 2016, 20 pages.	
	C10	Search Report issued for European Patent Application No. 12827026.1, issued on June 10, 2016, 6 pages.	
	C11	Office Action for Canadian Patent Application No. 2,846,462, issued November 4, 2016, 3 pages.	

Examiner Signature		Date Considered	

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06Q 99/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200580028482.0

[43] 公开日 2007 年 10 月 3 日

[11] 公开号 CN 101048794A

[22] 申请日 2005.8.18
[21] 申请号 200580028482.0
[30] 优先权
[32] 2004.8.18 [33] US [31] 60/602,594
[86] 国际申请 PCT/US2005/029758 2005.8.18
[87] 国际公布 WO2006/023839 英 2006.3.2
[85] 进入国家阶段日期 2007.2.25
[71] 申请人 万事达卡国际股份有限公司
地址 美国纽约州
[72] 发明人 J·万克穆勒

[74] 专利代理机构 上海专利商标事务所有限公司
代理人 张鑫

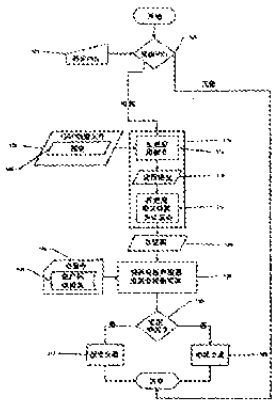
权利要求书 3 页 说明书 10 页 附图 3 页

[54] 发明名称

使用动态授权码授权交易的方法和系统

[57] 摘要

一种用于执行安全交易的方法和装置包括基于不能标识账户的保密数据在移动装置上生成动态认证码。认证码和金融账户标识信息被发送到共享关于该保密数据的信息的验证实体，以授权交易。



Mastercard, Ex1002, p. 645

1. 一种用于授权交易的方法，所述方法包括：

将账户保密数据与授权数据库中的唯一金融账户标识符相关联；

至少部分地基于与所述账户保密数据相关联的数据生成个人化数据；

将所述个人化数据发送至移动处理设备用于存储，所述移动处理设备不包含所述唯一金融账户标识符；

在授权端接收授权请求以授权交易，所述请求包括所述唯一金融账户标识符和由所述移动处理设备生成的动态认证码；

判断所述动态认证码是否是由包含至少部分地基于与账户保密数据相关联的数据而生成的个人化数据的移动处理设备生成的，其中账户保密数据与授权数据库中的金融账户标识符相关联；以及

根据所述判断步骤授权所述交易。

2. 如权利要求 1 所述的方法，其特征在于，进一步包括：

所述移动处理设备提示输入标识 PIN；以及

在移动处理设备生成所述动态认证码之前，由移动处理设备验证所述标识 PIN。

3. 如权利要求 1 所述的方法，其特征在于，所述账户保密数据是加密密钥。

4. 如权利要求 3 所述的方法，其特征在于，与账户保密数据相关联的所述数据是所述加密密钥。

5. 如权利要求 3 所述的方法，其特征在于，所述加密密钥是私钥，并且与账户保密数据相关联的所述数据是与所述私钥相关联的公钥。

Mastercard, Ex1002, p. 646

6. 如权利要求 1 所述的方法，其特征在于，由所述移动处理设备生成的所述动态认证码至少部分基于存储在所述移动处理设备上的交易计数器。

7. 如权利要求 6 所述的方法，其特征在于，所述交易计数器的副本被保存在所述授权数据库中，所述方法进一步包括校验用于生成所述动态认证码的所述交易计数器是否与所述交易计数器的所述副本相匹配。

8. 如权利要求 6 所述的方法，其特征在于，当生成所述动态认证码时，所述交易计数器递增。

9. 一种用于授权交易的系统，其特征在于，所述系统包括：

包含至少一个唯一金融账户标识符以及与所述标识符相关联的账户保密数据的授权数据库；

不包含所述唯一金融账户标识符、用于生成动态认证码的移动处理设备；

用于将个人化数据发送至所述移动处理设备的发射器，所述个人化数据至少部分地基于与所述账户保密数据相关联的数据；

用于接收授权请求以授权交易的接收器，所述授权请求包括所述唯一金融账户标识符和动态认证码；

授权处理器，用于判断所述动态认证码是否是由包含至少部分地基于与账户保密数据相关联的数据而生成的个人化数据的移动处理设备生成的，其中账户保密数据与认证数据库中的金融账户标识符相关联，以及根据所述判断步骤授权所述交易。

10. 如权利要求 9 所述的系统，其特征在于，所述账户保密数据是加密密钥。

11. 如权利要求 10 所述的系统，其特征在于，与账户保密数据相关联的

Mastercard, Ex1002, p. 647

所述数据是所述加密密钥。

12. 如权利要求 10 所述的系统，其特征在于，所述加密密钥是私钥，并且与账户保密数据相关联的所述数据是与所述私钥相关联的公钥。

13. 如权利要求 9 所述的系统，其特征在于，所述移动处理设备包括交易计数器，并且所述移动处理设备至少部分地使用所述交易计数器来生成所述动态认证码。

14. 如权利要求 13 所述的系统，其特征在于，所述授权数据库进一步包括所述交易计数器的副本，并且所述授权处理器进一步用于校验用于生成所述动态认证码的所述交易计数器是否与所述交易计数器的所述副本相匹配。

15. 如权利要求 13 所述的系统，其特征在于，当生成所述动态认证码时，所述交易计数器递增。

Mastercard, Ex1002, p. 648

使用动态授权码授权交易的方法和系统

相关申请

本申请要求于 2004 年 8 月 18 日提交的申请号为 60/602，594 的题为"用于生成支付或金融交易使用的授权码的方法和系统（Method And System for Generating Authentication Codes For Use in Payment or Financial Transactions）"的美国临时申请的优先权。

背景技术

在远程交易中信用卡和借记卡的使用一直持续增长。无论是通过电话、通过邮件、在零售店、或者通过互联网，共同的是需要不经过面对面的接触而进行交易。然而，远程交易没有面对面交易安全并且欺诈的可能性相对较高，尤其是当交易卡遗失或被窃。

一种最小化欺诈的方法是通过使用个人标识号或者 PIN。用这种方法，在交易时，用户的卡插入或者划过读卡器。读取器从卡上提取特定数据，如账号。接着读卡器要求用户在小键盘上输入他或她的 PIN。PIN 被加密或以其它方式进行保护，而安全的 PIN 数据被发送至授权端，诸如授权计算机，在那里存储着持卡人数据。在授权计算机处，用账户标识数据来查找并获取账户信息，获取的信息被用于校验持卡人输入的 PIN 是否正确。这种方法使欺诈减至最小，因为卡的拥有者必须同时知道保密的 PIN 以完成交易。这种方法的一项缺点是：由于 PIN 是静态的，窃贼可以在合法交易中截取 PIN 并在之后的欺诈交易中重新使用该 PIN。

在另一种本发明人最近建议的方法中，用频繁改变的动态码来取代静态 PIN。这种方法在共同待批的申请号为 60/626,649 的题为"允许使用动态码用于认证的方法和系统(Method And System For Enabling The Use Of Dynamic Codes For Authentication)"的美国专利申请中有更详细的描述，该申请全文被引用并

Mastercard, Ex1002, p. 649

合并与此。这种方法的一个方面包括使用智能卡和智能卡读取器来生成动态码。智能卡是本领域公知的，其典型地是信用卡状的卡，并包括安全数据存储区域和处理器。在可能交易时，智能卡用智能卡的安全存储器中存储的保密数据生成应用密文。应用密文的生成是本领域公知的，例如，在由 EMVCo.LLC 发布的可在互联网上地址为http://www.emvco.com看到的题为"用于支付系统的 EMV 集成电路卡规范（EMV Integrated Circuit Card Specifications for Payment Systems）"的公知的智能卡规范中有更详细的解释，该规范被引用整体上结合于此。接着该数据（或其一部分）被作为动态码发送至授权计算机。授权计算机可基于从授权数据库获取的与账号相关联的账户信息来校验是否该动态码是由与当前使用的账号相关联的智能卡生成以完成交易的。

使用智能卡以增强交易的安全性的一项缺点是与更传统的磁条式卡相比制造相对昂贵。另外，智能卡需要在每次交易中使用智能卡读取器，这就需要对现有的为磁条式卡设计的销售点进行升级。由于这些或其它的原因，智能卡和智能卡读取器尚没有在美国境内广泛使用。

发明内容

本发明使交易可以以更安全的方式被授权而不需要广泛设置智能卡和智能卡读取器。取而代之地，使用持卡者已经拥有的（诸如 PDA 或者手机之类的）移动消费设备的处理能力来生成与具体持卡者账户相关联的动态授权码。移动设备不会包含可以识别与之相关联的具体账户的数据。接着，动态码与账户标识数据一起被发送至认证计算机以校验交易的真实性。

在本发明的一个示例性的实施例中，提供了一种授权交易的方法。该方法需要将账户保密数据与授权数据库中唯一的金融账户标识符相关联，并至少部分地基于与该账户保密数据相关联的数据生成个人化数据。个人化数据被发送至移动处理设备（诸如 PDA 或手机）用于存储于其中，该移动处理设备不包含所述唯一的金融账户标识符。接着，授权端接收到授权请求。该请求包括金融账户标识符和由移动处理设备生成的动态认证码。接着进行判断，判断该认证码是否是由包含至少部分地基于与账户保密数据相关联的数据而生成的个

Mastercard, Ex1002, p. 650

人化数据的移动处理设备生成的，其中账户保密数据与授权数据库中的金融账户标识符相关联。

附图说明

为了对本发明更全面的理解，下面结合附图给出以下对示例性的实施例的详细描述，在附图中：

图 1 是根据本发明的一个示例性实施例的使用生成的认证码和账户标识信息进行交易的步骤的流程图；

图 2 是用于生成认证码的一个示例性系统的方框图；以及

图 3 是本发明的一个示例性实施例的方框图。

具体实施方式

图 1 是描述本发明的一个示例性实施例的流程图，其限定了使用生成的动态认证码 130 和账户标识信息或唯一金融账户标识符 140 来进行交易。以下描述将基于假设的通过（诸如互联网之类的）计算机网络进行的交易。然而，可以理解的是本发明的实施例不局限于通过计算机网络的交易，而是可以容易地适用于其它类型的交易，诸如通过电话、邮件、面对面、或其它方式的交易。

假设的交易开始于个人计算机（PC）用户使用网络浏览器或类似运行在个人计算机上的应用软件发起请求以购买来自销售商的货物或服务。需要注意的是，任何用于请求或进行交易的设备、系统或方案均可用来替换 PC，这包括诸如 PDA 或手机之类的移动设备。接着用户的请求使销售商的计算机调用授权请求服务器以认证用户的身份并校验交易是否合法。授权请求服务器或授权处理器（其可以是大型机或其它具有处理器、存储器以及通信连接的计算机）提示用户使用他或她的移动处理设备来提供动态授权码。

在步骤 101，用户激活他或她的移动处理设备（诸如个人数字助理（PDA）或手机）并调用功能以生成动态认证码。（在此将更详细讨论的）

Mastercard, Ex1002, p. 651

移动处理设备包括用于生成动态码的软件或电路。在具体的示例性实施例中，移动设备上的软件或电路具有典型智能卡几乎全部的功能，虽然不具备任何可以直接用于唯一地标识金融或支付账号的数据。在一实施例中，一旦移动设备被激活，用户就会被提示使用小键盘、键盘、或一些其它用于将用户输入接收到移动处理设备中的技术来输入标识 PIN。应当理解的是移动处理设备可以是膝上型计算机或其它个人计算机，也可以是与用于正讨论的假设交易的计算机相同的个人计算机。然而典型的是，执行交易的个人计算机与移动设备是独立的设备。接着在步骤 103，移动设备通过将 PIN 与存储在该设备上的数据相比较来证实该 PIN 是否有效。值得注意地，步骤 101 和 103 不是必需的，但可用于有效地增强授权系统的安全性并阻止欺诈。另外，如此处更为详细讨论的那样，当使用 PIN 时，PIN 输入过程可以被延迟直到用户将与交易有关的其它数据输入到移动设备以后。

在一个示例性实施例中，授权处理器还可为用户提供口令号，或其它用户将输入到他或她的移动处理设备中去的不可预测的数据，该数据随后被用于（典型地与诸如加密密钥之类的其它数据一起）生成动态认证码。该不可预测数据可以是随机数、可以基于当前时间、预测交易额的单项散列、上述的某些组合、或者不能在交易前被轻易预测的任何其它数据。用户还可以被提示将与交易有关的其它数据输入到移动设备中，诸如交易额和货币种类，设备可以使用这一数据以及其它保密数据来生成将成为在此较详细讨论的动态授权码的密文。

在步骤 110，移动处理设备使用（诸如加密密钥之类的）密钥 120 来生成动态认证码 130。密钥 120 可以是 DES 密钥、私钥、公钥、上述的某些组合、或者用于加密或生成用于后续认证的保密消息的任何其它数据。密钥可保存在例如移动处理设备的应用存储器中。如果移动处理设备包括安全或受保护存储器（例如在插入到手机或 PDA 中的订户身份模块（SIM）卡中），则密钥也可以有效地存储在那里。密钥 120 还可被加密或存放在不可被其它处理器、运行在移动设备上的程序或应用程序访问的存储器单元中。例如，密钥可以用（诸如用户 PIN、移动设备序列号、其它数据或

Mastercard, Ex1002, p. 652

上述组合的）另一密钥加密。值得注意地，移动设备中的安全存储器不是必需的。

移动设备的存储器应不包含任何将标识密钥 120 所对应的账户的信息。特别地，密钥 120（以及移动设备存储器）不应包含支付账号（PAN）、卡有效期限、典型地存储在交易卡磁条上的卡片轨道数据、账户持有者姓名、或可以唯一标识金融账户的任何其它数据。这样，如果移动设备被窃或被危害，设备不会被用于执行交易，因为不会有任何数据能够标识密钥 120 所对应的金融账户。

在示例性的实施例中，密钥 120 与应用简档标识符、应用交易计数器、以及其它数据一起被存放在芯片认证程序（CAP）数据文件 125 中。在 MasterCard 的芯片认证程序规范中可找到更多关于芯片认证程序格式和功能的细节，该规范可以从纽约州 Purchase 的 MasterCard 国际股份有限公司购买许可，其被全文引用并合并于此。在示例性实施例中，CAP 数据文件 125 可被加密，并随后通过用户输入的 PIN、从进行解密的设备收集的（诸如电话号码或设备序列号之类的）移动设备标识符、或两者组合来解密。这样，CAP 数据文件的使用可被限制为知晓 PIN、被批准的设备、或两者组合的个人。在示例性实施例中，（被任选地包含在数据文件 125 中的）交易计数器是顺序计数器，其在每一次生成动态授权码后递增。

生成认证码的步骤 110 可进一步理解为包括在步骤 112 中应用密文 115 的生成。应用密文使用智能卡设计或工作领域中公知的技术（例如以下形式：当提供 GENERATE AC 命令时，兼容 EMV 的智能卡工作）从密钥 120、以及诸如交易计数器之类的其它数据生成。在前述的授权处理器为用户提供不可预测数据的示例性实施例中，除密钥 120 和交易计数器以外还基于该不可预测数据来生成应用密文。有关交易的其它数据也可被用于计算应用密文，诸如交易额、交易日期/时间、货币种类等。例如，在一个实施例中，不可预测数据、交易计数器、以及任何其它有关数据可以连接在一起并通过密钥 120 来加密以生成应用密文。认证处理器和/或发行银行可选择哪些数据该用于计算由该发行银行维护的交易账户的应用密文。因此，在

Mastercard, Ex1002, p. 653

本示例性实施例中，移动设备本质上成为与智能卡的 CAP 规范所描述的类似功能的"软件智能卡"。

在示例性实施例中，应用密文 115 是可由以下数据项目组成的中间数据格式，数据项目以二进制表示并从最高位到最低为连接如下：密文信息数据（8 位）、交易计数器（16 位）、移动处理计算的密文（64 位）、以及发行方应用数据（0-256 位）。发行方应用数据是由维护持卡者账户的金融机构选择的数据并可以是任何数据；然而，对于本发明的目的，较佳的是发行方应用数据不包括能够被用于标识持卡者或与持卡者相关联的金融账户的信息。

由于该中间步骤的输出可能导致数据值最多达到 43 字节的长度（即值的范围从 0 到 2^{344} 或约 $3.6x10^{103}$），这作为十进制数而言太大以致于无法提供给用户，该数据在显示给用户之前必须被压缩或限制。事实上，考虑到用户可能需要重新向他们进行交易的计算机上的网络浏览器输入动态码，即使是（形成中间数据的一部分的）64 位的密文在十进制格式中也太长以致无法显示给用户。因此，在步骤 117，中间数据被缩减到更容易管理的数据大小并被呈现给用户。在示例性实施例中，中间密文数据被缩减到 8 个数字字符，使得可能的值在 0 至 99,999,999 范围内。在示例性实施例中，该缩减是通过使用位映射（bitmap）来实现的，该位映射标识在中间数据格式中的哪些位应该被保留并用于计算动态认证码。例如，位映射可标识位 1—15、17—19、以及 21—27 作为从中间计算中保留的位。接着，保留的位被连接在一起并显示为二进制编码的十进制格式（BCD）。用这种方法，为了确保显示给用户的可能值不超过 8 个数字，可以被保留的位的最大数量是 26。保留的准确的位数可根据具体应用和情况而定；然而，授权处理器还必须知道用于选择待保留位的算法，使授权处理器可校验移动处理设备生成的动态认证码。

在示例性实施例中，在生成的最终动态认证码中不包括授权处理器知道的位和数据、或授权服务器可以从它所知道的或在动态认证码中提供的其它数据中得到的数据。例如，如果使用了交易计数器并且认证处理器在

Mastercard, Ex1002, p. 654

授权数据库中保存有与移动设备相关联的交易计数器的副本，完整的交易计数器不需要被包含在用于生成动态码的数据中。例如，可能仅需要包括该计数器的一些最低位。那样，即使授权数据库中存储的交易计数器的副本与移动设备中的计数器不同步，授权处理器也可以重建交易计数器，并使用从移动设备接收到的动态授权码中有关计数器的部分数据来准确计算它自身版本的密文。

只要保存合理数量的位，中间数据的其它位（包括经计算的密文）也可被排除，以最小化错误认证的可能性，牢记的是授权处理器会使用与移动设备共享的保密信息（即示例性实施例中的密钥）来计算它本身版本的密文、以及交易特定数据，诸如不可预测数字、交易计数器等，并且如果处理器确定（经从移动设备接收的动态授权码证实的）由移动设备计算的密文与（借助前述位映射来隐蔽之后的）由授权处理器计算的密文相匹配，则授权交易。

密文计算的方式可以与在此描述的不同并且有无数种。在一实施例中，密文要求基于由账户持有者的发行银行所选择的数据来进行计算，并将计算的结果用存储在卡上的（诸如加密密钥之类的）保密信息加密。然而，密文生成步骤 110 应产生动态的（而非静态的）、即使对于相同类型和金额的重复交易也不可预测地变化的认证码 130。这会降低偷听者截取动态授权码、并在并不真正由与用于进行交易的金融账户相关联的持卡者所授权的之后的尝试交易中再现该动态授权码的可能性。另外，计算应证实与正用于交易的金融账户相关联的持卡者已授权了该交易。在较佳实施例中，这通过在生成动态认证码之前要求输入 PIN 到设备来实现。

虽然认证码是动态的并且基于（诸如具体交易特点和其它随机和变化数据之类的）各种因素频繁变化，但生成步骤 110 可要求具体认证码的产生在时间上大于一次，而不背离本发明要求的范围。生成步骤 110 可在（诸如 PDA、移动电话或手机、膝上型计算机、或其它设备的）移动处理设备上执行。设备应具有能够执行生成认证码 130 所必需步骤的能力的处理器。移动处理设备还可是智能卡，而生成步骤 110 可由智能卡执行。

Mastercard, Ex1002, p. 655

如图 2 中所示，在示例性实施例中，移动设备包括包含用于生成动态认证码的数据（包括由设备的用户输入的数据）的数据储存区域 1030，诸如 RAM、闪存、硬盘驱动器、或其它存储器。设备还包括认证码生成器 1020，其可以是被编程为生成基于在此所述的且为本领域技术人员所熟知的任何技术的认证码的处理器。生成器 1020 生成之前所述的动态认证码 130，并将该码提供给输出设备 1010。该认证码输出设备 1010 可将生成的动态认证码 130 呈现给用户，诸如通过 LCD 屏幕或其它显示器、通过同步语音技术或声响、或一些其它手段。可选地（或附加地），设备 1010 可将认证码 130 通过电线、红外线、或射频信号发送到另一设备（诸如进行交易的个人计算机或终端）用于随后发送至授权端。在另一示例性实施例中，移动设备可通过（诸如无线通信网络、互联网、或上述组合之类的）通信网络将动态认证码直接发送至授权端的授权处理器。

另外，为了有助于标识为之生成认证码 130 的账户（例如，设备能够为与设备的用户或多个用户相关联的多个不同账户生成码的情况），认证码输出设备 1010 可向用户显示或发送增强名称（promotional name）、图案标记、或标识记号，以助于用户与设备交互，以选择合适的要为之生成动态码的账户。

现在回到图 1，（诸如加密密钥之类的）账户保密数据存储在授权处理器（未示出）可以访问的授权数据库中。保密数据对应于具体的与移动处理设备的用户相关联的金融账户（例如，信用或借记账户）。授权数据库较佳地仅可由授权处理器和/或维护该用户账户的银行或金融机构（典型地，本领域技术人员称为"发行"银行）访问。如果移动设备被窃或被危害，持有设备的人不能进行交易，因为没有某些其它的（诸如标识了应为货物或服务应向其记账的具体金融账户的主要账号（PAN））的金融账户标识符，由设备生成的授权码 130 不能被用于认证交易。

因此，在交易时，金融账户标识符 140 应用本领域技术人员熟知的各种技术来收集。例如，账户标识符 140 可存储在磁条式卡 145 或智能卡上，或通过小键盘、键盘、或其它输入设备由用户输入到设备中来收集。

Mastercard, Ex1002, p. 656

在步骤 150，动态授权码 130（与金融账户标识符数据 140 一起）被发送到（诸如授权处理器之类的）授权端。基于来自授权端的响应（步骤 160），交易在步骤 170 被授权或在步骤 180 被拒绝。

如上所述，授权过程可能需要使用与移动设备所执行的相同的数据和算法在授权端计算动态认证码，并将计算的结果与接收到的动态码作比较以确定计算的结果与接收到的码相匹配。该过程使用（诸如加密密钥之类的）与提供交易的金融账户标识符相关联的保密数据。在实施例中，分析授权端接收到的动态码以判断该码是否包含移动设备用来计算授权处理器不知道的应用密文的任何数据。例如，有可能移动设备用交易计数器来计算应用密文，其中则必须将该计数器同样提供给授权处理器，使它可以使用相同的数据来计算它的版本的应用密文。如前所述，虽然与具体账户或移动设备相关联的交易计数器的副本可以存储在授权数据库中，或者在授权端，但由于之前的没有被发送至授权处理器或授权数据库的失败交易，存储的计数器的副本可能与移动设备上的计数器不同步。因此，一旦授权处理器从动态认证码中所提供的数据中提取出或重生成任何必需的数据，授权处理器能使用之前所述的技术来计算动态授权码，所述技术包括用相关交易数据和（诸如与账户相关联的加密密钥之类的）保密账户信息来执行计算。接着如前所述的，将经计算的码与从移动设备接收到的动态码相比较。

一种将必要的程序和数据部署到移动处理设备中的示例性技术需要部署服务器。在本实施例中，移动设备的用户访问由用户的发行银行指定的网站，用户要求将动态认证码生成器应用安装在用户的移动设备上。用户被提示要求与应用和用户的移动设备标识符相关联的 PIN。用户还可被提示要求他或她的金融账户标识符，或者这一数据可通过某些其它方法来确定。（诸如加密密钥或密钥对之类的）账户保密数据被生成并与用户的金融账户标识符相关联。接着至少一部分该保密数据（例如加密密钥或密钥对中的一个或多个密钥）被存储在与用户的金融账户标识符相关联的授权数据库记录中。

Mastercard, Ex1002, p. 657

接着基于与之前生成的保密数据相关联的数据来生成个人化数据。例如，加密密钥或密钥对中的一个或多个密钥通过使用之前由用户输入的PIN和移动设备标识符来加密（如通过三重DES技术）作为临时密钥以生成个人化数据。接着，将个人化数据和任何其它的可执行程序文件从部署服务器发送到移动设备。该通信可通过用户的移动设备和（诸如PC之类的）另一计算机之间的直接连接来进行，或者通过使用移动或无线数据网络的空中（OTA）服务器来进行。接着，应用和个人化数据可被放置在移动设备的存储器中，如前所述的那样，在移动设备中它们可被用于生成动态认证码。账户保密数据和任何加密或个人化数据可在或者预定量的时间后或者应用和个人化数据被成功安装之后删去。然而，至少一部分保密数据仍然存储在授权数据库中以在之后的授权请求中使用。

在一实施例中，应用可以能由移动处理设备上安装的Javc虚拟机执行的Java程序的形式来提供。在一实施例中，为了进一步的安全性，Java程序命令可被搀混，例如通过使用俄亥俄州Cleveland的Preemptive Solutions公司的DashO。

图3显示了使用Java语言2090和Javc虚拟机（JVM）2080的本发明的示例性实施例的方框图。首先，移动设备用户使用（诸如小键盘或键盘之类的）接口2060来请求调用动态认证应用。接着JVM 2080调用M-CAP.jar沙箱（Sandbox）2020。JVM 2080提示用户输入PIN，该PIN接着从接口2060被接收。然后，Java应用的CAP生成器2030部分使用CAP数据2040根据之前描述的技术来生成8位的动态认证码。该8位码通过JVM 2080返回到电话用户接口2060。驻于电话存储器2010中的CAP数据2040或M-CAP JarSandbox 2020可通过例如来自http://www.bouncycastle.org/的用于J2ME的Bouncy Castle Crypto API来加密。

虽然本发明是结合某些较佳实施例来描述的，但本领域技术人员可以理解不背离本发明的精神或范围的各种修改、选择、和替换。本发明的许多其它应用对本领域普通技术人员是显而易见的。

Mastercard, Ex1002, p. 658

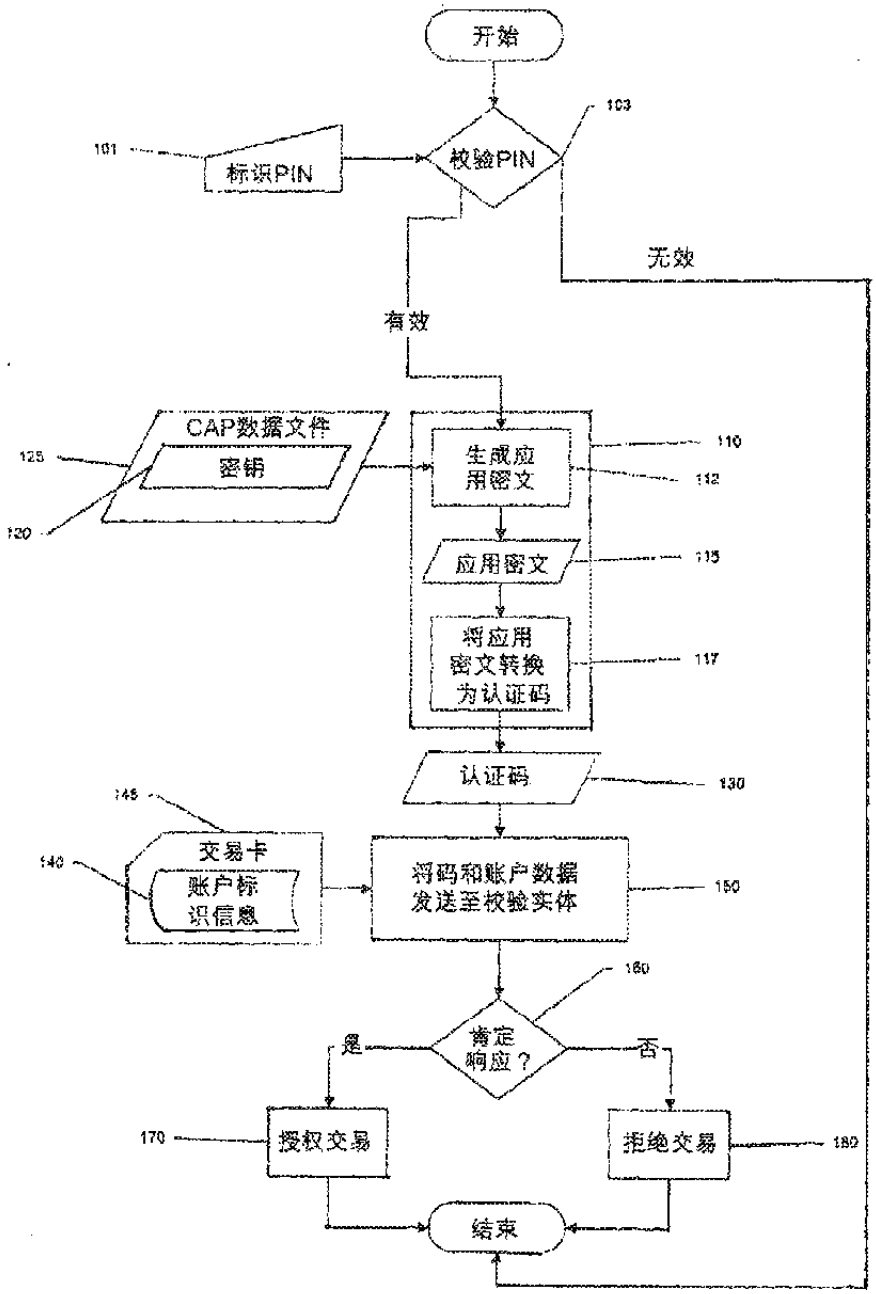


图 1

Mastercard, Ex1002, p. 659

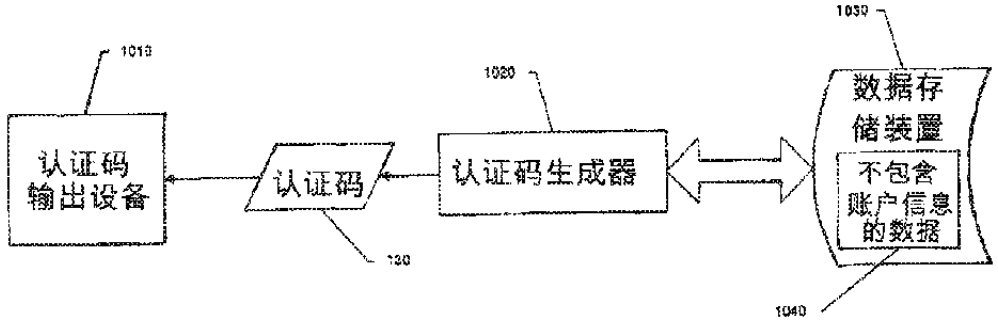


图 2

Mastercard, Ex1002, p. 660

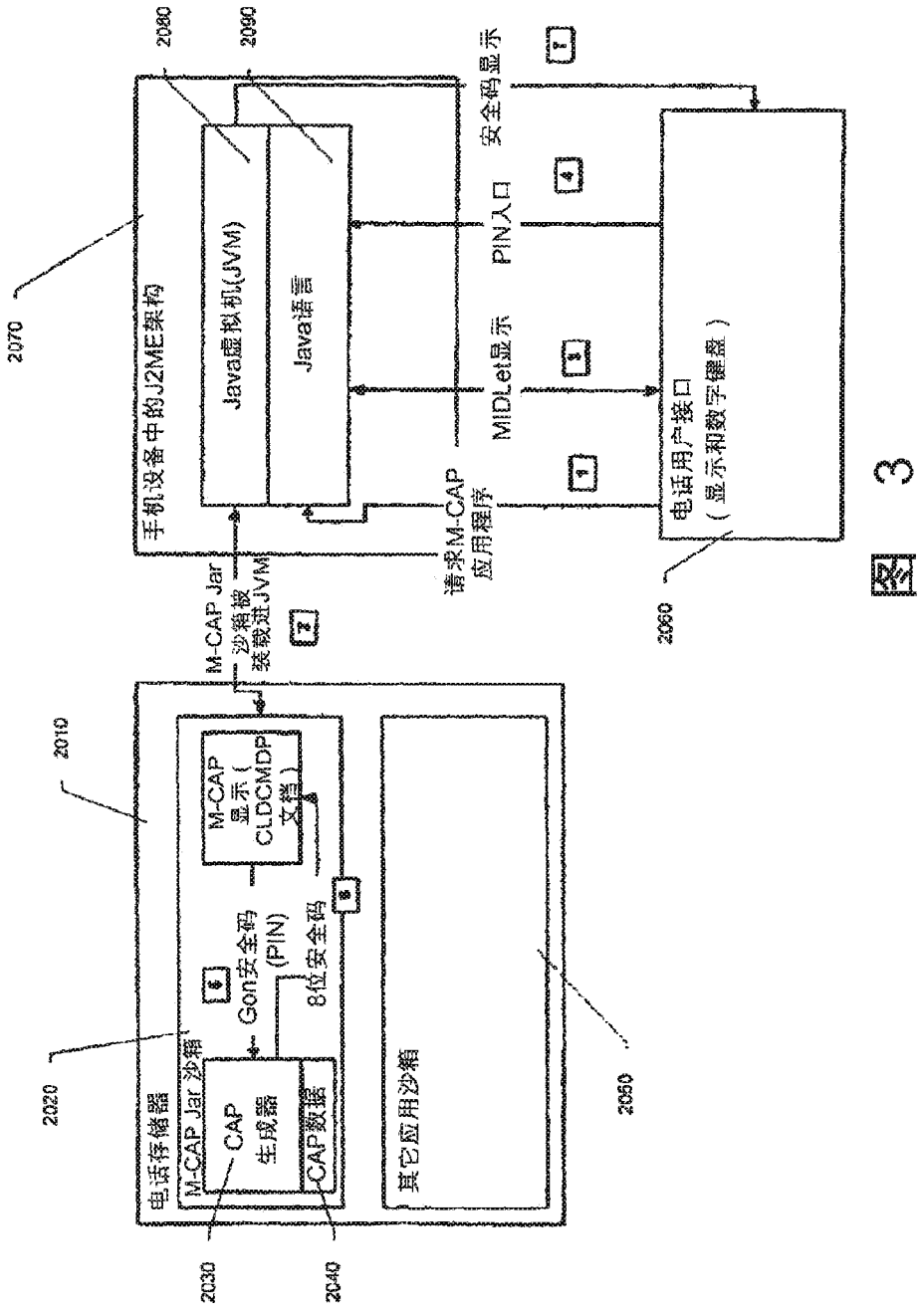


图 3

Mastercard, Ex1002, p. 661

Australian Government
IP Australia

P TM D PBR

ABN 38 113 072 755
P 1300 651 010
Int +61 2 6283 2999
www.ipaustralia.gov.au

Address: Pizzeys Patent and Trade Mark Attorneys
Pty Ltd
GPO Box 1374
BRISBANE QLD 4001
Australia

Date of issue: 22 November 2016

Patent Examination Report No. 1

Application Details

Patent Application No.:	2012301897
Applicant/s:	SimplyTapp, Inc.
Your reference:	42005SIM/WGB
Earliest Priority Date:	30 August 2011
Examination Request Date:	08 December 2015

Your application has been examined under Section 45 of the *Patents Act 1990*. I consider that the application does not meet the requirements of the Act for the reasons indicated below.

Actions you can take

NOTE: There is a current postponement of acceptance in place. If you overcome all other objections before the expiration of that postponement, the Commissioner will only accept the application at that time if you have filed a clear and unambiguous statement requesting the withdrawal of that postponement. Otherwise, a further adverse report will be issued.

You have **12 months** from the date of this report to overcome all my objection(s) otherwise your application will lapse.

You will also need to pay any annual continuation fees that apply. Information about fees may be obtained by phoning 1300 651 010 or by visiting www.ipaustralia.gov.au.

Basis of the report

In examining your application I have considered:

- the PCT pamphlet as originally filed

Statement of Novelty, Inventive Step and Patentable Subject Matter

Novelty/Inventive Step	Claim No. NONE Claim No. 1-29	Yes No
Patentable Subject Matter	Claim No. 1-29 Claim No. NONE	Yes No

Section 40 (Support, Disclosure, Clarity, Lack of Unity)

1 Claims 1-3, 8, 23 and 28 (and their dependencies) are not clear as they recite acronyms (such as POS and HSM) which have not been defined.

2 The invention defined by claim 3 (and dependencies) lacks support under subsection 40(3) because it omits the feature of a remote application system which appear necessary to perform the claimed invention.

In the absence of this feature the claimed invention is not sufficiently enabled because a remote application system is essential to the definition of the invention, since this is the third party which used verifying the correctness of the authorization data.

Documents Cited or Considered Relevant

D1 : US 2011099079 A1 (WHITE SPENCER NEIL) 28 April 2011 *
Category: **X** Claims: 3-12, 14-23, 27

D2 : US 2008040285 A1 (WANKMUELLER JOHN) 14 February 2008 **
Category: **X** Claims: 1, 2, 28
Category: **Y** Claims: 3-24, 27, 29

D3 : US 2004143550 A1 (CREAMER THOMAS E et al.) 22 July 2004 **
Category: **Y** Claims: 3-24, 27, 29

D4 : US 2007075133 A1 (YEAGER C. D) 05 April 2007 #
Category: **X** Claims: 1
Category: **Y** Claims: 2, 27

D5 : US 2010185545 A1 (ROYYURU VIJAY K et al.) 22 July 2010 #
Category: **Y** Claims: 3-7, 12-14, 17, 18, 24-27

D6 : US 2009006262 A1 (BROWN KERRY D et al.) 01 January 2009 #
Category: **Y** Claims: 3-7, 12-14, 17, 18, 24-27

D7 : US 2009124234 A1 (FISHER MICHELLE et al.) 14 May 2009 #
Category: **Y** Claims: 12-14, 18

D8 : US 2006022033 A1 (SMETS PATRICK et al.) 02 February 2006 #
Category: **Y** Claims: 2, 7, 17

D9 : US 2010207742 A1 (BUHOT THOMAS et al.) 19 August 2010 #
Category: **Y** Claims: 25

Cited in the International Search Report and the IPRP/IPRPII

Mastercard, Ex1002, p. 663

* Cited in the EP European search opinion dated 06 May 2015 for Publication No. 2751754.
** Cited in the US Examination Report dated 06 October 2015 for Publication No. 20130054474.

Special categories of cited documents:

X: The claimed invention cannot be considered novel under subsection 7(1) in light of the document and/or cannot be considered to involve an inventive step under subsection 7(2) of the Act in light of the common general knowledge considered together with the document.
Y: The claimed invention cannot be considered to involve an inventive step under subsection 7(2) of the Act in light of the common general knowledge when considered together with a combination of the document and one or more other such documents.

Novelty and Inventive Step

3 Claims 1, 2 and 28 are not novel and lack an inventive step in light of the prior art document D2 discussed in the section titled "Claim Rejections - 35 USC § 102" on pages 7-13 of the US Examination Report dated 06 October 2015 for Publication No. 20130054474.

While the objection regarding these documents was not made under Australian law, I agree with the reasons given in that report and consider that they support a corresponding objection against the Australian claims, the minor amendments notwithstanding.

4 The invention claimed in claims 3-24, 27 and 29 does not involve an inventive step in light of the prior art documents D2 and D3. The disclosures of these documents are discussed in the section titled "Claim Rejections - 35 USC § 103" on pages 14-42 of the US Examination Report dated 06 October 2015 for Publication No. 20130054474.

While the objection regarding these documents was not made under Australian law, I agree with the reasons given in that report and consider that they support a corresponding objection against the Australian claims the minor amendments notwithstanding. It is considered that in seeking a solution to the problem a person skilled in the art would be reasonably expected to combine the disclosures of these documents and arrive at a solution that is the same as the claimed invention.

5 Claims 3-12, 14-23 and 27 lack an inventive step in light of the prior art documents discussed at items 4.1-4.4.13 of the European search opinion dated 06 May 2015 for Publication No. 2751754 in relation to corresponding claims 1-21.

While the objection regarding these documents was not made under Australian law, I agree with the reasons given in that report and consider they support a corresponding objection against the Australian claims.

6 Furthermore:

Claim 1 is not novel and lacks an inventive step in light of the prior art document D4 discussed in Box V the IPRP dated 04 March 2014.

While the objection regarding these documents was not made under Australian law, I agree with the reasons given in that report and consider that they support a corresponding objection against the Australian claims, the minor amendments notwithstanding.

7 The invention claimed in claims 1-7, 12-14, 17-18, 24-27 does not involve an inventive step in light of the prior art documents D4-D9. The disclosures of these documents are discussed in Box V the IPRP dated 04 March 2014.

While the objection regarding these documents was not made under Australian law, I agree with the reasons given in that report and consider that they support a corresponding objection against the Australian claims. It is considered that in seeking a solution to the problem a person skilled in

Mastercard, Ex1002, p. 664

the art would be reasonably expected to combine the disclosures of these documents and arrive at a solution that is the same as the claimed invention.

How to contact us

Examiner: Peter Garay
ELEC 3 – Computing
Electrical
(02) 6283 2451

Corporate Telephone: 1300 651 010
(9am-5pm Mon- Fri)

Website: www.ipaustralia.gov.au

Mail: IP Australia
PO Box 200
Woden, ACT 2606

Website QR code

View your application in AusPat by going to http://www.ipaustralia.gov.au/auspat/ and entering your application number.

Did you know you can now submit over 150 service requests through IP Australia's eServices portal including Examination responses? For more information on how to register for eServices please visit us at www.ipaustralia.gov.au.

Mastercard, Ex1002, p. 665

CPEL1450577P

State Intellectual Property Office, P.R. China

Address : Receiving Section of the Chinese Patent Office, No. 6 Tucheng Road West, Haidian District, Beijing, Postal code: 100088

Applicant	SIMPLYTAPP, INC.			**Seal of Examiner**	**Date of Issue**
Agent	China Patent Agent (H.K.) Ltd.				June 22, 2016
Patent Application No.	201280053080.6	**Application Date**	August 30, 2012	**Exam Dept.**	
Title of Invention	SYSTEMS AND METHOD FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM				

First Office Action

(PCT application entering into the national phase)

1. ☑ Under the provision of Art. 35, para. 1 of the Patent Law, the examiner has made an examination as to substance of the captioned patent application for invention upon the request for substantive examination filed by the applicant.

   ☐ Under the provision of Art. 35, para. 2 of the Patent Law, the Chinese Patent Office has decided to conduct an examination of the captioned patent application for invention on its own initiative.

2. ☑ The applicant requests that
   the filing date August 30, 2011 at the US Patent Office be taken as the priority date of the present application,
   the filing date September 6, 2011 at the US Patent Office be taken as the priority date of the present application,
   the filing date March 26, 2012 at the US Patent Office be taken as the priority date of the present application,
   the filing date June 8, 2012 at the US Patent Office be taken as the priority date of the present application.

3. ☐ Through examination, the amended document(s) submitted by the applicant on ____ is/are not in conformity with the provision of Rule 51 of the Implementing Regulations of the Patent Law and is/are not accepted.

4. ☑ Examination is conducted on the Chinese version of the initially-submitted

Mastercard, Ex1002, p. 666

international application.

☐ Examination is conducted on the following document(s):

☐ page _____ of the description, based on the Chinese version of the initially-submitted international application documents;

page _____ of the description, based on the Chinese version of the annex to the international preliminary examination report;

page _____ of the description, based on the amended documents submitted according to the provision of Art. 28 or Art. 41 of the Patent Cooperation Treaty;

page _____ of the description, based on the amended documents submitted according to the provision of Rule 51 of the Implementing Regulations of the Patent Law.

☐ claim(s) _____ , based on the Chinese version of the initially-submitted international application documents;

claim(s) _____ , based on the Chinese version of the amended documents submitted according to the provision of Art. 19 of the Patent Cooperation Treaty;

claim(s) _____ , based on the Chinese version of the annex to the international preliminary examination report;

claim(s) _____ , based on the amended documents submitted according to the provision of Art. 28 or Art. 41 of the Patent Cooperation Treaty;

claim(s) _____ , based on the amended documents submitted according to the provision of Rule 51 of the Implementing Regulations of the Patent Law.

☐ Fig(s) _____ , based on the Chinese version of the initially-submitted international application documents;

Fig(s) _____ , based on the Chinese version of the annex to the international preliminary examination report;

Fig(s) _____ , based on the amended documents submitted according to the provision of Art. 28 or Art. 41 of the Patent Cooperation Treaty;

Fig(s) _____ , based on the amended documents submitted according to the provision of Rule 51 of the Implementing Regulations of the Patent Law.

5. ☑ The following reference document(s) is/are cited in this Office Action (its/their serial number(s) will continue to be used in the subsequent course of examination):

Serial No.	Number or Title(s) of Document(s)	Date of Publication (or filing date of interfering application)

Mastercard, Ex1002, p. 667

1	US2011090979A1	20110428
2	CN101048794A	20071003
3	US2010153721A1	20100617
4		

6. Concluding comments on the examination:

☐ On the description:

☐ What is stated in the application comes within the scope of that no patent right shall be granted as prescribed in Art. 5 of the Patent Law.

☐ The description is not in conformity with the provision of Art. 26, para. 3 of the Patent Law.

☐ The description is not in conformity with the provision of Art. 33 of the Patent Law.

☐ The drafting of description is not in conformity with the provision of Rule 18 of the Implementing Regulations.

☑ On the claims:

☐ Claim(s) _____ come(s) within the scope of that no patent right shall be granted as prescribed in Art. 25 of the Patent Law.

☐ Claim(s) _____ has/have no novelty as prescribed in Art. 22, para. 2 of the Patent Law.

☑ Claim(s) 1-29 has/have no inventiveness as prescribed in Art. 22, para. 3 of the Patent Law.

☐ Claim(s) _____ has/have no practical applicability as prescribed in Art. 22, para. 4 of the Patent Law.

☐ Claim(s) _____ is/are not in conformity with the provision of Art. 26, para. 4 of the Patent Law.

☐ Claim(s) _____ is/are not in conformity with the provision of Art. 31, para. 1 of the Patent Law.

☐ Claim(s) _____ is/are not in conformity with the provisions of Rule 20 of the Implementing Regulations.

☐ Claim(s) _____ is/are not in conformity with the provision of Art. 9 of the Patent Law.

☐ Claim(s) _____ is/are not in conformity with the provision of Rule 23 of the Implementing Regulations.

See the text portion of this Office Action for detailed analysis of the above concluding comments.

7. Based on the above concluding comments, the examiner deems that

☐ the applicant should make amendment to the application document(s) according

Mastercard, Ex1002, p. 668

to the requirements put forward in the text portion of this Office Action.

☐ the applicant should expound in his/its observations why the captioned patent application is patentable and make amendment to what is not in conformity with the provisions pointed out in the text portion of this Office Action, otherwise, no patent right shall be granted.

☑ the patent application contains no substantive content(s) for which a patent right may be granted. If the applicant has no sufficient reason(s) to state or his/its stated reason(s) is/are not sufficient, said application will be rejected.

8. The applicant should note the following items:

(1) Under Art. 37 of the Patent Law, the applicant should submit his/its observations within **four** months from the date of receipt of this Office Action; if, without any justified reason(s), the time limit for making written response is not met, said application shall be deemed to have been withdrawn.

(2) The amendment made by the applicant to said application should be in conformity with the provision of Art. 33 of the Patent Law, the amended text should be in duplicate and its form should conform with the related provisions of the Guide to Examination.

(3) If no arrangement is made in advance, the applicant and/or the agent shall not come to the Chinese Patent Office to have an interview with the examiner.

(4) The observations and/or amended text should be sent to the Receiving Section of the Chinese Patent Office by mail or by personal delivery, if not sent to the Receiving Section by mail or by personal delivery, the document(s) will have no legal effect.

9. This Office Action consists of the text portion totalling 8 page(s) and of the following attachment(s):

☐ _____ copy(copies) of the reference document(s) totalling _____ page(s).

Examination Dept. No. _____ Examiner _____

9016

Mastercard, Ex1002, p. 669

CPEL1450577P

Text of the First Office Action

Application number: 2012800530806

The present application relates to a system and method for authorizing a transaction with an unexpected cryptogram. After examination, the comments are hereby given as follows.

1. Claim 1 claims a method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction. D1 (US2011099079A1) discloses secure mobile-based financial transactions, and particularly discloses the following features (see paras. [0021]-[0033] of the Description): the sale terminal sends the amount to the mobile terminal, the mobile terminal submits a payment request including the payment number and the amount to the POS device, the payment number includes a one-time digital key and a random number, the one-time digital key is sent automatically from the payment server to the mobile terminal (equivalent to using a remote permanent cryptographic key to calculate an expected cryptogram that is expected to comprise at least a portion of the digital credential data, wherein the remote permanent cryptographic key is persistently stored at a remote source that is remote from the mobile device; performing an interrogation between the point-of-sale terminal and the mobile device comprising: sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device requesting the digital credential data; and sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal comprising the expected cryptogram as the at least a portion of the digital credential data); the

Mastercard, Ex1002, p. 670

payment server verifies the payment number and confirms the transaction to the POS device (equivalent to wherein the financial transaction being authorized). As the technical solution claimed by claim 1 is compared to the content disclosed by D1, the distinguishing feature is the following: and wherein the mobile device does not access a duplicate local permanent cryptographic key persistently stored locally to the mobile device. Based on the distinguishing feature, it can be determined that the problem actually solved by claim 1 is: how to acquire a cryptogram. However, on the basis that D1 discloses the payment server sending a one-time key, in order to realize security of payment, those skilled in the art conceive the mobile device not accessing a locally stored key, which is common technical means in the secure payment field.

It can be seen that it is obvious for those skilled in the art to obtain the technical solution claimed by claim 1 on the basis of D1 in combination with the common technical means in the art. Therefore, claim 1 neither possesses prominent substantive features nor represents a notable progress, and does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

2. Claim 2 is a dependent claim of claim 1. Its additional technical feature is disclosed by D1 (see paras. [0021]-[0033] of the Description): the payment server automatically sends the next digital key to the mobile terminal to be stored there until the next transaction is processed (equivalent to sending the remote permanent cryptographic key to the mobile device from the remote source; and transiently caching the remote permanent cryptographic key in the mobile device as a cached transient permanent cryptographic key); the sale terminal sends the amount to the mobile terminal (equivalent to the step of sending through the communication channel the at least one POS command communication comprising sending unpredictable data); the mobile terminal submits a

Mastercard, Ex1002, p. 671

payment request including the payment number and the amount to the POS device, the payment number includes a one-time digital key and a random number, the one-time digital key is input to a number generator algorithm to generate the payment number (equivalent to the step of sending through the communication channel the at least one POS command communication comprising sending a request for an expected cryptogram that is expected to be calculated by the mobile device, at least in part, from the unpredictable data; and the step of sending through the communication channel the at least one device response communication from the mobile device to the point-of-sale terminal comprising sending the expected cryptogram calculated, at least in part, from the unpredictable data and, at least in part, from the cached transient cryptographic key). Therefore, under the condition that claim 1 being referred to does not possess inventiveness, claim 2 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

3. Claim 3 claims a method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction. D1 discloses secure mobile-based financial transactions, and particularly discloses the following features (see paras. [0021]-[0033] of the Description): the sale terminal sends the amount to the mobile terminal to acquire the corresponding payment number and etc., the one-time digital key is input to a number generator algorithm to generate the payment number (equivalent to performing an interrogation between the point-of-sale terminal and the mobile device comprising: sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device, the at least one POS command communication comprising (a) a request for the digital credential data that is expected to comprise an expected cryptogram that is expected to be calculated, at least in part, from a permanent cryptographic key and (b) the unpredictable data); the mobile

Mastercard, Ex1002, p. 672

terminal submits a payment request including the payment number and the amount to the POS device (equivalent to sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal, the at least one device response communication comprising at least a portion of the digital credential data that comprises an unexpected cryptogram, substituted in place of the expected cryptogram); the payment server verifies the payment number and confirms the transaction to the POS device (equivalent to wherein the financial transaction being authorized). As the technical solution claimed by claim 3 is compared to the content disclosed by D1, the distinguishing feature is the following: an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data. Based on the distinguishing feature, it can be determined that the problem actually solved by claim 3 is: how to generate an expected cryptogram.

D2 (CN101048794A) discloses a method for authorizing a transaction using a dynamic authorization code, and particularly discloses the following feature (see line 1, page 4-line 28, page 5 and line 1, page 8-line 19, page 9 of the Description): the unpredictable data includes the transaction amount and etc., the device uses the unpredictable data together with other secret data to generate a dynamic authorization code (equivalent to an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data). The feature performs the same function in D2 as it performs in claim 3, both generating a cryptogram using unpredictable data, that is, those skilled in the art can get inspiration and apply the method of generating a cryptogram in D2 to the payment number generation process of D1. It can be seen that it is obvious for those skilled in the art to obtain the technical solution claimed by claim 3 on the basis of D1 in combination with D2. Therefore, claim 3 neither possesses prominent substantive features nor represents a notable

Mastercard, Ex1002, p. 673

progress, and does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

4. Claims 4-5 are dependent claims of claim 3. Their additional technical features are disclosed by D2 (see line 1, page 4-line 28, page 5 and line 1, page 8-line 19, page 9 of the Description): the unpredictable data may be a random number, can be based on the current time, a one-way hash of the proposed transaction amount, some combination thereof. Therefore, under the condition that claim 3 being referred to does not possess inventiveness, claims 4-5 do not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

5. Claim 6 is a dependent claim of claim 3. Its additional technical feature is disclosed by D1 (see paras. [0021]-[0033] of the Description): the payment server automatically sends the next digital key to the mobile terminal to be stored there until the next transaction is processed. Therefore, under the condition that claim 3 being referred to does not possess inventiveness, claim 6 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

6. Claim 7 is a dependent claim of claim 6. Its additional technical feature is disclosed by D1 (see paras. [0021]-[0033] of the Description): the one-time digital key is input to a number generator algorithm to generate the payment number. Therefore, under the condition that claim 6 being referred to does not possess inventiveness, claim 7 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

7. Claim 8 is a dependent claim of claim 6. D3 (US2010153721A1) discloses a method for accessing remote secure elements, and particularly discloses the following feature (see paras. [0006]-[0007] and [0029]-[0042] of the Description): the portable electronic device includes

Mastercard, Ex1002, p. 674

a virtual secure element module, which is configured to communicate with one or more remote secure element servers, the secure element (equivalent to an HSM) is located on the remote secure element server (equivalent to a remote application system). The feature performs the same function in D3 as it performs in claim 8, both generating a cryptogram using a remote secure module, that is, those skilled in the art can get inspiration and apply the method of generating a cryptogram in D3 to the payment number generation process of D1. On said basis, those skilled in the art easily conceive generating unpredictable data by a remote application system and sending it to an HSM to generate a predetermined cryptogram so as to send it directly to the mobile device. It can be seen that it is obvious for those skilled in the art to obtain the technical solution claimed by claim 8 on the basis of D1 in combination with D2, D3 and the common technical means in the art. Therefore, under the condition that claim 6 being referred to does not possess inventiveness, claim 8 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

8. Claim 9 is a dependent claim of claim 6. Its additional technical feature is disclosed by D1 (see paras. [0021]-[0033] of the Description): the payment server generates a one-time digital key and sends it to the mobile terminal, the mobile terminal generates a payment number based on the one-time digital key. Therefore, under the condition that claim 6 being referred to does not possess inventiveness, claim 9 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

9. Claim 10 is a dependent claim of claim 6. Its additional technical feature is disclosed by D2 (see line 1, page 4-line 28, page 5 and line 1, page 8-line 19, page 9 of the Description): unpredictable data that the user will enter into his or her mobile processing device, which will subsequently be used to generate the dynamic authentication code,

Mastercard, Ex1002, p. 675

typically in conjunction with other data such as an encryption key. Therefore, under the condition that claim 6 being referred to does not possess inventiveness, claim 10 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

10. Claim 11 is a dependent claim of claim 6. D2 discloses the following feature (see line 1, page 4-line 28, page 5 and line 1, page 8-line 19, page 9 of the Description): unpredictable data that the user will enter into his or her mobile processing device, which will subsequently be used to generate the dynamic authentication code, typically in conjunction with other data such as an encryption key. Moreover, card risk management data is common critical data, determining the unexpected cryptogram based on the card risk management data is common technical means in the secure payment field. Therefore, under the condition that claim 6 being referred to does not possess inventiveness, claim 11 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

11. Claims 12-13 are dependent claims of claim 6. (Omitted, for the additional technical features pertain to the disclosure of D1). Therefore, under the condition that claim 6 being referred to does not possess inventiveness, claims 12-13 do not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

12. Claim 14 is a dependent claim of claim 6. (Omitted, for the additional technical feature pertains to the disclosure of D1). Therefore, under the condition that claim 6 being referred to does not possess inventiveness, claim 14 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

13. Claim 15 is a dependent claim of claim 6. (Omitted, for the additional

Mastercard, Ex1002, p. 676

technical feature pertains to the disclosure of D2 and the common technical means in the art). Therefore, under the condition that claim 6 being referred to does not possess inventiveness, claim 15 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

14. Claim 16 is a dependent claim of claim 6. (Omitted, for the additional technical feature pertains to the disclosure of D2 and the common technical means in the art). Therefore, under the condition that claim 6 being referred to does not possess inventiveness, claim 16 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

15. Claim 17 is a dependent claim of claim 3. (Omitted, for the additional technical feature pertains to the disclosure of D1). Therefore, under the condition that claim 3 being referred to does not possess inventiveness, claim 17 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

16. Claim 18 is a dependent claim of claim 3. (Omitted, for the additional technical feature pertains to the disclosure of D1 and the common technical means in the art). Therefore, under the condition that claim 3 being referred to does not possess inventiveness, claim 18 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

17. Claim 19 is a dependent claim of claim 3. (Omitted, for the additional technical feature pertains to the disclosure of D1). Therefore, under the condition that claim 3 being referred to does not possess inventiveness, claim 19 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

Mastercard, Ex1002, p. 677

18. Claim 20 is a dependent claim of claim 3. (Omitted, for the additional technical feature pertains to the disclosure of D1). Therefore, under the condition that claim 3 being referred to does not possess inventiveness, claim 20 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

19. Claim 21 is a dependent claim of claim 3. (Omitted, for the additional technical feature pertains to the disclosure of D1 and the common technical means in the art). Therefore, under the condition that claim 3 being referred to does not possess inventiveness, claim 21 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

20. Claim 22 is a dependent claim of claim 21. (Omitted, for the additional technical feature pertains to the disclosure of D1 and D2, is easily conceived by those skilled in the art on said basis and pertains to the common technical means in the art). Therefore, under the condition that claim 21 being referred to does not possess inventiveness, claim 22 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

21. Claim 23 is a dependent claim of claim 3. (Omitted, for the additional technical feature pertains to the disclosure of D1 and D3, and is easily conceived by those skilled in the art on said basis). Therefore, under the condition that claim 3 being referred to does not possess inventiveness, claim 23 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

22. Claim 24 is a dependent claim of claim 3. (Omitted, for the additional technical feature pertains to the disclosure of D1). Therefore, under the

Mastercard, Ex1002, p. 678

condition that claim 3 being referred to does not possess inventiveness, claim 24 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

23. Claim 25 is a dependent claim of claim 3. (Omitted, for the additional technical feature pertains to the common technical means in the art). Therefore, under the condition that claim 3 being referred to does not possess inventiveness, claim 25 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

24. Claim 26 is a dependent claim of claim 3. (Omitted, for the additional technical feature pertains to the disclosure of D1). Therefore, under the condition that claim 3 being referred to does not possess inventiveness, claim 26 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

25. Claim 27 is a dependent claim of claim 3. (Omitted, for the additional technical feature pertains to the disclosure of D1).

26. Claim 28 claims a method for acquiring digital credential data by a point-of-sale terminal from a secure mobile device for authorization of a financial transaction. D1 discloses secure mobile-based financial transactions, and particularly discloses the following features (see paras. [0021]-[0033] of the Description): the sale terminal sends the amount to the mobile terminal to acquire the corresponding payment number and etc., the one-time digital key is input to a number generator algorithm to generate the payment number (equivalent to performing an interrogation between the point-of-sale terminal and the secure mobile device comprising: sending through a communication channel at least one POS command communication from the point-of-sale terminal to the secure mobile device, the at least one POS command communication comprising

Mastercard, Ex1002, p. 679

(a) a request for the digital credential data that is expected to comprise an expected cryptogram that is expected to be calculated, at least in part, from a permanent cryptographic key and (b) the unpredictable data); the mobile terminal submits a payment request including the payment number and the amount to the POS device (equivalent to sending through the communication channel at least one device response communication from the secure mobile device to the point-of-sale terminal, the at least one device response communication comprising at least a portion of the digital credential data that comprises the expected cryptogram); the mobile terminal sends the transaction amount to the payment server (equivalent to in a step that follows the step of performing an interrogation, a secure mobile device transmitting step comprising sending over a second communication channel the unpredictable data from the secure mobile device to a remote application system); the POS device sends the payment number to the payment server (equivalent to in a step that follows the step of performing an interrogation, a point-of-sale terminal transmitting step comprising sending over a third communication channel an authorization request from the point of sale terminal to the remote application system, the authorization request comprising the expected cryptogram); the payment server performs verification and authorization, verifying whether the cryptogram is correct (equivalent to in a step that follows the secure mobile device transmitting step and the point-of-sale terminal transmitting step, a corroborative authorizing step comprising: verifying a correctness of the expected cryptogram by the application system); upon verification pass, the payment server sends the authorization information to the POS device and confirms the transaction (equivalent to sending through the third communication channel an authorization response from the remote application system to the point-of-sale terminal wherein data contained in the authorization response is determined at least in part by the verifying of the correctness of the expected cryptogram; wherein the financial

Mastercard, Ex1002, p. 680

transaction is authorized). As the technical solution claimed by claim 28 is compared to the content disclosed by D1, the distinguishing feature is the following: an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data; the point-of-sale terminal sending the unpredictable data; verifying a correctness of the unpredictable data by the application system by comparing the unpredictable data sent over the second communication channel with the unpredictable data sent over the third communication channel; (data contained in the authorization response being determined) at least in part, by the verifying of the correctness of the unpredictable data. Based on the distinguishing feature, it can be determined that the problem actually solved by claim 28 is: how to generate and verify an expected cryptogram.

D2 (CN101048794A) discloses a method for authorizing a transaction using a dynamic authorization code, and particularly discloses the following feature (see line 1, page 4-line 28, page 5 and line 1, page 8-line 19, page 9 of the Description): the unpredictable data includes the transaction amount and etc., the device uses the unpredictable data together with other secret data to generate a dynamic authorization code (equivalent to an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data). The feature performs the same function in D2 as it performs in claim 3, both generating a cryptogram using unpredictable data, that is, those skilled in the art can get inspiration and apply the method of generating a cryptogram in D2 to the payment number generation process of D1. Moreover, D1 discloses verifying the correctness of the one-time digital key and the random number, on said basis, those skilled in the art easily conceive verifying the correctness of the unpredictable data.

It can be seen that it is obvious for those skilled in the art to obtain the

Mastercard, Ex1002, p. 681

technical solution claimed by claim 28 on the basis of D1 in combination with D2 and the common technical means in the art. Therefore, claim 28 neither possesses prominent substantive features nor represents a notable progress, and does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

27. Claim 29 is a dependent claim of claim 28. (Omitted, for the additional technical feature pertains to the disclosure of D1 and D2, is easily conceived by those skilled in the art on said basis, and pertains to the common technical means in the art). Therefore, under the condition that claim 28 being referred to does not possess inventiveness, claim 29 does not possess inventiveness as prescribed in Art. 22, para. three of the Patent Law.

Based on the reasons stated above, none of the independent and dependent claims of the present application possesses inventiveness, meanwhile, the Description does not recite any other substantive content that can be granted a patent right. It is not hopeful for the present application to be granted a patent right. If the applicant cannot provide sufficient reasons within the time limit for response as specified in the Office Action, the present application will be rejected.

Mastercard, Ex1002, p. 682

CPEL1450577P

State Intellectual Property Office of People's Republic China

Search Report

Application No.: 201280053080.6	Filing Date: August 30, 2012	☑ First Search ☐ Supplementary Search
Applicant: SIMPLYTAPP, INC.	Earliest Priority: August 30, 2011	
Number of Claims: 29	Paragraphs of Description: 204	
IPC Class Allotted by Examiner: G06Q20/32, G06Q20/40		
Search Findings (Information of Key Words or Characters for Search): Database: CNABS, DWPI, SIPOABS, CNKI, GOOGLE; Actually searched Class: G06Q20/+, G06Q50/+, G06F21/+; Keywords: 交易，授权，数字凭证，密码，密钥，远程，移动终端，销售点终端，transaction, authorization, digital credit, key, remote, long-distance, mobile, POS		

Relevant Patent Documents

Category	Country & Reference No. Shown in [11]	Date Shown in [43] or [45]	IPC No.	Related Paragraphs and/or Figs	Related Claims
X	US2011099079A1	20110428	G06Q50/00	paras. [0021]-[0033] of the Description	1-2
Y	US2011099079A1	20110428	G06Q50/00	paras. [0021]-[0033] of the Description	3-29
Y	CN101048794A	20071003	G06Q99/00	line 1, page 4-line 28, page 5 and line 1, page 8-line 19, page 9 of the Description	3-29
Y	US2010153721A1	20100617	G06F21/20	paras. [0006]-[0007] and [0029]-[0042] of the Description	8

310401
2010.2

A	US2002026414A1	20020228	G06Q50/00	full text	1-29
A	US2011125638A1	20110526	G06Q20/04	full text	1-29
A	US2009037285A1	20090205	G06Q20/00	full text	1-29
A	US2009124234A1	20090514	H04M11/00	full text	1-29
A	CN101248646A	20080820	H04L29/08	full text	1-29
A	US2010185545A1	20100722	H04L9/30	full text	1-29
A	US2009006262A1	20090101	H04L9/00	full text	1-29
A	CN101019126A	20070815	G06K5/00	full text	1-29

310401
2010.2

Relevant Non-Patent Documents					
Category	Title of Book (Version & Volume)	Date of Publication	Name of Author & Publisher	Related Pages	Related Claims
Type	Title of Periodicals or Abstract (Version & Issue No.)	Date of Issuance	Author's Name & Title of Article	Related Pages	Related Claims

Remarks:

1. The IPC classification number of the field where the examiner has made the search should be indicated in the place of a main group and/or sub-group of the classification.

2. Abbreviation of the title of a periodical or any other periodical publication may be used that conforms to the generally accepted international practice.

3. Explanation of the types of relevant documents:

X: A document that will alone affect the novelty or inventive step of the invention.

Y: Documents that, combining with the other type-Y documents cited in the same search report, will affect the inventive step of the invention.

A: Documents that define the general state of the art.

R: A patent or a patent application relating to the identical invention and filed by any entity or individual with SIPO on the filing date of the invention.

P: Intermediate documents published prior to the filing date of the application, but later than the priority date claimed.

E: A conflicting application.

Examiner: He Longping

Examining Department: Examination department for electrical invention of Patent Examination Cooperation Center, Sichuan

Date: June 14, 2016

Mastercard, Ex1002, p. 685

Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
Postbus 5818
2280 HV Rijswijk
NETHERLANDS
Tel: +31 70 340 2040
Fax: +31 70 340 3016

Boult Wade Tennant
Verulam Gardens
70 Gray's Inn Road
London WC1X 8BT
ROYAUME-UNI

Formalities Officer
Name: Berthon, Claude
Tel: +31 70 340 - 1001
or call
+31 (0)70 340 45 00

Substantive Examiner
Name: Horan, David
Tel: +31 70 340 - 3112

Application No	Ref.	Date
12 827 025.1 - 1955	PEH/P131279EP00	10.06.2016
Applicant: SimplyTapp, Inc.		

Communication pursuant to Article 94(3) EPC

The examination of the above-identified application has revealed that it does not meet the requirements of the European Patent Convention for the reasons enclosed herewith. If the deficiencies indicated are not rectified the application may be refused pursuant to Article 97(2) EPC.

You are invited to file your observations and insofar as the deficiencies are such as to be rectifiable, to correct the indicated deficiencies within a period

of 4 months

from the notification of this communication, this period being computed in accordance with Rules 126(2) and 131(2) and (4) EPC. One set of amendments to the description, claims and drawings is to be filed within the said period on separate sheets (R. 50(1) EPC).

If filing amendments, you must identify them and indicate the basis for them in the application as filed. Failure to meet either requirement may lead to a communication from the Examining Division requesting that you correct this deficiency (R. 137(4) EPC).

Failure to comply with this invitation in due time will result in the application being deemed to be withdrawn (Art. 94(4) EPC).

Registered letter
EPO Form 2001 12.10CSX

Horat, David
Primary Examiner
For the Examining Division

Enclosure(s): 4 page/s reasons (Form 2906)

Datum Date Date	10.06.2016	Blatt Sheet Feuille	1	Anmelde-Nr: Application No: Demande n°:	12 827 026.1

The examination is being carried out on the **following application documents**

Description, Pages

1, 3, 4, 6-82	as published	
5, 5a-5k	filed in electronic form on	10-11-2014
2	filed in electronic form on	23-03-2016

Claims, Numbers

1-21	filed in electronic form on	23-03-2016

Drawings, Sheets

1/24-24/24	as published	

1 Cited Documents

1.1 Reference is made to the following documents; the numbering will be adhered to in the rest of the procedure.

D1 US 2011/099079 A1 (WHITE SPENCER NEIL [US])
28 April 2011 (2011-04-28)

D2 WO 01/08113 A1 (VISA INT SERVICE ASS [US]; DAVIS VIRGIL M [US]; CUTINO SUZANNE C [US];)
1 February 2001 (2001-02-01)

D3 US 2010/153721 A1 (MELLQVIST ANDERS [SE])
17 June 2010 (2010-06-17)

D4 WO 2009/017754 A1 (EBAY INC [US]; MURPHY TIMOTHY [US]) 5 February 2009 (2009-02-05)

D5 US 2002/026414 A1 (NAKAJIMA MITSURU [JP] ET AL)
28 February 2002 (2002-02-28)

2 **Amendments (Art. 123(2) EPC)**

2.1 With the letter received on 23-03-2016, the applicant submitted information about the some background in payment card technology as basis when dealing with Article 123(2) EPC.

Nevertheless, the first examiner would like to clarity that Article 123(2) EPC is about the European patent application which may not be amended in such a way that it contains subject-matter which extends beyond the content of the application as filed.

Moreover, the fact that a certain technology is well-known in the field, does not mean that it is implicit or directly and unambiguously derivable from the application as filed.

Unfortunately, with the letter received on 23-03-2016, the applicant has filed amendments which do not appear to meet the requirements of Article 123(2) based on the reasons provided. The examiner would like to request the applicant to show which part of the application forms the basis for each of the changes made.

2.2 Moreover, some of the previously objections under Article 123(2) EPC are still outstanding:

2.2.1 Claim 8 (former claim 11) has been amended to include the fact that "the unexpected cryptogram comprises the unpredictable cryptogram". Nevertheless, the paragraphs cited in the letter, i.e. [0116] and [0118], do not describe the unpredictable cryptogram and description [0117] describes that the unpredictable cryptogram refers to a type of unexpected cryptogram. Thus, there is no basis for one comprising the other.

2.2.2 The same reasoning applies mutatis mutandis to claims 9 and 10 (former claims 12 and 13).

2.2.3 Claims 9 and 10 (former claims 12 and 13) also have been amended to include "calculating a plurality of unpredictable cryptograms". In the letter it is specified that there is a step of logically determining which unpredictable cryptogram to use and thus a plurality of these must be calculated using the temporary cryptographic key. Nevertheless, there are several possibilities about the origin of such cryptograms and not necessarily using the temporary cryptographic key, since there could be other unexpected cryptograms with other keys. Thus, there is no basis for such amendments.

3 **Clarity and Conciseness (Art. 84 EPC)**

3.1 The use of vague words, such as for instance in claim 21 "expected cryptogram", makes the reading of the claims unclear and, hence, does not meet the requirements of Article 84 EPC. These words should be amended to include the technical features which are disclosed in the description paragraphs [0116]-[0118] in order for such words to have a technical meaning.

3.2 Moreover, several claims contain the word HSM which is vague and unclear and thus should be amended to be in line with Article 84 EPC. In general, abbreviations should not be used for the claims unless there is no alternative. For the purpose of this report, the examining division will interpret it as in description [0040], being "Hardware Security Module".

3.3 Independent claim 1 does not meet the requirement following from Article 84 EPC, taken in combination with Rule 43(1) and (3) EPC, that any independent claim must contain all the technical features essential to the definition of the invention because it is clear from the description on paragraphs [0007] and [0137]-[0139] that the feature of a remote application system is essential to the definition of the invention, since this is the third party which authorizes the financial transaction by verifying the correctness of the received data.

4 **Novelty and Inventive Step (Art. 52(1), 54 and 56 EPC)**

4.1 The examiner would like to point out that due to the large amount of issues under Article 123(2) EPC and Article 84 EPC, a proper assessment of Articles 54 and 56 EPC could not be made.

4.2 Nevertheless, the examiner is of the opinion that once these problems have been solved, the application would still lack an inventive step under Article 56 EPC as for the reasons already presented in the European Search Opinion.

5 **Procedure**

5.1 It is not at present apparent which part of the application could serve as a basis for a new, allowable claim. Should the applicant nevertheless regard some particular matter as patentable, an independent claim should be filed taking account of Rule 43(1) EPC. The applicant should also indicate how the subject-matter of the new claim differs from the state of the art and the significance thereof.

5.2 When filing amended claims the applicant should at the same time bring the description into conformity with the amended claims. Care should be taken during revision, especially of the introductory portion and of any statements of problem or advantage, not to add subject-matter which extends beyond the content of the application as originally filed (Article 123(2) EPC).

5.3 In order to comply with the requirements of Rule 137(4) EPC, the applicant should clearly identify the amendments made, irrespective of whether they concern amendments by addition, replacement or deletion, and indicate the passages of the application as filed on which these amendments are based (Guidelines H-III, 2.1).

5.4 According to the application of Rule 50(1) EPC in combination with Rule 49(8) EPC, no hand-written amendments by the applicant are accepted (Office Journal of the EPO 2013, 603-604).

5.5 The independent claim is not in the two-part form in accordance with Rule 43 (1) EPC, which in the present case would be appropriate, with those features known in combination from the prior art being placed in the preamble (Rule 43 (1)(a) EPC) and the remaining features being included in the characterising part (Rule 43(1)(b) EPC).

5.6 The features of the claims should be provided with reference signs placed in parentheses to increase the intelligibility of the claims (Rule 43(7) EPC). This applies to both the preamble and characterising portion (see Guidelines F-IV, 4.19).

Office de la propriété intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An Agency of Industry Canada

4 November 2016 (04-11-2016)

GOWLING WLG (CANADA) LLP
2600 - 160 Elgin Street
OTTAWA Ontario
K1P 1C3

Application No.	:	**2,846,462**
PCT No.	:	**US2012053129**
Owner	:	SIMPLYTAPP, INC.
Title	:	**SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM**
Classification	:	G06Q 20/40 (2012.01)
Your File No.	:	**08927357CA**
Examiner	:	Kazem Ziaie

YOU ARE HEREBY NOTIFIED OF A REQUISITION BY THE EXAMINER IN ACCORDANCE WITH SUBSECTION 30(2) OF THE *PATENT RULES*. IN ORDER TO AVOID ABANDONMENT UNDER PARAGRAPH 73(1)(*a*) OF THE *PATENT ACT*, A WRITTEN REPLY MUST BE RECEIVED WITHIN THE **SIX (6)** MONTH PERIOD AFTER THE ABOVE DATE.

This application has been examined taking into account the:

Description,	pages 1-82, as originally filed;
Claims,	1-63, as received on 3 September 2015 (03-09-2015) during the national phase; and
Drawings,	pages 1-24, as originally filed.

The number of claims in this application is 63.

A search of the prior art has thus far failed to reveal any pertinent references.

The examiner has identified the following defects in the application:

Miscellaneous

The description contains a statement that incorporates by reference another document and does not comply with subsection 81(1) of the *Patent Rules*. Such a statement is found at paragraph 0051 and should be removed.

The abstract does not comply with section 79 of the *Patent Rules*. The present abstract on file fails to allow a clear understanding of the technical problem, the gist of the solution of that problem

through the alleged invention, and the principal use or uses of the alleged invention. The applicant is advised to refer to section 79 of the *Patent Rules*, where the specifications of an acceptable abstract are outlined. Note that an abstract should be within 150 words.

In view of the foregoing defects, the applicant is requisitioned, under subsection 30(2) of the *Patent Rules*, to amend the application in order to comply with the *Patent Act* and the *Patent Rules* or to provide arguments as to why the application does comply.

Under section 34 of the *Patent Rules*, any amendment made in response to this requisition must be accompanied by a statement explaining the nature thereof, and how it corrects each of the above identified defects.

Kazem Ziaie
Patent Examiner
819-639-8376

As per CIPO Client Service Standards, a response to a telephone enquiry or voice mail should be provided by the end of the next business day. In the event that attempts to reach the examiner are unsuccessful, the examiner's Section Head, Eric Lafontaine, can be reached at 819-635-3356.

CIPO values your feedback and invites you to complete a short and anonymous ongoing survey on patent examination products and services. You can access the survey at the following link: http://ic.sondages-surveys.ca/s/SCB-OPS/langeng.

The Examination Search Report is provided for reference only and is not part of any requisition made by the examiner in accordance with the *Patent Act* or *Rules*. The applicant is not required to respond to the information contained in the Examination Search Report.

Examination Search Report

Box I: General Information

Application No.	2,846,462	Search Report Date	2016-08-02
Title	SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM		
Examiner	Kazem Ziaie	Search Conducted?	Yes

Box II: Family Prosecution

Family Member	File Wrapper Reviewed	Status of Prosecution
US2012317628 A1	2016-08-02	In Progress
EP 2 751 754 A4	2016-08-02	In Progress

Box III: Search History

Claims Searched	1-63	Date of Search	2016-08-02

Type of Search Conducted (select all that apply):

Canadian first to file search	■	Supplemental/top up search	□
Inventor/applicant search	□	Non laid open search	□
Comprehensive search	■	In-house searcher	□

Search History from Databases Consulted:

```
##### CANADIAN PATENT DATABASE/INTELLECT ##########
(crypt* <IN> claims) <AND> (transaction <IN> claims) <AND> (mobile <IN> claims)

##### QUESTEL-ORBIT ##########
( ((CRYPT+ W KEY))/CLMS AND (TRANSACTION)/CLMS AND (MOBILE)/CLMS AND (TERMINAL)/CLMS )
( ((CRYPT+ W KEY))/CLMS AND (TRANSACTION)/CLMS AND (MOBILE)/CLMS )
```

Version 8

Electronic Acknowledgement Receipt

EFS ID:	28261996
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Customer Number:	44654
Filer:	John L. Adair/Shenise Ramdeen
Filer Authorized By:	John L. Adair
Attorney Docket Number:	STAPP1100-5
Receipt Date:	03-FEB-2017
Filing Date:	30-AUG-2012
Time Stamp:	16:30:31
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		STAPP1100-5_IDS02-03-17.pdf	124719 6c4fae2a4f599e302f84a771ca34f8e60edfc20	yes	4

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	2	
	Information Disclosure Statement (IDS) Form (SB08)		3	4	
Warnings:					
Information:					
2	Foreign Reference	STAPP1100_Ref_B3.pdf	18230035 17135b3f3ebed5e9c251365993d84d70a90227c1	no	17
Warnings:					
Information:					
3	Non Patent Literature	STAPP1100_Ref_C8.pdf	174811 2bcdeaa1ef8bab0d7ac86eda8131f090839498ba	no	4
Warnings:					
Information:					
4	Non Patent Literature	STAPP1100_Ref_C9.pdf	11983199 79e261e9540ed80da36439a129f5240d555f4e9f6	no	20
Warnings:					
Information:					
5	Non Patent Literature	STAPP1100_Ref_C10.pdf	618488 4279603a24b95a3f24e81d62b506c12f491f6e2c	no	6
Warnings:					
Information:					
6	Non Patent Literature	STAPP1100_Ref_C11.pdf	134134 9076458d001954c339eb255158a568e516e53356	no	3
Warnings:					
Information:					
		Total Files Size (in bytes):	31265386		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. (Opt.) **STAPP1100-5**

First Named Inventor **C. Douglas Yeager**	
Application Number **13/599,647**	Date Filed **August 30, 2012**
Title **SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE (as amended)**	
Group Art Unit **3695**	Examiner **Puttaiah, Asha**
Confirmation Number **1919**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certification of Transmission Under 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on **February 3, 2017**.

Shenise Ramdeen

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. A copy of foreign patent documents as well as the information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

☐ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☐ This Information Disclosure Statement is being submitted before the mailing of a first Office action on the merits; or

☒ This Information Disclosure Statement is being submitted before the mailing of a first Office action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

Furthermore, pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application.

Applicant does not believe any fees are due and owing at this time. If Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

SPRINKLE IP LAW GROUP
Attorneys for Applicant

/John L. Adair/

John L. Adair
Reg. No. 48,828

Dated: February 3, 2017

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 317-9088

INFORMATION DISCLOSURE STATEMENT				Application Number	13/599,647
				Filing or 371 (c) Date:	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	Puttaiah, Asha
Sheet	1	of	1	Attorney Docket Number	STAPP1100-5

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C12	Office Action issued for Chinese Patent Application No. 201280053080.6, mailed March 7, 2017, 24 pages.	

Examiner Signature		Date Considered	

CPEL1450577P

State Intellectual Property Office, P.R. China

Address : Receiving Section of the Chinese Patent Office, No. 6 Tucheng Road West, Haidian District, Beijing, Postal code: 100088

Applicant	SIMPLYTAPP, INC.			**Date of Issue**
Agent	China Patent Agent (H.K.) Ltd.			March 7, 2017
Patent Application No.	201280053080.6	**Application Date**	August 30, 2012	
Title of Invention	SYSTEMS AND METHOD FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM			

2nd *Office Action*

1. ☑ The examiner has received the Observations, submitted by the applicant on December 22, 2016 in response to the 1st Office Action issued by the Patent Office, and on this basis continued to conduct examination as to substance of the captioned patent application.
   ☐ On the basis of the Reexamination Decision made by the Reexamination Board of the Chinese Patent Office on _____ , the examiner has continued to conduct examination as to substance of the captioned patent application.
   ☐

2. Further examination has been conducted in the light of the following application document(s):
   ☐ the amended application document(s) attached to the said observations.
   ☑ the application document(s) at which the previous Office Action is directed, and the replacement sheet(s) of the amended application document(s) attached to the said Observations.
   ☐ the application document(s) at which the previous Office Action is directed.
   ☐ the application document(s) confirmed in the said Reexamination Decision.
   ☐

3. ☑ In this Office Action no new reference documents have been cited.
   ☐ The following reference document(s) is/are cited in this Office Action. (Its/Their serial number(s) shall come after those previously cited and will continue to be used throughout the examination procedure):

Mastercard, Ex1002, p. 701

Serial No.	Number or Title(s) of Reference Document(s)	Date of Publication (or filing date of interfering appl.)

4. Concluding comments of the examiner:

☐ On the description:

- ☐ The amendment to the description is not in conformity with the provision of Art. 33 of the Patent Law.
- ☐ The content of the application comes within the scope where no patent right shall be granted as prescribed in Art. 5 of the Patent Law.
- ☐ The description is not in conformity with the provision of Art. 26, para. 3 of the Patent Law.
- ☐ The drafting of the description is not in conformity with the provision of Rule 18 of the Implementing Regulations.

☑ On the claims:

- ☐ The amendment to Claim(s) _____ is not in conformity with the provision of Art. 33 of the Patent Law.
- ☐ Claim(s) _____ come(s) within the scope where no patent right shall be granted as prescribed in Art. 25 of the Patent Law.
- ☐ Claim(s) _____ is/are not in conformity with the definition of invention in Rule 2, para. 1 of the implementing Regulations.
- ☐ Claim(s) _____ possess(es) no novelty as prescribed in Art. 22, para. 2 of the Patent Law.
- ☑ Claim(s) 1-20 possess(es)no inventiveness as prescribed in Art. 22, para. 3 of the Patent Law.
- ☐ Claim(s) _____ possess(es) no practical applicability as prescribed in Art. 22, para. 4 of the Patent Law.
- ☐ Claim(s) _____ is/are not in conformity with the provision of Art. 26, para. 4 of the Patent Law.
- ☐ Claim(s) _____ is/are not in conformity with the provision of Art. 31, para. 1 of the Patent Law.
- ☐ Claim(s) _____ is/are not in conformity with the provisions of Rule 20 of the Implementing Regulations.
- ☐ Claim(s) _____ is/are not in conformity with the provision of Art. 9 of the Patent Law.
- ☐ Claim(s) _____ is/are not in conformity with the provision of Rule 23 of the Implementing Regulations.

Mastercard, Ex1002, p. 702

See the text portion of this Office Action for a detailed analysis of the above concluding comments.

5. In view of the above concluding comments, the examiner deems that

☐ the applicant should make amendment to the application document(s) according to the requirements raised in the text portion of this Office Action.

☐ the applicant should expound in his/its observations the reason why the captioned patent application is patentable and make amendment to what is not in conformity with the provisions as pointed out in the text portion of this Office Action, otherwise the said application will be rejected.

☑ the patent application has no substantive content(s) for which the patent right may be obtained, if the applicant has no sufficient reason to demonstrate that the captioned application may be granted a patent right, said the application will be rejected.

6. **The applicant should pay attention to the following matters:**

(1) According to the provision of Art. 37 of the Patent Law, the applicant should submit his/its observations within **two** months from the date of receipt of this Office Action; if, without any justified reason(s), the time limit for making a response is not met, the said application shall be deemed to have been withdrawn.

(2) The amendment(s) made by the applicant to the application should be in conformity with the provisions of Art. 33 of the Patent Law and Rule 51 of the Implementing Regulations thereof, the amended text should be in duplicate and its form should conform to the relevant provisions of the Guidelines for Examination.

(3) The observations and/or amended text of the applicant should be submitted to the Receiving Section of the Chinese Patent Office by mail or by personal delivery. If not submitted Receiving Section by mail or by personal delivery, the document(s) will have no legal effect.

(4) If no appointment is made in advance, the applicant and/or the agent shall not come to the Chinese Patent Office to hold an interview with the examiner.

7. This Office Action consists of the text portion totaling 8 page(s) and of the following attachment(s):

☐ _____ copy(copies) of the reference document(s) cited totaling _____ page(s).

Examination Dept. No. _____ Examiner _____

2206

Mastercard, Ex1002, p. 703

Your Ref: STAPP1101-CN

Our Ref: CPEL1450577P

Application No: 201280053080.6

TEXT OF SECOND OFFICE ACTION

The applicant submitted an Observation and the amended application text on December 22, 2016. Upon further examination of said documents, the examiner has the following comments.

I. Claims 1-20 do not possess inventiveness as prescribed in Article 22(3) of the Patent Law.

Claim 1 claims a method for acquiring digital credential data by a point-of-sale (POS) terminal from a mobile device for authorization of a financial transaction. D1 (US2011099079A1) discloses secure mobile-based financial transactions, and particularly discloses the following features (see paragraphs [0021]-[0033] of the description): the payment server sends a one-time digital key to the mobile terminals (equivalent to prior to an interrogation, the mobile device requesting, over a network, a transaction cache from a remote application system; receiving the transaction cache, the transaction cache containing data required to properly create responses to commands); the sale terminal sends the amount to the mobile terminal, the mobile terminal submits a payment request including the payment number and the amount to the POS device, the payment number includes a one-time digital key and a random number, the one-time digital key is sent automatically from the payment server to the mobile terminal (equivalent to using a remote cryptographic key to calculate an expected cryptogram that is expected to comprise at least a portion of the digital credential data; performing an interrogation between the point-of-sale terminal and the mobile device comprising: sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device requesting the digital credential data; and sending through the communication channel at least one device response

Mastercard, Ex1002, p. 704

communication from the mobile device to the point-of-sale terminal comprising the expected cryptogram as the at least a portion of the digital credential data); the payment server verifies the payment number and confirms the transaction to the POS device (equivalent to wherein the financial transaction is authorized). As the technical solution claimed by claim 1 is compared to the content disclosed by D1, the distinguishing features are the following: (1) a transaction cache for a particular secure element from a remote application system that comprises a plurality of secure element representations; wherein the mobile device comprises an application running in an operating system of the mobile device that is capable of being interrogated by a POS; APDU commands; using a remote permanent cryptographic key, wherein the remote permanent cryptographic key is persistently stored at a remote source that is remote from the mobile device; (2) and wherein the mobile device does not access a duplicate local permanent cryptographic key persistently stored locally to the mobile device. Based on the distinguishing features, it can be determined that the problems actually solved by claim 1 are: (1) how to make transactions based on secure element; (2) how to acquire a cryptogram.

Regarding distinguishing feature (1), D3 (US2010153721A1) discloses a method for accessing remote secure elements, and particularly discloses the following feature (see paragraphs [0006]-[0007] and [0029]-[0042] of the description): the secure element (equivalent to an HSM) is located on the remote secure element server, the virtual secure element module is configured to communicate with one or more remote secure element servers. A secure transaction may be established using the virtual secure element module and the remote securing element (equivalent to a remote application system that comprises a plurality of secure element representations); customers can pay by simply waving their portable electronic device at a point-of-sale reader (equivalent to wherein the mobile device comprises an application running in an operating system of the mobile device that is capable of being interrogated by a POS). The feature performs the same function in D3 as it performs in

Mastercard, Ex1002, p. 705

claim 1, both making transactions using remote secure elements, that is, those skilled in the art can get inspiration and apply the method of using remote secure element in D3 to the payment transaction process of D1. In addition, generating payment cryptogram using permanent cryptogram of a secure element is a common way of a secure element. Therefore, on D3 has disclosed storing secure elements using a remote server for payment, those skilled in the art will easily conceive remotely storing permanent cryptogram corresponding to the secure element and sending the permanent cryptogram of the secure element to the mobile device, to thereby generate the payment cryptogram. In addition, an APDU command is a common data interaction for secure element transactions.

Regarding distinguishing feature (2), on the basis that D1 discloses the payment server sending a one-time key, in order to realize security of payment, those skilled in the art conceive the mobile device not accessing a locally stored key, which is common technical means in the secure payment field.

It can be seen that it is obvious for those skilled in the art to obtain the technical solution claimed by claim 1 on the basis of D1 in combination with D3 and the common technical means in the art. Therefore, claim 1 neither possesses prominent substantive features nor represents a notable progress, and does not possess inventiveness as prescribed in Article 22(3) of the Patent Law.

2. Claim 2 is a dependent claim of claim 1. Its additional technical feature is disclosed by D1 (see paragraphs [0021]-[0033] of the description): the payment server automatically sends the next digital key to the mobile terminal to be stored there until the next transaction is processed (equivalent to sending the remote permanent cryptographic key to the mobile device from the remote source; and transiently caching the remote permanent cryptographic key in the mobile device as a cached transient permanent cryptographic key); the sale terminal sends the amount to the mobile terminal (equivalent to the step of sending through the communication channel the at least one POS command

Mastercard, Ex1002, p. 706

communication comprising sending unpredictable data); the mobile terminal submits a payment request including the payment number and the amount to the POS device, the payment number includes a one-time digital key and a random number, the one-time digital key is input to a number generator algorithm to generate the payment number (equivalent to the step of sending through the communication channel the at least one POS command communication comprising sending a request for an expected cryptogram that is expected to be calculated by the mobile device, at least in part, from the unpredictable data; and the step of sending through the communication channel the at least one device response communication from the mobile device to the point-of-sale terminal comprising sending the expected cryptogram calculated, at least in part, from the unpredictable data and, at least in part, from the cached transient cryptographic key). On the basis that D3 has disclosed remotely storing the secure element, using the permanent cryptogram of the remote secure element to generate payment cryptogram is a common technical means of using secure element for payment. Therefore, when the referred claim 1 does not possess inventiveness, claim 2 does not possess the inventiveness as prescribed in Article 22(3) of the Patent Law.

3. Claim 3 claims a method for acquiring digital credential data by a point-of-sale (POS) terminal from a mobile device for authorization of a financial transaction. D1 discloses secure mobile-based financial transactions, and particularly discloses the following features (see paragraphs [0021]-[0033] of the description): the payment server sends a one-time digital key to the mobile terminals (equivalent to prior to an interrogation, the mobile device requesting, over a network, a transaction cache from a remote application system; receiving the transaction cache, receiving a temporary cryptographic key supplied in a response to the request); the sale terminal sends the amount to the mobile terminal to acquire the corresponding payment number and etc., the one-time digital key is input to a number generator algorithm to generate the payment number (equivalent to performing an interrogation between the

Mastercard, Ex1002, p. 707

point-of-sale terminal and the mobile device comprising: sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device, the at least one POS command communication requesting digital credential data, the at least one POS command communication comprising (a) a cryptogram request and (b) unpredictable data); the mobile terminal inputs a one-time digital key to the number generator algorithm to generate the payment number, also may generate in combination with a random number, and sends the payment number to the sale terminal (equivalent to the mobile device generating a cryptogram using the temporary cryptographic key and formulating a response containing the cryptograph generated using the temporary cryptographic key) includes a client payment logic 118 which, among other functions, generates a random number according to an algorithm. Client payment logic 118 also combines the random number with; the mobile terminal submits a payment request including the payment number and the amount (equivalent to sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal, the at least one device response communication comprising at least one part of the digital credential data, the digital credential data comprising the response); the payment server verifies the payment number and confirms the transaction to the POS device (equivalent to wherein the cryptogram is verified to authorized the transaction). As the technical solution claimed by claim 3 is compared to the content disclosed by D1, the distinguishing features are the following: (1) a transaction cache for a particular secure element from a remote application system that comprises a plurality of secure element representations; wherein the mobile device comprises an application running in an operating system of the mobile device that is capable of being interrogated by a POS; when receiving the response of the application system to the request, the temporary cryptographic key is associated with the particular secure element; APDU commands; (2) using unpredictable data for generating cryptogram. Based on the distinguishing

Mastercard, Ex1002, p. 708

features, it can be determined that the problems actually solved by claim 1 are: (1) how to make transactions based on secure element; (2) how to generate an expected cryptogram.

Regarding distinguishing feature (1), D3 (US20101537721A1) discloses a method for accessing remote secure elements, and particularly discloses the following feature (see paragraphs [0006]-[0007] and [0029]-[0042] of the description): the secure element (equivalent to an HSM) is located on the remote secure element server, the virtual secure element module is configured to communicate with one or more remote secure element servers. A secure transaction may be established using the virtual secure element module and the remote securing element (equivalent to a remote application system that comprises a plurality of secure element representations); customers can pay by simply waving their portable electronic device at a point-of-sale reader (equivalent to wherein the mobile device comprises an application running in an operating system of the mobile device that is capable of being interrogated by a POS). The feature performs the same function in D3 as it performs in claim 3, both making transactions using remote secure elements, that is, those skilled in the art can get inspiration and apply the method of using remote secure element in D3 to the payment transaction process of D1. In addition, the secure element being associated with the cryptogram, and generating payment cryptogram using the cryptogram of a secure element, is a common way of a secure element. Therefore, on D3 has disclosed storing secure elements using a remote server for payment, those skilled in the art will easily conceive remotely storing permanent cryptogram corresponding to the secure element and sending the cryptogram of the secure element to the mobile device, to thereby generate the payment cryptogram. In addition, an APDU command is a common data interaction for secure element transactions.

Regarding distinguishing feature (2), D2 (CN101048794A) discloses a method for authorizing a transaction using a dynamic authorization code, and

Mastercard, Ex1002, p. 709

particularly discloses the following feature (see line 1 on page 4 to line 28 on page 5 and line 1 on page 8 to line 19 on page 9 of the description): the unpredictable data includes the transaction amount and etc , the device uses the unpredictable data together with other secret data to generate a dynamic authorization code (equivalent to an expected cryptogram that is expected to be calculated, at least in part, from unpredictable data). The feature performs the same function in D2 as it performs in claim 3, both generating a cryptogram using unpredictable data, that is, those skilled in the art can get inspiration and apply the method of generating a cryptogram in D2 to the payment number generation process of D1.

Thus it can be seen that it is obvious to those skilled in the art to obtain the technical solution claimed by claim 3 on the basis of D1 in combination with D2, D3 and common technical means in the art. Therefore, claim 3 does not possess prominent substantive feature and notable progress, i.e. does not possess inventiveness as prescribed in Article 22(3) of the Patent Law.

4-5. Please refer to the First Office Action

6. Claim 7 is a dependent claim of claim 6. Its additional technical feature is disclosed by D1 (see paragraphs [0021]-[0033] of the description): the payment server automatically sends the next digital key to the mobile terminal to be stored there until the next transaction is processed. The mobile terminal generates the corresponding payment number based on the one-time digital key. Therefore, when the referred claim 6 does not possess inventiveness, claim 7 does not possess the inventiveness as prescribed in Article 22(3) of the Patent Law.

7. Claim 8 is a dependent claim of claim 6. D3 (US20101537211A1) discloses the following feature (see paragraphs [0006]-[0007] and [0029]-[0042] of the description): the portable electronic device includes a virtual secure element module, which is configured to communicate with one or more remote secure

Mastercard, Ex1002, p. 710

element servers, the secure element (equivalent to an HSM) is located on the remote secure element server. D2 discloses (see line 1 on page 4 to line 28 on page 5 and line 1 on page 8 to line 19 on page 9 of the description): unpredictable data that the user will enter into his or her mobile processing device, which will subsequently be used to generate the dynamic authentication code, typically in conjunction with other data such as an encryption key. On the basis of this, when using the secure element in D3 for transactions, those skilled in the art will easily conceive creating a temporary cryptographic key using unpredictable data and associating with the secure element, which is a common technical means for making transactions using secure element. Therefore, when the referred claim 6 does not possess inventiveness, claim 8 does not possess the inventiveness as prescribed in Article 22(3) of the Patent Law.

8. Claim 9 is a dependent claim of claim 1. D2 discloses (see line 1 on page 4 to line 28 on page 5 and line 1 on page 8 to line 19 on page 9 of the description): the mobile processing devices generates a dynamic authentication code using a key which can be a DES key and can be stored in a protected memory (equivalent to wherein generating the cryptogram using the cryptographic key comprises encrypting the set of inputs using the locally stored cryptographic key according to a digital encryption standard (DES) calculation to generate an output). That the cryptogram includes a portion of the output is commonly seen for outputting encrypted information. Therefore, when the referred claim 1 does not possess inventiveness, claim 9 does not possess the inventiveness as prescribed in Article 22(3) of the Patent Law.

9. Claim 10 is a dependent claim of claim 1. Since during practical transactions, secure elements are mainly used for generating transaction-related cryptogram, not contacting the remote application system during the interrogation is a common technical means in the art. Therefore, when the referred claim 1 does not possess inventiveness, claim 10 does not possess inventiveness as

Mastercard, Ex1002, p. 711

prescribed in Article 22(3) of the Patent Law.

10. Claim 11 is a dependent claim of claim 1. D1 discloses (see paragraphs [0021]-[0033] of the description): POS device communicates the amount to the payment server directly, and sends a payment number. The payment server disassembles the payment number, compares the one-time digital key and random number, and verifies that each of these is correct, and confirms the transaction to the POS after verifying (equivalent to receiving an authorization request from the point-of-sale terminal, the authorization request comprising the cryptogram; verifying a correctness of the response cryptogram by the system, wherein the received cryptogram is compared; and sending an authorization response from the system to the point-of-sale wherein data contained in the authorization response is determined, at least in part, by the verifying of the correctness of the received cryptogram). D2 discloses (see line 1 on page 4 to line 28 on page 5 and line 1 on page 8 to line 19 on page 9 of the description): the authorization process may entail calculating, at the authorization location, the dynamic authentication code using the same data and algorithm as performed by the mobile device, and comparing the calculated result to the received dynamic code to confirm that the calculated results matches the received code (equivalent to wherein the received cryptogram is compares with a result of a cryptogram calculation, the result generated based on the temporary cryptographic key associated with a transaction). Therefore, when the referred claim 1 does not possess inventiveness, claim 11 does not possess the inventiveness as prescribed in Article 22(3) of the Patent Law.

11. Claim 12 is a dependent claim of claim 11, and its additional technical feature has been disclosed by D2 (see line 1 on page 4 to line 28 on page 5 and line 1 on page 8 to line 19 on page 9 of the description): the unpredictable data includes the transaction amount and etc., the device uses the unpredictable data together with other secret data to generate a dynamic authorization code, the authorization process may entail calculating, at the authorization location, the

Mastercard, Ex1002, p. 712

dynamic authentication code using the same data and algorithm as performed by the mobile device, and comparing the calculated result to the received dynamic code to confirm that the calculated results matches the received code. Therefore, when the referred claim 11 does not possess inventiveness, claim 12 does not possess the inventiveness as prescribed in Article 22(3) of the Patent Law.

12. Claim 13 is a dependent claim of claim 12. During the authorization process, sending the values of the transaction is a common technical means in the art. ISO8583 is a common data format. Therefore, when the referred claim 12 does not possess inventiveness, claim 13 does not possess the inventiveness as prescribed in Article 22(3) of the Patent Law.

13-19. Please refer to the First Office Action

II. Reply to the applicant's observations

The examiner deems: 1. D1 discloses (see paragraphs [0021]-[0033] of the description): the payment number includes a one-time digital key and a random number, the one-time digital key is sent automatically from the payment server to the mobile terminal, the one-time digital key, in the form of a multi-digit number, is effectively multiplied by the number generator algorithm to create a payment number. Thus it can be seen that D1, like the present application, also generates the payment number (equivalent to cryptogram) by using one-time digital key (equivalent to key). Although the key is not permanent, D3 has given the hint of making transaction payments with remote secure element. And during the process of the secure transactions of secure elements, generating cryptograms using permanent keys to authorize the transaction is a common technical means in the art. For example, D2 has disclosed: the software or circuitry on the mobile device has substantially all of the functionality of a typical smart card, although (equivalent to a secure element); the mobile processing device generates a dynamic authentication code 130

Mastercard, Ex1002, p. 713

using a key 120, such as an encryption key. The key 120 may be a DES key, a private key, a public key, some combination thereof, or any other data used for encryption or generating a secure message for subsequent authentication. The key may be stored, for example in application memory in the mobile processing device. 2. D1 discloses: a one-time digital key (equivalent to a temporarily used key); D2 discloses: the encryption key or one or more of the keys in a key pair may be encrypted, such as with triple-DES, using the PIN and a Mobile Device Identifier, previously entered by the user, as the temporary key to create the personalization data. the application cryptogram is generated based on the unpredictable data in addition to the key 120 and transaction counter (equivalent to generating the cryptogram using the unpredictable data and the temporary cryptographic key). Besides, on the basis that D3 has disclosed making transaction payments using a remote secure element, those skilled in the art will easily conceive sending keys related to the secure element from the remote to the mobile device; 3. Hash is a common way of data encryption. On the basis that D2 has disclosed that the key 120 may be a DES key, a private key, a public key, some combination thereof, those skilled in the art will easily conceive using Hash for encryption.

For the abovementioned reasons, neither the independent claims nor the dependent claims of the present application possess inventiveness; meanwhile, the description does not possess any other patentable substantive contents. The present application does not have a prospect to be granted the patent right. If the applicant fails to provide weighty reasons within the time limit for making a response as prescribed in this Office Action, the present application will be rejected.

Mastercard, Ex1002, p. 714

100035
北京市西城区裨皮厂胡同 2 号国际商会大厦 16 层 中国专利代理（香港）有限公司
臧霁晨 刘春元

发文日：
2017 年 03 月 07 日

申请号或专利号：201280053080.6　　发文序号：201703020139460O

申请人或专利权人：易太普公司

发明创造名称：用于授权利用不可预测密码的交易的系统和方法

第二次审查意见通知书

1. ☒审查员已经收到申请人于 2016 年 12 月 22 日提交的意见陈述书，在此基础上审查员对上述专利申请继续进行实质审查。
☐根据国家知识产权局专利复审委员会于　　年　　月　　日作出的复审决定，审查员对上述专利申请继续进行实质审查。
☐_____
2. ☐经审查，申请人于_____提交的修改文件，不符合专利法实施细则第 51 条第 3 款的规定，不予接受。
3. 继续审查是针对下列申请文件进行的：
☐上述意见陈述书中所附的经修改的申请文件。
☒前次审查意见通知书所针对的申请文件以及上述意见陈述书中所附的经修改的申请文件替换文件。
☐前次审查意见通知书所针对的申请文件。
☐上述复审决定所确定的申请文件。
☐_____
4. ☒本通知书未引用新的对比文件。
☐本通知书引用下列对比文件（其编号续前，并在今后的审查过程中继续沿用）：

编号	文件号或名称	公开日期（或优先权申请的申请日）

5. 审查的结论性意见：
关于说明书：
☐申请的内容属于专利法第 5 条规定的不授予专利权的范围。
☐说明书不符合专利法第 26 条第 3 款的规定。
☐说明书的修改不符合专利法第 33 条的规定。
☐说明书的撰写不符合专利法实施细则第 17 条的规定。
☐_____
关于权利要求书：
☐权利要求　　不符合专利法第 2 条第 2 款的规定。
☐权利要求_____不符合专利法第 9 条第 1 款的规定。

纸件申请，回函请寄：100088 北京市海淀区蓟门桥西土城路 6 号　国家知识产权局专利局受理处收
电子申请，应当通过电子专利申请系统以电子文件形式提交相关文件。除另有规定外，以纸件等其他形式提交的文件视为未提交。

Mastercard, Ex1002, p. 715

☐权利要求　　不具备专利法第22条第2款规定的新颖性。
☒权利要求 1-20 不具备专利法第22条第3款规定的创造性。
☐权利要求_____不具备专利法第22条第4款规定的实用性。
☐权利要求_____属于专利法第25条规定的不授予专利权的范围。
☐权利要求_____不符合专利法第26条第4款的规定。
☐权利要求_____不符合专利法第31条第1款的规定。
☐权利要求_____的修改不符合专利法第33条的规定。
☐权利要求_____不符合专利法实施细则第19条的规定。
☐权利要求　　不符合专利法实施细则第20条的规定。
☐权利要求_____不符合专利法实施细则第21条的规定。
☐权利要求_____不符合专利法实施细则第22条的规定。
☐_____

☐申请不符合专利法第26条第3款或者实施细则第26条的规定。
☐申请不符合专利法第20条第1款的规定。
☐分案申请不符合专利法实施细则第43条第1款的规定。
上述结论性意见的具体分析见本通知书的正文部分。

6.基于上述结论性意见，审查员认为：

☐申请人应当按照通知书正文部分提出的要求，对申请文件进行修改。
☐申请人应当在意见陈述书中论述其专利申请可以被授予专利权的理由，并对通知书正文部分中指出的不符合规定之处进行修改，否则将不能授予专利权。
☒专利申请中没有可以被授予专利权的实质性内容，如果申请人没有陈述理由或者陈述理由不充分，其申请将被驳回。
☐_____

7. 申请人应注意下列事项：

（1）根据专利法第37条的规定，申请人应当在收到本通知书之日起的2个月内陈述意见，如果申请人无正当理由逾期不答复，其申请将被视为撤回。

（2）申请人对其申请的修改应当符合专利法第33条的规定，不得超出原说明书和权利要求书记载的范围，同时申请人对专利申请文件进行的修改应当符合专利法实施细则第51条第3款的规定，按照本通知书的要求进行修改。

（3）申请人的意见陈述书和/或修改文本应当邮寄或递交国家知识产权局专利局受理处，凡未邮寄或递交给受理处的文件不具备法律效力。

（4）未经预约，申请人和/或代理人不得前来国家知识产权局与审查员举行会晤。

8. 本通知书正文部分共有8页，并附有下列附件：

☐引用的对比文件的复印件共　　份　　页。
☐_____

审查员：贺龙涛　　联系电话：028-62967610　　审查部门：专利审查协作四川中心电学发明审查部

Mastercard, Ex1002, p. 716

第二次审查意见通知书

申请号：201280050806

申请人于2016年12月22日提交了意见陈述书和经过修改的申请文件，审查员在阅读了上述文件后，对本申请继续进行审查，现提出如下审查意见：

一、权利要求1-20不具备专利法第22条第3款所规定的创造性

1、权利要求1请求保护一种用于通过销售点（POS）终端从移动设备获取数字凭证数据以便授权财务交易的方法，对比文件1（US 2011099079A1）公开了一种基于移动终端的安全金融交易，并具体公开了如下特征（参见说明书第[0021]-[0033]段）：支付服务器向移动终端发送一次性数字密钥（相当于在询问前，所述移动设备通过网络从远程应用程序系统请求交易缓存；接收所述交易缓存，所述交易缓存包含适当地创建对命令的响应所需的数据）；销售终端将数量发送给移动终端，移动终端向POS提交支付请求，支付请求包括支付码及数量，支付码包括一次性数字密钥及随机数，一次性数字密钥从支付服务器自动发送到移动终端（相当于使用远程的使用密码的密钥来计算预期包括数字凭证数据的至少一部分的预期密码，执行销售点终端和移动设备之间的询问，包括：通过通信信道将至少一个POS命令通信从销售点终端发送到请求数字凭证数据的移动设备；以及通过所述通信信道将至少一个设备响应通信从移动设备发送到包括作为数字凭证数据的至少一部分的预期密码的销售点终端）；支付服务器鉴定支付码并向POS确认交易（相当于其中所述财务交易被授权）。权利要求1所请求保护的技术方案与对比文件1所公开的内容相比，区别特征为：（1）从包括多个安全元件表示的远程应用程序系统请求用于特定安全元件的交易缓存，其中所述移动设备包括在能够被POS询问的所述移动设备的操作系统中运行的应用程序；APDU命令；远程永久的使用密钥，其中所述远程永久的使用密码的密钥被持久地存储在远离移动设备的远程源处；（2）且其中移动设备不访问持久地本地存储到移动设备的复制本地永久的使用密码的密钥。基于上述区别特征，可以确定权利要求1实际解决的问题是：（1）如何基于安全元件进行交易；（2）如何获取密码。

对于区别特征（1），对比文件3（US 2010153721A1）公开了一种用于访问远程安全元件的方法，并具体公开了如下特征（参见说明书第[0006]-[0007]、[0029]-[0042]段）：安全元件（相当于HSM）被设置在远程安全元件服务器，虚拟安全元件模块被配置成与一个或更多个远程安全元件服务器进行通信，利用远程安全元件服务器和虚拟安全模块来建立安全业务（相当于包括多个安全元件表示的远程应用程序系统）；顾客可以通过简单地在销售点的读取器处晃动他们的便携式电子装置来付款（相当于其中所述移动设备包括在能够被POS询问的所述移动设备的操作系统中运行的应用程序）。上述特征在对比文件3中所起的作用与其在权利要求1中所起的作用相同，都是利用远程安全元件进行交易，也就是说，本领域技术人员能够获得启示，将对

Mastercard, Ex1002, p. 717

比文件 3 中利用远程安全元件的方法应用到对比文件 1 的支付交易过程中。此外，利用安全元件的永久密码生成支付密码，这是安全元件的常见处理方式，因此，在对比文件 3 公开了利用远程服务器存储安全元件进行支付的基础上，本领域技术人员容易想到远程存储安全元件对应的永久密码，并将安全元件的永久密码发送给移动设备，以生成支付密码。此外，APDU 命令是安全元件交易的常用数据交互方式。

对于区别特征（2），在对比文件 1 公开了支付服务器发送一次性密码的基础上，为了实现支付的安全性，本领域技术人员容易想到移动设备不访问本地存储的密钥，这是安全支付领域的常用技术手段。

由此可知，在对比文件 1 的基础上结合对比文件 3 及本领域的常用技术手段得到权利要求 1 所要求保护的技术方案，对本领域的技术人员来说是显而易见的，因此权利要求 1 不具有突出的实质性特点和显著的进步，不具备专利法第 22 条第 3 款所规定的创造性。

2、权利要求 2 是权利要求 1 的从属权利要求，对比文件 1 公开了（参见说明书第[0021]-[0033]段）：支付服务器自动发送下一个数字密钥到移动终端，并将其保存在移动终端以便下次交易使用（相当于将所述远程使用密码的密钥从远程源发送到移动设备；以及将所述远程使用密码的密钥暂时缓存在移动设备中作为缓存的暂时的永久的使用密码的密钥）；销售终端将数量发送给移动终端（相当于通过所述通信信道发送所述至少一个 POS 命令通信的步骤包括发送不可预知数据）；移动终端向 POS 提交支付请求，支付请求包括支付码及数量，支付码包括一次性数字密钥及随机数，将一次性数字密码输入数字生成算法以生成支付码（相当于通过所述通信信道发送所述至少一个 POS 命令通信的步骤包括发送对预期由移动设备至少部分根据不可预知数据计算的预期密码的请求；以及通过所述通信信道将所述至少一个设备响应通信从移动设备发送到销售点终端的步骤包括发送至少部分根据不可预知数据以及至少部分根据所述缓存的暂时的使用密码的密钥计算的预期密码）。在对比文件 3 公开了远程存储安全元件的基础上，利用远程安全元件的永久密码以生成支付密码这是利用安全元件进行支付时的常用技术手段。因此，在其引用的权利要求 1 不具备创造性的情况下，权利要求 2 不具备专利法第 22 条第 3 款所规定的创造性。

3、权利要求 3 请求保护一种用于通过销售点（POS）终端从移动设备获取数字凭证数据以便授权财务交易的方法，对比文件 1 公开了一种基于移动终端的安全金融交易，并具体公开了如下特征（参见说明书第[0021]-[0033]段）：支付服务器向移动终端发送一次性数字密钥（相当于在询问前，所述移动设备通过网络从远程应用程序系统请求交易缓存；接收对所述请求的响应中所提供的临时的使用密码的密钥）；销售终端将数量发送给移动终端，以获取相应的支付码

Mastercard, Ex1002, p. 718

等，将一次性数字密码输入数字生成算法以生成支付码（相当于执行销售点终端和移动设备之间的询问，通过通信信道将至少一个 POS 命令通信从销售点终端发送到移动设备，所述至少一个 POS 命令通信请求数字凭证数据，所述至少一个 POS 命令通信包括（a）密码请求；以及（b）不可预知数据）；移动终端将一次性数字密码输入数字生成算法以生成支付码，同时可结合随机数生成，并将支付码发送给销售终端（相当于所述移动设备使用所述临时的使用密码的密钥来生成密码，且制定包含使用所述临时的使用密码的密钥生成的密码的响应）；移动终端向 POS 提交支付请求，支付请求包括支付码及数量（相当于通过所述通信信道将至少一个设备响应通信从移动设备发送到销售点终端，所述至少一个设备响应通信包括数字凭证数据的至少一部分，所述数字凭证数据包括所述响应）；支付服务器鉴定支付码并向 POS 确认交易（相当于其中所述密码被验证以授权所述交易）。权利要求 3 所请求保护的技术方案与对比文件 1 所公开的内容相比，区别特征为：（1）从包括多个安全元件表示的远程应用程序系统请求用于特定安全元件的交易缓存，其中所述移动设备包括在能够被 POS 询问的所述移动设备的操作系统中运行的应用程序；接收在所述应用程序系统对所述请求的响应中，所述临时的使用密码的密钥与所述特定安全元件相关联；APDU 命令；（2）使用不可预知数据来生成密码。基于上述区别特征，可以确定权利要求 3 实际解决的问题是：（1）如何基于安全元件进行交易；（2）如何生成预期密码。

对于区别特征（1），对比文件 3（US 2010153721A1）公开了一种用于访问远程安全元件的方法，并具体公开了如下特征（参见说明书第[0006]-[0007]、[0029]-[0042]段）：安全元件（相当于 HSM）被设置在远程安全元件服务器，虚拟安全元件模块被配置成与一个或更多个远程安全元件服务器进行通信，利用远程安全元件服务器和虚拟安全模块来建立安全业务（相当于包括多个安全元件表示的远程应用程序系统）；顾客可以通过简单地在销售点的读取器处晃动他们的便携式电子装置来付款（相当于其中所述移动设备包括在能够被 POS 询问的所述移动设备的操作系统中运行的应用程序）。上述特征在对比文件 3 中所起的作用与其在权利要求 3 中所起的作用相同，都是利用远程安全元件进行交易，也就是说，本领域技术人员能够获得启示，将对比文件 3 中利用远程安全元件的方法应用到对比文件 1 的支付交易过程中。此外，安全元件与密码相关联，并利用安全元件的密码生成支付密码，这是安全元件的常见处理方式，因此，在对比文件 3 公开了利用远程服务器存储安全元件进行支付的基础上，本领域技术人员容易想到远程存储安全元件对应的密码，并将安元件的密码发送给移动设备，以生成支付密码。此外，APDU 命令是安全元件交易的常用数据交互方式。

对于区别特征（2），对比文件 2（CN 101048794A）公开了一种使用动态授权码授权交易的

Mastercard, Ex1002, p. 719

方法，并具体公开了如下特征（参见说明书第 4 页第 1 行-第第 5 页第 28 行、第 8 页第 1 行-第 9 页第 19 行）：不可预测数据包括交易额等，设备使用不可预测数据及其它保密数据来生成动态授权码（相当于所述预期密码被预期至少部分根据不可预知数据来计算）。上述特征在对比文件 2 中所起的作用与其在权利要求 3 中所起的作用相同，都是利用不可预测数据生成密码，也就是说，本领域技术人员能够获得启示，将对比文件 2 中生成密码的方法应用到对比文件 1 的支付码生成过程中。

由此可知，在对比文件 1 的基础上结合对比文件 2、对比文件 3 及本领域的常用技术手段得到权利要求 3 所要求保护的技术方案，对本领域的技术人员来说是显而易见的，因此权利要求 3 不具有突出的实质性特点和显著的进步，不具备专利法第 22 条第 3 款所规定的创造性。

4、权利要求 4-5 是权利要求 3 的从属权利要求，其附加技术特征被对比文件 2 公开（参见说明书第 4 页第 1 行-第第 5 页第 28 行、第 8 页第 1 行-第 9 页第 19 行）：不可预测的数据可以是随机数、可以基于当前时间、预测交易额的单项散列、上述的某些组合。因此，在其引用的权利要求 3 不具备创造性的情况下，权利要求 4-5 不具备专利法第 22 条第 3 款所规定的创造性。

5、权利要求 6 是权利要求 3 的从属权利要求，其附加技术特征被对比文件 1 公开（参见说明书第[0021]-[0033]段）：支付服务器自动发送下一个数字密钥到移动终端，并将其保存在移动终端以便下次交易使用。因此，在其引用的权利要求 3 不具备创造性的情况下，权利要求 6 不具备专利法第 22 条第 3 款所规定的创造性。

6、权利要求 7 是权利要求 6 的从属权利要求，其附加技术特征被对比文件 1 公开（参见说明书第[0021]-[0033]段）：支付服务器自动发送下一个数字密钥到移动终端，并将其保存在移动终端以便下次交易使用，移动终端基于一次性数字密钥生成相应的支付码。因此，在其引用的权利要求 6 不具备创造性的情况下，权利要求 7 不具备专利法第 22 条第 3 款所规定的创造性。

7、权利要求 8 是权利要求 6 的从属权利要求，对比文件 3 公开了（参见说明书第[0006]-[0007]、[0029]-[0042]段）：便携式电子装置包括虚拟安全元件模块，虚拟安全元件模块被配置成与一个或更多个远程安全元件服务器进行通信，安全元件（相当于 HSM）被设置在远程安全元件服务器。对比文件 2 公开了（参见说明书第 4 页第 1 行-第第 5 页第 28 行、第 8 页第 1 行-第 9 页第 19 行）：用户将输入到他或她的移动处理设备中去的不可预测的数据，该数据随后被用于（典型地与诸如加密密钥之类的其它数据一起）生成动态认证码。在此基础上，当利用对比文件 3 中的安全元件进行交易时，本领域技术人员容易想到利用不可预测的数据临时创建密钥，并与安全元件关联，这是利用安全元件进行交易时的常用技术手段。因此，在其引用的权利要求 6 不具备创造性的情况下，权利要求 8 不具备专利法第 22 条第 3 款所规定的创造

Mastercard, Ex1002, p. 720

性。

8、权利要求 9 是权利要求 1 的从属权利要求，对比文件 2 公开了（参见说明书第 4 页第 1 行-第第 5 页第 28 行、第 8 页第 1 行-第 9 页第 19 行）：移动处理设备使用密钥生成动态认证码，密钥可以是 DES 密钥，密钥可以保存在受保护的存储器中（相当于其中使用所述使用密码的密钥生成所述密码包括按照数字加密标准（DES）计算使用所述本地存储的使用密码的密钥来加密所述输入的组以生成输出）。密码包括输出的一部分是进行加密信息输出时的常见方式。因此，在其引用的权利要求 1 不具备创造性的情况下，权利要求 9 不具备专利法第 22 条第 3 款所规定的创造性。

9、权利要求 10 是权利要求 1 的从属权利要求，由于实际交易过程中，安全元件主要用于生成交易相关的密码，因此在交易询问期间不联系远程应用程序系统，这是本领域的常用技术手段。因此，在其引用的权利要求 1 不具备创造性的情况下，权利要求 10 不具备专利法第 22 条第 3 款所规定的创造性。

10、权利要求 11 是权利要求 1 的从属权利要求，对比文件 1 公开了（参见说明书第[0021]-[0033]段）：POS 终端可以将数量直接发送给支付服务器，并传送支付码，支付服务器分解支付码，比较一次性数字密码及随机数，验证其正确性，验证通过后，向 POS 确认交易（相当于从所述销售点终端接收授权请求，所述授权请求包括所述密码；由所述系统验证所述响应密码的正确性，其中将所接收的密码进行比较；以及从所述系统向所述销售点发送授权响应，其中至少部分地通过验证所接收的密码的正确性来确定包含在所述授权响应中的数据）。对比文件 2 公开了（参见说明书第 4 页第 1 行-第第 5 页第 28 行、第 8 页第 1 行-第 9 页第 19 行）：授权过程可能需要使用与移动设备所执行的相同的数据和算法在授权端计算动态认证码，并将计算的结果与接收到的动态码作比较以确定计算的结果与接收到的码相匹配（相当于其中将所接收的密码与密码计算的结果进行比较，所述结果基于与交易相关联的所述临时的使用密码的密钥而生成）。因此，在其引用的权利要求 1 不具备创造性的情况下，权利要求 11 不具备专利法第 22 条第 3 款所规定的创造性。

11、权利要求 12 是权利要求 11 的从属权利要求，其附加技术特征被对比文件 2 公开（参见说明书第 4 页第 1 行-第第 5 页第 28 行、第 8 页第 1 行-第 9 页第 19 行）：不可预测数据包括交易额等，设备使用不可预测数据及其它保密数据来生成动态授权码，授权过程可能需要使用与移动设备所执行的相同的数据和算法在授权端计算动态认证码，并将计算的结果与接收到的动态码作比较以确定计算的结果与接收到的码相匹配。因此，在其引用的权利要求 11 不具备创造性的情况下，权利要求 12 不具备专利法第 22 条第 3 款所规定的创造性。

Mastercard, Ex1002, p. 721

12、权利要求 13 是权利要 12 的从属权利要求，在交易授权过程中，发送交易的值是本领域的常用技术手段。IS08583 是常用的数据格式。因此，在其引用的权利要求 12 不具备创造性的情况下，权利要求 13 不具备专利法第 22 条第 3 款所规定的创造性。

13、权利要求 14 是权利要求 3 的从属权利要求，对比文件 1 公开了（参见说明书第[0021]-[0033]段）：POS 终端可以将数量直接发送给支付服务器，并传送支付码，移动终端将数量等发送给支付服务器，支付服务器分解支付码，比较一次性数字密码及随机数，验证其正确性，验证通过后，向 POS 确认交易。在对比文件 1 公开了销售点终端及移动终端都能发送不可预知数据的基础上，为了避免数据被篡改，本领域技术人员容易想到在服务器端比较两数据是否相同，这是信息验证领域的常用技术手段。因此，在其引用的权利要求 3 不具备创造性的情况下，权利要求 14 不具备专利法第 22 条第 3 款所规定的创造性。

14、权利要求 15 是权利要求 14 的从属权利要求，对比文件 1 公开了（参见说明书第[0021]-[0033]段）：将交易数量发送到支付服务器。对比文件 2 公开了（参见说明书第 4 页第 1 行-第第 5 页第 28 行、第 8 页第 1 行-第 9 页第 19 行）：该认证码输出设备可将生成的动态认证码呈现给用户，诸如通过 LCD 屏幕或其它显示器，并将其随后发送至受权端。在此基础上，当对交易数据进行验证时，本领域技术人员容易想到将其显示到移动设备的显示器，此外，验证交易量数据是交易验证时的常用技术手段。因此，在其引用的权利要求 14 不具备创造性的情况下，权利要求 15 不具备专利法第 22 条第 3 款所规定的创造性。

15、权利要求 16 是权利要求 3 的从属权利要求，其附加技术特征被对比文件 1 公开（参见说明书第[0021]-[0033]段）：移动终端将交易数量发送到支付服务器。因此，在其引用的权利要求 3 不具备创造性的情况下，权利要求 16 不具备专利法第 22 条第 3 款所规定的创造性。

16、权利要求 17 是权利要求 3 的从属权利要求，然而，ISO7816-4 数据协议是常用的数据通信协议，因此，POS 命令通信及设备响应通信遵守 ISO7816-4 数据协议是数据通信领域的常用技术手段。因此，在其引用的权利要求 3 不具备创造性的情况下，权利要求 17 不具备专利法第 22 条第 3 款所规定的创造性。

17、权利要求 18 是权利要求 3 的从属权利要求，其附加技术特征被对比文件 1 公开（参见说明书第[0021]-[0033]段）：支付可以采用近场通信。因此，在其引用的权利要求 3 不具备创造性的情况下，权利要求 18 不具备专利法第 22 条第 3 款所规定的创造性。

18、权利要求 19 是权利要求 3 的从属权利要求，其附加技术特征被对比文件 1 公开（参见说明书第[0021]-[0033]段）：移动终端保存一次性数字密码以便下次交易使用，基于一次性数字密码生成支付码。因此，在其引用的权利要求 3 不具备创造性的情况下，权利要求 19 不具备专

Mastercard, Ex1002, p. 722

利法第22条第3款所规定的创造性。

19、权利要求20是权利要求3的从属权利要求，哈希是常用的数据加密方式。因此，在其引用的权利要求3不具备创造性的情况下，权利要求20不具备专利法第22条第3款所规定的创造性。

二、针对申请人意见陈述的答复

申请人认为：1、对比文件1并没有公开用于生成被发送到POS终端的“密码”的“永久的使用密码的密钥”。尽管对比文件1确实提到“密钥”，但该密钥不是永久性的，其也不是使用密码的密钥，并且也不是用于生成密码；“支付号码”不是密码；2、对比文件1未能公开“临时的使用密码的密钥”，以及移动设备“使用所述不可预知数据和所述临时的使用密码的密钥来产生密码，且制定包含使用所述临时的使用密码的密钥产生的密码的响应APDU”。对比文件3既没有教导交易缓存也没有教导临时的使用密码的密钥；3、权利要求20记载了密码是哈希。

审查员认为：1、对比文件1公开了（参见说明书第[0021]-[0033]段）：支付码包括一次性数字密钥及随机数，一次性数字密钥从支付服务器自动发送到移动终端，一次性数字密钥能通过与随机数相乘等方式计算得到支付码。由此可知，对比文件1与本申请一样，都是通过一次性数字密钥（相当于密钥）生成支付码（相当于密码）。虽然该密钥不是永久性的，但对比文件3中给出了利用远程安全元件进行交易支付的启示，而在安全元件进行安全交易的过程中，利用永久的密钥生成密码以授权交易，这是本领域的常用技术手段，例如对比文件2中公开了：移动设备上的软件生成电路具有典型智能卡几乎全部的功能（相当于安全元件），移动处理设备使用（诸如加密密钥之类的）密钥120来生成动态认证码130，密钥120可以是DES密钥、私钥、公钥、上述的某些组合、或者用于加密或生成用于后续认证的保密消息的任何其它数据，密钥可保存在例如移动处理设备的应用存储器中；2、对比文件1公开了：一次性数字密钥（相当于临时使用的密钥）；对比文件2公开了：加密密钥或密钥对中的一个或多个密钥通过使用之前由用户输入的PIN和移动设备标识符来加密（如通过三重DES技术）作为临时密钥以生成个人化数据，除密钥120和交易计数器以外还基于该不可预测数据来生成应用密文（相当于使用所述不可预知数据和所述临时的使用密码的密钥来产生密码）；此外，在对比文件3公开了利用远程安全元件进行交易支付的基础上，本领域技术人员容易想到将安全元件相关的密钥等由远程发送到移动设备；3、哈希是常见的数据加密方式，在对比文件2公开了密钥120可以是DES密钥、私钥、公钥、上述的某些组合的基础上，本领域技术人员容易想到利用哈希进行加密。

基于上述理由，本申请的独立权利要求以及从属权利要求都不具备创造性，同时说明书中也没有记载其他任何可以授予专利权的实质性内容，本申请也不具备被授予专利权的前景。如

纸件申请，回函请寄：100088 北京市海淀区蓟门桥西土城路6号 国家知识产权局专利局受理处收
电子申请，应当通过电子专利申请系统以电子文件形式提交相关文件。除另有规定外，以纸件等其他形式提交的文件视为未提交。

Mastercard, Ex1002, p. 723

果申请人不能在本通知书规定的答复期限内提出充分的理由，本申请将被驳回。

审查员姓名：贺龙萍　　审查员代码：295930

纸件申请，回函请寄：100088 北京市海淀区蓟门桥西土城路 6 号　国家知识产权局专利局受理处收
电子申请，应当通过电子专利申请系统以电子文件形式提交相关文件。除另有规定外，以纸件等其他形式提交的文件视为未提交。

Electronic Acknowledgement Receipt

EFS ID:	29238578
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Customer Number:	44654
Filer:	John L. Adair/Margarita Marquez
Filer Authorized By:	John L. Adair
Attorney Docket Number:	STAPP1100-5
Receipt Date:	17-MAY-2017
Filing Date:	30-AUG-2012
Time Stamp:	16:06:21
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		STAPP1100-5_IDS_05-17-2017.pdf	1064955 21a7e81756899c385e7f1be3952a52013b5fc342	yes	3

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	2	
	Information Disclosure Statement (IDS) Form (SB08)		3	3	
Warnings:					
Information:					
2	Non Patent Literature	STAPP1100_Ref_C12.pdf	14933207 9a745da8d2ed561e5aeade1f140f86e1d88b2a2c4	no	24
Warnings:					
Information:					
		Total Files Size (in bytes):	15998162		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. (Opt.) **STAPP1100-5**

First Named Inventor **C. Douglas Yeager**	
Application Number **13/599,647**	Date Filed **August 30, 2012**
Title **SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE (as amended)**	
Group Art Unit **3695**	Examiner **Puttaiah, Asha**
Confirmation Number **1919**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATION OF TRANSMISSION UNDER 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on May 15, 2017.

M. Marquez

Margarita Marquez

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. A copy of foreign patent documents as well as the information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

☐ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☐ This Information Disclosure Statement is being submitted before the mailing of a first Office action on the merits; or

☒ This Information Disclosure Statement is being submitted before the mailing of a first Office action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

Furthermore, pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application.

Applicant does not believe any fees are due and owing at this time. If Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

SPRINKLE IP LAW GROUP
Attorneys for Applicant

John L. Adair
Reg. No. 48,828

Dated: May 11, 2017

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 317-9088

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/599,617	08/30/2012	C. Douglas YEAGER	STAPP1100-5	1919

44654 7590 06/05/2017

Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705

EXAMINER
PUTTALAH, ASHA

ART UNIT	PAPER NUMBER
3695	

MAIL DATE	DELIVERY MODE
06/05/2017	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 13/599,647	Applicant(s) YEAGER, C. DOUGLAS	
	Examiner ASHA PUTTAIAH	Art Unit 3695	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/14/16*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *30-58* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *30-58* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *3 Feb 17; 17 May 17*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

1. The present application is being examined under the pre-AIA first to invent provisions.

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 14 December 2016 has been entered.

3. The following is a non- final office action in response to the request for continuation filed 14 December 2016.

4. No amendments have been submitted. Claims 1-29 were previously cancelled. Claims 30-58 have been examined and are pending.

Specification

5. The use of the trademark VISA® and MASTERCARD® has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology (® or ™).

6. Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Response to Arguments

7. Applicant's arguments filed 14 December 2016 have been fully considered but they are not persuasive.

8. With regard to the rejections under 35 USC 101, Applicant's arguments are persuasive. The instant invention is similar to the patent eligible claims in Bascom in that the instant invention is directed to providing a technical solution to a technical problem (security issues specific to situations requiring a mobile device to be interrogated) in an effort to improve mobile device/point of sale payment technology.

9. With regard to the rejections under 35 USC 103, Applicant argues that the Examiner's reliance on Manduley is 'misplaced' because the teaching does not show that the 'encryption used by the smart card with card readers" is changed in any way. (Applicant's response pg. 14) .

10. Examiner respectfully disagrees. It is noted that Manduley is cited a to show the updating an encryption key (i.e. receiving the second non-permanent cryptographic key ...and replacing the first non-permanent cryptographic key with non-permanent cryptographic key...) ((See at least Manduley, Fig. 4 update encryption key, C2L 29-35, update an encryption key used to generate the encryption; C4L22-41 updated key) (see also C4L 15-21, invention response may also include variable information reflecting the history of transactions made using the card) .It should be noted that the update of the encryption key occurs after validation. If there is an inconsistency or an improper decryption the card is

deactivated (C4L34-57; C5L36L50). This is a change in the underlying smart card. Applicant's argument that the combination of the Royyuro and Manduley would not disclose the invention as claimed is not persuasive as Manduley allows for the updating of the encryption key/card deactivation after 'inspection/'validation. Therefore the claims are disclosed as recited. Applicant seems to be interpreting the claims more narrowly/specifically than recited.

Claim Rejections - 35 USC § 112

11. The following is a quotation of 35 U.S.C. 112(b):

> (B) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

12. **Claims 42, 43, 57 and 58** are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

13. **Claims 42 and 57** recite "Track 2 format." The limitation seems to be specifying a 'standard format.' As such render the claim indefinite as an industry standard can change upon updates and is therefore, transitory-in-nature. Consequently, the standard limitation without a set-in-stone definition renders the metes and bounds of the claim confusing.

14. **Claims 43 and 58** recite a "BER-TLV format." The limitation specifying an ISO standard (BER-TLV format) render the claim indefinite as the ISO standard is an industry standard which can change upon updates and is therefore, transitory-in-nature. Consequently, the ISO standard limitation without a set-in-stone definition renders the metes and bounds of the claim confusing.

15. Applicant is respectfully requested to correct the deficiencies noted above. Applicant is also required to provide citation to the original disclosure for any amendments.

Claim Rejections - 35 USC § 103

16. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. **Claims 30, 31, 33, 34, 35, 37, 38, 39, 40, 41, 42, 44, 45, 47, 48, 49, 51, 52, 53, 54, 55, 56, and 57** are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over US 20100185545 A1, Royyuru et al. hereinafter referred to as Royyuru further in view of US 5737423, Manduley hereinafter referred to as Manduley.

18. **Claims 30 and 44**

Royyuru *discloses a method for secure application-based participation in a payment card transaction authorization process by a mobile device, and a system for secure application-based participation by a mobile device in point-of-sale interrogations, the system comprising:*

a mobile device (See at least Royyuru, Fig. 3 [0021] mobile device) *comprising:*

a controller configured to route communications received over a communication channel from an electronic reader; a wireless interface to connect

to a wireless network; a processor; a computer readable storage medium accessible by the processor storing an application interrogable for digital credential data to authorize transactions against an account having a digital credential, the application executable in an operating system of the mobile device to participate in interrogations, (See at least Royyuru, Fig. 1-3 [0021] mobile device) *wherein the application is executable to: during an interrogation:*

- *receiving over a wireless network at a mobile device a first non-permanent cryptographic key associated with an account having a corresponding digital credential, wherein the mobile device comprises an operating system and an application executable in the operating system, the application interrogable for digital credential data corresponding to the account, wherein the application does not access a permanent cryptographic key associated with the account during interrogations;* (See at least Royyuru, Fig. 3 [0021] mobile device, [0033] dynamic cryptograms… Dynamic Transaction Cryptogram)
- *locally storing a first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account; ;* (See at least Royyuru, pg. 9, Table, Card-Key, CK, random CK can by system generated…)
- *participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device comprising:*

- *receiving at least one POS command communication sent by the POS terminal over a communications channel, wherein the at least one POS command communication comprises a request for digital credential data to authorize a transaction against the account;* (See at least Royyuru, [0044-46] read information from presentation instrument... passed from POS... and/or merchant system via network to payment processor system for approval and/or processing of the transaction)
- *generating a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram; and* (See at least Royyuru, Claim 1, Fig. 3 [0021] mobile device, [0033] dynamic cryptograms... Dynamic Transaction Cryptogram)
- *responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to an electronic reader through the communication channel, the at least one device response communication comprising at least a portion of the digital*

credential data, (See at least Royyuru, [0033] dynamic cryptograms… Dynamic Transaction Cryptogram)

- *wherein the at least a portion of the digital credential data comprises the response cryptogram and an account identifier for the account;* (See at least Royyuru, Fig. 3 [0021] mobile device, [0033] dynamic cryptograms… Dynamic Transaction Cryptogram ; pg. 9 table Pseudo-PAN, DTC)

Royyuru further discloses the single use cryptogram and a random card key which is system-generated (See at least Royyuru, [0033] dynamic cryptograms… Dynamic Transaction Cryptogram…valid for single transaction; pg. 9 table)

Royyuru does not directly disclose the following; however, Manduley teaches:

- *receiving a second non-permanent cryptographic key at the mobile device, wherein the second non-permanent cryptographic key is associated with the account; and* (See at least Manduley, Fig. 4 update encryption key, C2L 29-35, update an encryption key used to generate the encryption)
- *replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key as the local cryptographic key associated with the account prior to the*

application participating in a subsequent interrogation. (See at least Manduley, Fig. 4 update encryption key, C2L 29-35, update an encryption key used to generate the encryption; C4L22-41 updated key)

The Supreme Court has supported in *KSR International Co. Teleflex Inc. (KSR), 550US___, 82 USPQ2d 1385 (2007),* that merely applying a known technique to a known method, yield predictable results, render the claimed invention obvious over such combination. In the instant case, Royyuru discloses a method and system of handling information related to a financial transactions including mobile devices/card including utilizing dynamic cryptograms including a single use cryptographic key. Manduley is merely another method and system of inspecting transactions of smart cards and updating/re-keying of encryption keys. One of ordinary skill in the art would clearly recognize that this combination would lead to a predictable result (i.e. a method and system of handling information related to a financial transactions including mobile devices/card including utilizing dynamic cryptograms including a single use cryptographic key including updating/re-keying/re-placing the cryptographic key). As such the claimed invention is obvious over Royyuru / Manduley.

19. Claims 31 and 45

Royyuru and Manduley disclose the invention as claims above in Claims 30 and 44.

Royyuru further discloses:

- *wherein the mobile device is an NFC emulating device.* (See at least Royyuru, [0044-0046] NFC modules)

20. Claims 33 and 47

Royyuru and Manduley disclose the invention as claims above in Claims 30 and 44.

Royyuru further discloses:

- *wherein the interrogation conforms to a card specification, the set of inputs is specified by the card specification and the at least one device response is formulated according to the card specification.* (See at least Royyuru, pg. 9 table Pseudo-PAN, DTC)

21. Claims 34 and 48

Royyuru and Manduley disclose the invention as claims above in Claims 33 and 47.

Royyuru further discloses:

- *wherein the request for digital credential data comprises a request for a first cryptogram according to the card specification and the at least one device response communication comprises a second*

cryptogram, wherein the second cryptogram is the response cryptogram. (See at least Royyuru, pg. 9 table Pseudo-PAN, DTC…wherein the DTC is the response cryptogram)

22. Claims 35 and 49

Royyuru and Manduley disclose the invention as claims above in Claims 30 and 44.

Royyuru further discloses:

- *wherein generating the response cryptogram comprises encrypting the set of inputs using the local cryptographic key according to a digital encryption standard (DES) calculation to generate an output, wherein the response cryptogram includes a portion, but not all, of the output.* (See at least Royyuru, [0032] dynamic Primary Account Number (PAN)…portion of the real PAN can be retained)

23. Claim 37

Royyuru and Manduley disclose the invention as claims above in Claims 30 and 44.

Royyuru further discloses:

- *prior to the interrogation, generating at a remote system the first non-permanent cryptographic key,* (See at least Royyuru, pg. 9, Table, Card-Key, CK, random CK can by system generated…)
- *associating the first non-permanent cryptographic key with the account, and* (See at least Royyuru, Claim 1, Fig. 3 [0021] mobile

device, [0033] dynamic cryptograms… Dynamic Transaction Cryptogram)

- *sending the first non-permanent cryptographic key and the account identifier to the mobile device over the wireless network; and* (See at least Royyuru, pg. 9, Table, Card-Key, CK, random CK can by system generated…)

Royyuru does not directly disclose; however, Manduley teaches:

- *after the interrogation generating at the remote system, the second non-permanent cryptographic key, associating the second non-permanent cryptographic key with the account and* (See at least Manduley, Fig. 4 update encryption key, C2L 29-35, update an encryption key used to generate the encryption)
- *sending the second non-permanent cryptographic key and the account identifier to the mobile device over the wireless network.* (See at least Manduley, Fig. 4 update encryption key, C2L 29-35, update an encryption key used to generate the encryption; C4L22-41 updated key)

24. Claims 38 and 53

Royyuru and Manduley disclose the invention as claims above in Claims 37 and 52.

Royyuru further discloses:

- *wherein the digital credential comprises a secure element representation maintained at the remote system.* (See at least Royyuru, [0033] institution key; pg. 8-9 table [0057] institution key…stored in the database or repository of the payment processor)

25. Claims 39 and 54

Royyuru and Manduley disclose the invention as claims above in Claims 30 and 44.

Royyuru further discloses:

- *receiving an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the response cryptogram and the account identifier;* (See at least Royyuru, [0048] authorization request…PAN …DTC)
- *determining a current non-permanent cryptographic key associated with the account using the account identifier;* (See at least Royyuru, pg. 9, Table, Card-Key, CK, random CK can by system generated…)
- *calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account;* (See at least Royyuru, Fig. 3 [0021] mobile device, [0033] dynamic cryptograms… Dynamic Transaction Cryptogram ; pg. 9 table Pseudo-PAN, DTC [0047])
- *verifying a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram;* (See at least Royyuru, [0044-46] read

information from presentation instrument... passed from POS... and/or merchant system via network to payment processor system for approval and/or processing of the transaction…approval or denial response….)

- *and sending an authorization response to the POS terminal,* (See at least Royyuru, [0044-46] read information from presentation instrument... passed from POS... and/or merchant system via network to payment processor system for approval and/or processing of the transaction [0049-0050] if authorized, and authorization code…)
- *wherein the data contained in the authorization response is determined, at least in part, by the verifying the correctness of the response cryptogram.* (See at least Royyuru, [0044-46] read information from presentation instrument... passed from POS... and/or merchant system via network to payment processor system for approval and/or processing of the transaction[0048-0050] DTC… decryption module)

26. Claims 40 and 55

Royyuru and Manduley disclose the invention as claims above in Claims 39 and 54.

Royyuru further discloses:

- *wherein: the set of inputs comprises unpredictable data; the authorization data comprises the unpredictable data; and the calculated cryptogram is calculated using the unpredictable data.* (See at least Royyuru, [0051] unpredictable

numbers or counters; pg. 10 table, unpredictable number, DTC … combining several fields including unpredictable number)

27. Claims 41 and 56

Royyuru and Manduley disclose the invention as claims above in Claims 40 and 55.

Royyuru further discloses:

- *wherein the POS command communications comprise the unpredictable data.* (See at least Royyuru, [0051] unpredictable numbers or counters; pg. 10 table, unpredictable number)

28. Claims 42 and 57

Royyuru and Manduley disclose the invention as claims above in Claims 41 and 55.

Royyuru further discloses:

- *wherein the authorization data further comprises values from the transaction and wherein the POS terminal communicates the values from the transaction, the response cryptogram and the account identifier to the remote system in track 2 format.* (See at least Royyuru, pg. 7 [0049] Track 2 layout)

29. Claim 51

Royyuru and Manduley disclose the invention as claims above in Claim 44.

Royyuru does not directly disclose; however, Manduley teaches:

- *wherein the mobile device is programmed to request a new non-permanent cryptographic key after the interrogation.* (See at least Manduley, Fig. 4 update encryption key, C2L 29-35, update an encryption key used to generate the encryption; C4L22-41 updated key)

30. Claim 52

Royyuru and Manduley disclose the invention as claims above in Claim 44. Royyuru further discloses:

- *further comprising a remote computer system configured to generate the non-permanent cryptographic keys associated with the account and send each of the non-permanent cryptographic keys and the account identifier to the mobile device over the wireless network.* (See at least Royyuru, [0037] wireless network)

31. **Claims 32 and 46** are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Royyuru further in view of Manduley further in view of non-patent literature Wikipedia: Cryptographic hash function (https://en.wikipedia.org/w/index.php?title=Cryptographic_hash_function&oldid=344034775) 14 Feb 2010 hereinafter referred to as Wikipedia:Hash

32. Claims 32 and 46

Royyuru and Manduley disclose the invention as claims above in Claims 30 and 44.

Royyuru does not directly disclose the following; however, Wikipedia teaches:

Cryptographic hash function teaches:

- *wherein the response cryptogram is a hash.* (See at least Wikipedia: Cryptographic hash function : functions have many information security applications including authentication)

The Supreme Court has supported in *KSR International Co. Teleflex Inc. (KSR), 550US___, 82 USPQ2d 1385 (2007),* that merely applying a known technique to a known method, yield predictable results, render the claimed invention obvious over such combination. In the instant case, Royyuru discloses a method and system of handling information related to a financial transactions including mobile devices/card including utilizing dynamic cryptograms including encrypting keys. Wikipedia: Hash is merely a description/definition of a known procedure used in encryption. One of ordinary skill in the art would clearly recognize that this combination would lead to a predictable result (i.e. a method and system of handling information related to a financial transactions including mobile devices/card including utilizing dynamic cryptograms including using known techniques/procedures such as the use of hash). As such the claimed invention is obvious over Royyuru / Wikipedia: Hash.

33. **Claims 36 and 50** are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Royyuru further in view of Manduley further in view of US 2010/0317318 Al, Carter hereinafter referred to as Carter.

34. **Claims 36 and 50**

Royyuru and Manduley disclose the invention as claims above in Claims 30 and 44.

Royyuru does not directly disclose; however, Carter teaches:

- *wherein the mobile device does not have connectivity to the wireless network during the interrogation.* (See Carter, [0032] offline purchase transaction…proximity reader… POS terminal…mobile telephone [0042] transaction clearing application.... clear office transactions)

The Supreme Court has supported in *KSR International Co. Teleflex Inc. (KSR), 550US___, 82 USPQ2d 1385 (2007),* that merely applying a known technique to a known method, yield predictable results, render the claimed invention obvious over such combination. In the instant case, Royyuru discloses a method and system of handling information related to a financial transactions including mobile devices/card including utilizing dynamic cryptograms including encrypting keys. Carter is a method of authorizing transactions using a mobile device including an offline feature. One of ordinary skill in the art would clearly recognize that this combination would lead to a predictable result (i.e. a method and system of handling information related to a financial transactions including

mobile devices/card including utilizing dynamic cryptograms including authorizing transactions using a mobile device including an offline feature). As such the claimed invention is obvious over Royyuru /Carter.

35. **Claims 43 and 58** are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Royyuru further in view of Manduley further in view of ISO 7816-4(http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816-4_annex-d.aspx) 13 Feb 2009 hereinafter referred to as ISO 7816-4.

36. **Claims 43 and 58**

Royyuru and Manduley disclose the invention as claims above in Claims 41 and 55.

Royyuru does not directly disclose; however, ISO 7816-4 teaches:

- *wherein the authorization data further comprises values from the transaction and wherein the POS terminal communicates values from the transaction, the response cryptogram and the account identifier in BER-TLV format.* (See at least ISO 7816-4, BER-TLV data object…)

The Supreme Court has supported in *KSR International Co. Teleflex Inc. (KSR), 550US___, 82 USPQ2d 1385 (2007),* that merely applying a known technique to a known method, yield predictable results, render the claimed invention obvious over such combination. In the instant case, Royyuru discloses a method and system of handling information related to a financial transactions

including mobile devices/card including utilizing dynamic cryptograms including a single use cryptographic key. ISO 7816-4 is a known protocol standard/technology to establish communications. One of ordinary skill in the art would clearly recognize that this combination would lead to a predictable result (i.e. a method and system of handling information related to a financial transactions including mobile devices/card including utilizing dynamic cryptograms including a single use cryptographic key which uses a known protocol standard to establish communications). As such the claimed invention is obvious over Royyuru / ISO 7816-4.

Conclusion

37. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US 20100211504 A1; US 20110246369 A1

38. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ASHA PUTTAIAH whose telephone number is (571)270-1352. The examiner can normally be reached on Monday- Friday 8:00am - 5:00 pm EST.

39. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ryan Donlon can be reached on (571) 270-3602. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

40. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ASHA PUTTAIAH/

Primary Examiner, Art Unit 3695

Notice of References Cited	Application/Control No. 13/599,647	Applicant(s)/Patent Under Reexamination YEAGER, C. DOUGLAS	
	Examiner ASHA PUTTAIAH	Art Unit 3695	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-5,636,280 A	06-1997	Kelly; Tadhg	G06F21/31	380/281
*	B	US-2012/0109764 A1	05-2012	Martin; Philippe	G06Q20/204	705/17
*	C	US-2004/0143550 A1	07-2004	Creamer, Thomas E.	G06Q20/04	705/41
*	D	US-2008/0040285 A1	02-2008	Wankmueller; John	G06Q20/32	705/67
*	E	US-2010/0185545 A1	07-2010	Royyuru; Vijay K.	G06Q20/04	705/67
*	F	US-5,737,423 A	04-1998	Manduley; Flavio M.	G06K19/0723	380/273
*	G	US-2010/0317318 A1	12-2010	Carter; Ronald D.	G06Q20/20	455/408
*	H	US-2011/0246369 A1	10-2011	de Oliveira; Marcelo Gomes	G06Q20/382	705/64
*	I	US-2010/0211504 A1	08-2010	Aabye; Christian	G06Q20/10	705/44
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author. Title Date, Publisher. Edition or Volume. Pertinent Pages)
*	U	ISO 7816-4(http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816-4_annex-d.aspx) 13 Feb 2009
*	V	Wikipedia: Cryptographic hash function (https://en.wikipedia.org/w/index.php?title=Cryptographic_hash_function&oldid=344034775) 14 Feb 2010
	W	
	X	

*A copy of this reference is not being furnished with this Office action (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13599647	YEAGER, C. DOUGLAS
	Examiner	Art Unit
	ASHA PUTTAIAH	3695

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor Search	9/27/2015	AP
East Search (please see attached)	9/29/2015	AP
East Search (please see attached)	6/10/2016	AP
East Search (please see attached)	5/29/2017	AP

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

	/ASHA PUTTAIAH/ Primary Examiner.Art Unit 3695

INFORMATION DISCLOSURE STATEMENT				Application Number	13/599,647
				Filing or 371 (c) Date:	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	Puttaiah, Asha
Sheet	1	of	1	Attorney Docket Number	STAPP1100-5

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C12	Office Action issued for Chinese Patent Application No. 201280053080.6, mailed March 7, 2017, 24 pages.	

Examiner Signature	/ASHA PUTTAIAH/	Date Considered	05/29/2017

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.P/

Substitute Form PTO/SB/08a

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/599,647
				Filing Date	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	Puttaiah, Asha
Sheet	1	of	1	Attorney Docket Number	STAPP1100-5

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	B3	CN101048794	10-03-2007	Mastercard International Inc.	

Examiner Signature	/ASHA PUTTAIAH/	Date Considered	05/29/2017

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.P/

Substitute Form PTO/SB/08b

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/599,647
				Filing Date	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	Puttaiah, Asha
Sheet	1	of	1	Atty Docket Number	STAPP1100-5

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C8	Patent Examination Report for Australian Patent Application No. 2012301897, issued on November 22, 2016, 4 pages.	
	C9	Office Action for Chinese Patent Application No. 201280053080.6, issued on June 22, 2016, 20 pages.	
	C10	Search Report issued for European Patent Application No. 12827026.1, issued on June 10, 2016, 6 pages.	
	C11	Office Action for Canadian Patent Application No. 2,846,462, issued November 4, 2016, 3 pages.	

Examiner Signature	/ASHA PUTTAIAH/	05/29/2017 Date Considered	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.P/

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	56	(mobile same (POS or point-of-sale or "point of sale")) same cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2017/05/29 16:02
L2	53	((mobile same (POS or point-of-sale or "point of sale")) same cryptogram) and (first or second)	US-PGPUB; USPAT; USOCR	AND	OFF	2017/05/29 16:02
L3	2	((mobile same (POS or point-of-sale or "point of sale")) same cryptogram) and ((first or second) same replac$4)	US-PGPUB; USPAT; USOCR	AND	OFF	2017/05/29 16:02
L4	50	((mobile same (POS or point-of-sale or "point of sale")) same cryptogram) and (first and second)	US-PGPUB; USPAT; USOCR	AND	OFF	2017/05/29 16:08
L5	5	((mobile same (POS or point-of-sale or "point of sale")) same cryptogram) and ((first and second) same (replac$3 or updat$3))	US-PGPUB; USPAT; USOCR	AND	OFF	2017/05/29 16:09
S1	20	("20040118914" | "20070266131" | "20070278291" | "20110140841" | "20060022033" | "20090124234" | "20100185545" | "20100274726" | "6199762" | "7774231" | "20100207742" | "20080046367" | "20070075133" | "20090006262" | "20110112918" | "20060224470" | "20030163708" | "20080238610" | "20090044012" | "20080219444").PN.	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:04
S2	84	"pos command"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:05
S3	2	"expected cryptogram"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:06
S4	0	"pos command" with (expected adj value adj cryptogram)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:07
S5	0	"pos command" same (expected adj value adj cryptogram)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:07
S6	0	"pos command" same (expected with value with cryptogram)	US-PGPUB; USPAT;	AND	OFF	2015/09/24 22:07

			USOCR			
S7	1	"pos command" same (cryptogram)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:07
S8	1	"pos command" and cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:07
S9	1	"unexpected cryptogram"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:08
S11	20	cryptogram same value same expected	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:09
S12	5	cryptogram same value same expected and (mobile with point)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:09
S13	20	cryptogram same (mobile with point)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:10
S14	6	S1 and calculat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:19
S15	123874	(cryptogram or authenticat$5) calculatS3	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:23
S16	20011	(cryptogram or authenticat$5) same calculat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:24
S17	11595	(cryptogram or authenticat$5) with calculat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:24
S18	101	(cryptogram or authenticat$5) with calculat$3 and (permanent near4 key)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:25
S19	96	(cryptogram or authenticat$5) with calculat$3 and (permanent near3 key)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:25
S20	1	(cryptogram or authenticat$5) with calculat$3 and (remote with permanent near3 key)	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:26
S21	1	(cryptogram or authenticat$5) with calculat$3 and (remote same (permanent near3 key))	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:27
S22	56	(remote same (permanent near3 key))	US-	AND	OFF	2015/09/24

			PGPUB; USPAT; USOCR			22:27
S23	56	(remote same (permanent near3 key))	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/24 22:28
S24	5	"pos command" and "unpredictable"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 13:26
S25	458	"unpredictable data"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 13:27
S26	0	"unpredictable data" and crytogra,	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 13:27
S27	0	"unpredictable data" and crytogram	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 13:27
S28	7	"unpredictable data" and cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 13:27
S29	29	$2expected with cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 13:29
S30	72	ISO7816-4	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 13:58
S31	4	ISO7816-4 and POS	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 14:01
S32	20	("2008/0040285").URPN.	USPAT	AND	OFF	2015/09/28 20:08
S33	143	transaction adj PIN	USPAT	AND	OFF	2015/09/28 20:12
S34	18	transaction adj PIN with amount	USPAT	AND	OFF	2015/09/28 20:12
S35	51	transaction adj PIN with amount	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:12
S36	84	"pos command"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:14
S37	0	S35 and S36	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:14
S38	0	S35 and S36	US-	AND	OFF	2015/09/28

			PGPUB; USPAT; USOCR			20:14
S39	18	S35 and S34	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:14
S40	0	transaction adj PIN with amount and "unpredictable data"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:15
S41	0	(transaction adj PIN with amount) and "unpredictable data"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:16
S42	0	(transaction adj PIN with amount) and "unpredictable"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:16
S43	20	("20040118914" | "20070266131" | "20070278291" | "20110140841" | "20060022033" | "20090124234" | "20100185545" | "20100274726" | "6199762" | "7774231" | "20100207742" | "20080046367" | "20070075133" | "20090006262" | "20110112918" | "20060224470" | "20030163708" | "20080238610" | "20090044012" | "20080219444").PN.	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:44
S44	0	S34 and S43	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:44
S45	4	S43 and cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/28 20:44
S46	20	("20040118914" | "20070266131" | "20070278291" | "20110140841" | "20060022033" | "20090124234" | "20100185545" | "20100274726" | "6199762" | "7774231" | "20100207742" | "20080046367" | "20070075133" | "20090006262" | "20110112918" | "20060224470" | "20030163708" | "20080238610" | "20090044012" | "20080219444").PN.	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/29 11:08
S47	84	"pos command"	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/29 11:08
S48	600	cryptogram same value	US-PGPUB; USPAT; USOCR	AND	OFF	2015/09/29 11:08
S49	33585	key with cryptographic	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:02
S50	7656	key with cryptographic with device	US-	AND	OFF	2016/06/06

			PGPUB; USPAT; USOCR			17:02
S51	183	(key adj cryptographic) same (device with stor$4) and "transaction"	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:14
S52	18	(key adj cryptographic) same (mobile with device with stor$4) and "transaction"	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:15
S53	88	(key adj cryptographic) same (mobile with device with stor$4) and authori$5	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:17
S54	0	(key adj cryptographic adj local) same (mobile with device with stor$4) and authori$5	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:19
S55	0	(key adj cryptographic adj local) same (mobile with device with stor$4)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:19
S56	0	(key adj cryptographic adj local) same (mobile with device)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:19
S57	571	key with cryptographic with local	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:25
S58	2	key with cryptographic with local with replac$5	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:25
S59	9	key with cryptographic with local same replac$5	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:39
S60	9	(key with cryptographic with local) same replac$5	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:39
S61	20	(key with cryptographic with (local or internal)) same replac$5	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 17:40
S62	1	"20100185545"	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/06 20:18
S63	8	("20020026414" | "20070156436" | "20090075592" | "20090143104" | "20090210308" | "20100153721" | "20110099079" | "20120317628").PN.	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/08 18:07
S64	14	(US-20100317318-$ or US-20070254712-$ or US-20050190769-$ or US-20080040285-$ or US-20120109764-$ or US-20140188738-$ or US-20100185545-$ or	US-PGPUB; USPAT	AND	OFF	2016/06/09 14:43

		US-20070156436-$ or US-20110099079-$).did. or (US-5636280-$ or US-3842629-$ or US-5196840-$ or US-7890997-$ or US-8996869-$).did.				
S65	0	S64 and rekey	US-PGPUB; USPAT	AND	OFF	2016/06/09 14:43
S66	5	S64 and re -key	US-PGPUB; USPAT	AND	OFF	2016/06/09 14:43
S67	0	S64 and re-key	US-PGPUB; USPAT	AND	OFF	2016/06/09 14:43
S68	21	(mobile adj device) same cryptogram same POS	US-PGPUB; USPAT	AND	OFF	2016/06/09 14:45
S69	21	(mobile adj device) same cryptogram same POS	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:45
S70	0	rekey with cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:47
S71	97	(rekey$3 or updat$3) with cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:48
S72	1	(rekey$3 or updat$3) with cryptogram same (dynamic or temporary or non-permanent)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:51
S73	51	(rekey$3 or updat$3) with cryptogram and (mobile with device)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:51
S74	51	((rekey$3 or updat$3) with cryptogram) and (mobile with device)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:52
S75	2	((rekey$3 or updat$3) with cryptogram) same (mobile with device)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:52
S76	11	((rekey$3 or updat$3) with cryptogram) and ((mobile with device) same key)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:54
S77	2363	((mobile with device) same key same (rekey$3 or updat$3))	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:56
S78	18	((mobile with device) same key same (rekey$3 or updat$3)) and cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:56
S79	6	((mobile with device) same key same (rekey$3 or updat$3)) same cryptogram	US-PGPUB;	AND	OFF	2016/06/09 14:57

			USPAT; USOCR			
S80	0	((mobile with device) same (key with (rekey$3 or updat$3))) same cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:58
S81	7	((mobile with device) same (key with (rekey$3 or updat$3))) and cryptogram	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 14:58
S82	4	S64 and updat$3	US-PGPUB; USPAT	AND	OFF	2016/06/09 15:09
S83	49711	((mobile with device) same (cryptographic with rekey$3 or updat$3))	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 15:11
S84	28348	((mobile with device) with (cryptographic with rekey$3 or updat$3))	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 15:12
S85	15	cryptogram with key with updat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 15:39
S86	1	(cryptogram with key with updat$3) same card	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 15:39
S87	4439	encryption with key with updat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 15:42
S88	2445	(encryption adj key) with updat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 15:42
S89	90	(card with (encryption adj key)) with updat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 15:42
S90	0	(card with (local near3 (encryption adj key))) with updat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 15:45
S91	15	((local or stored) with card with (encryption adj key)) with updat$3	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 15:45
S92	33	"BER-TLV"	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 16:25
S93	15	(US-20100317318-$ or US-20070254712-$ or US-20050190769-$ or US-20080040285-$ or US-20120109764-$ or US-20140188738-$ or US-20100185545-$ or US-20070156436-$ or US-20110099079-$).did. or (US-5636280-$ or US-3842629-S	US-PGPUB; USPAT	AND	OFF	2016/06/09 16:41

		or US-5196840-$ or US-7890997-$ or US-8996869-$ or US-5737423-$).did.				
S94	3	S93 and hash	US-PGPUB; USPAT	AND	OFF	2016/06/09 16:41
S95	199	(offline with transaction) same encryption	US-PGPUB; USPAT	AND	OFF	2016/06/09 18:04
S96	96	(offline with transaction) same (encryption with key)	US-PGPUB; USPAT	AND	OFF	2016/06/09 18:04
S97	0	(offline with transaction) same (encryption with key) same cryptogram	US-PGPUB; USPAT	AND	OFF	2016/06/09 18:04
S98	0	(offline with transaction) same (encryption with key) same hash	US-PGPUB; USPAT	AND	OFF	2016/06/09 18:04
S99	0	(offline with transaction) same (encryption with key) and (cryptogram)	US-PGPUB; USPAT	AND	OFF	2016/06/09 18:05
S100	6	(offline with transaction) same (encryption with key) and (hash)	US-PGPUB; USPAT	AND	OFF	2016/06/09 18:05
S101	6	(offline with transaction) same (encryption with key) and (hash)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 18:05
S102	2	(offline with transaction) same (encryption with key) and ((hash) same response)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 18:05
S103	2593	(encryption with key) and (hash with response)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 18:17
S104	357	(encryption with key) same (hash with response)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 18:19
S105	76	(encryption with key) same (hash with response) and transactions	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 18:19
S106	20	(encryption with key) same (hash with response) and (offline with transactions)	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 18:27
S107	0	("l30andoffline").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2016/06/09 19:42
S108	44	"l30" and offline	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 19:42
S109	44	"l30" and offline	US-PGPUB; USPAT;	AND	OFF	2016/06/09 19:42

			USOCR			
S110	43	"I30" and offline	US-PGPUB; USPAT	AND	OFF	2016/06/09 19:43
S111	15	(US-20100317318-$ or US-20070254712-$ or US-20050190769-$ or US-20080040285-$ or US-20120109764-$ or US-20140188738-$ or US-20100185545-$ or US-20070156436-$ or US-20110099079-$).did. or (US-5636280-$ or US-3842629-$ or US-5196840-$ or US-7890997-$ or US-8996869-$ or US-5737423-$).did.	US-PGPUB; USPAT	AND	OFF	2016/06/09 19:43
S112	1	S111 and offline	US-PGPUB; USPAT; USOCR	AND	OFF	2016/06/09 19:43
S113	15	(US-20100317318-$ or US-20070254712-$ or US-20050190769-$ or US-20080040285-$ or US-20120109764-$ or US-20140188738-$ or US-20100185545-$ or US-20070156436-$ or US-20110099079-$).did. or (US-5636280-$ or US-3842629-$ or US-5196840-$ or US-7890997-$ or US-8996869-$ or US-5737423-$).did.	US-PGPUB; USPAT	AND	OFF	2016/06/10 15:35
S114	0	S113 and "TLV"	US-PGPUB; USPAT	AND	OFF	2016/06/10 15:35
S115	8137	"TLV"	US-PGPUB; USPAT	AND	OFF	2016/06/10 15:35

EAST Search History (Interference)

<This search history is empty>

5/29/2017 4:13:14 PM
C:\Users\aputtaiah1\Documents\EAST\Workspaces\13599647.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13599647	YEAGER, C. DOUGLAS
	Examiner	Art Unit
	ASHA PUTTAIAH	3695

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	09/29/2015	06/10/2016	05/29/2017						
	1	✓	-	-						
	2	✓	-	-						
	3	✓	-	-						
	4	✓	-	-						
	5	✓	-	-						
	6	✓	-	-						
	7	✓	-	-						
	8	✓	-	-						
	9	✓	-	-						
	10	✓	-	-						
	11	✓	-	-						
	12	✓	-	-						
	13	✓	-	-						
	14	✓	-	-						
	15	✓	-	-						
	16	✓	-	-						
	17	✓	-	-						
	18	✓	-	-						
	19	✓	-	-						
	20	✓	-	-						
	21	✓	-	-						
	22	✓	-	-						
	23	✓	-	-						
	24	✓	-	-						
	25	✓	-	-						
	26	✓	-	-						
	27	✓	-	-						
	28	✓	-	-						
	29		-	-						
	30		✓	✓						
	31		✓	✓						
	32		✓	✓						
	33		✓	✓						
	34		✓	✓						
	35		✓	✓						
	36		✓	✓						

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13599647	YEAGER, C. DOUGLAS
	Examiner	Art Unit
	ASHA PUTTAIAH	3695

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	09/29/2015	06/10/2016	05/29/2017						
	37		✓	✓						
	38		✓	✓						
	39		✓	✓						
	40		✓	✓						
	41		✓	✓						
	42		✓	✓						
	43		✓	✓						
	44		✓	✓						
	45		✓	✓						
	46		✓	✓						
	47		✓	✓						
	48		✓	✓						
	49		✓	✓						
	50		✓	✓						
	51		✓	✓						
	52		✓	✓						
	53		✓	✓						
	54		✓	✓						
	55		✓	✓						
	56		✓	✓						
	57		✓	✓						
	58		✓	✓						

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/599,617	08/30/2012	C. Douglas YEAGER	STAPP1100-5	1919

44654 7590 09/25/2017

Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705

EXAMINER
PUTTALAH, ASHA

ART UNIT	PAPER NUMBER
3695	

MAIL DATE	DELIVERY MODE
09/25/2017	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Applicant-Initiated Interview Summary	**Application No.**	**Applicant(s)**	
	13/599,647	YEAGER, C. DOUGLAS	
	Examiner	**Art Unit**	
	ASHA PUTTAIAH	3695	

All participants (applicant, applicant's representative, PTO personnel):

(1) *ASHA PUTTAIAH*. (3) *C. Douglas Yeager*.

(2) *John Adair*. (4)_____.

Date of Interview: *06 September 2017*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☐ No.
If Yes, brief description: _____.

Issues Discussed ☒101 ☐112 ☒102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *Royyru and Manduley*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicants and Examiner discussed the proposed amendments and the novelty of the invention.Examiner suggested clarifying amendments. Applicants will consider the suggestions. No agreement was reached .

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☒ Attachment

/ASHA PUTTAIAH/ Primary Examiner, Art Unit 3695	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Background

[0003] In some payment technologies such as smartcard payment, a microchip referred to as a "Secure Element" (SE) is embedded into a payment card, a payment fob (medallion), a cell phone, or other mobile devices that may be used for making payments. For the purpose of simplifying language in this document, a device that houses the SE will be referred to as a "card" or "card device". It is important to note that the "card" or "card device" may not physically resemble the shape or size of a typical payment card and may come in various form factors such as embedded into a mobile phone or embedded into a removable storage or removable device. Also, it is important to note that the SE may be an emulated software based SE and not strictly hardware based. For example, virtually any electronic device with a digital memory and processor or controller may be adapted to emulate and pretend to be an SE.

Application at ¶ [0003]

Mastercard, Ex1002, p. 772

Permanent Cryptographic Key

[0165] Also, the card specification may define a cryptogram to be calculated by the card, SE, or mobile device based, at least in part, on a cryptographic key, where the cryptographic key is a "permanent cryptographic key". In this context, it is said that the cryptogram delivered by the mobile device is "expected" because the card specification indicates it will be calculated, at least in part, from a permanent cryptographic key and that is what the card specification expects. Used herein the term "permanent cryptographic key" refers to a cryptographic key that is unchanging (or static) throughout the life of a card, SE, mobile device, or digital credential.

Application at ¶ [0165]

[0041] Prior to card issuance, an SE is typically injected with personalization or "credential" data that is generated from a "Hardware Security Module" (HSM). The HSM securely contains the cryptographic keys and algorithms that relate to a particular banking application and more specifically may contain a set of individual digital credentials. An HSM typically is accessed in a secure environment and never allows direct access to master keys which are used to create diversified keys or to encrypt or decrypt input data that may be provided to the HSM.

Application at ¶ [0041]

An example of an HSM used in the industry at the time of this filing is currently distributed by SafeNet Inc. and is named the Luna EFT Mark II Edition. An example, from the MasterCard PayPass MSD v3.3 card specification document, of an encryption key that may be stored on the HSM is called an Issuer Master Key (IMK). The HSM can then, for example, use the embedded algorithms **204** to create a "diversified key for card verification code creation" (KDcvc3) from the IMK that is used for each individual card that is issued based on a certain algorithm that is also stored in the HSM. The HSM is

* * *

[0176] KDcvc3 calculation may be preformed inside the HSM because the HSM contains IMK. The application system will pass Y, which is defined as the PAN and PAN sequence number concatenated as an input to the HSM in conjunction with the IMK id to use. The HSM will respond back with the KDcvc3 as output. The KDcvc3 in this example would be considered a permanent cryptographic key because it will not change over the life of the digital credential, as none of the inputs to the calculation of KDcvc3 change over the life of the credential.

Application at ¶ ¶ [0149], [00176]

Figure 11

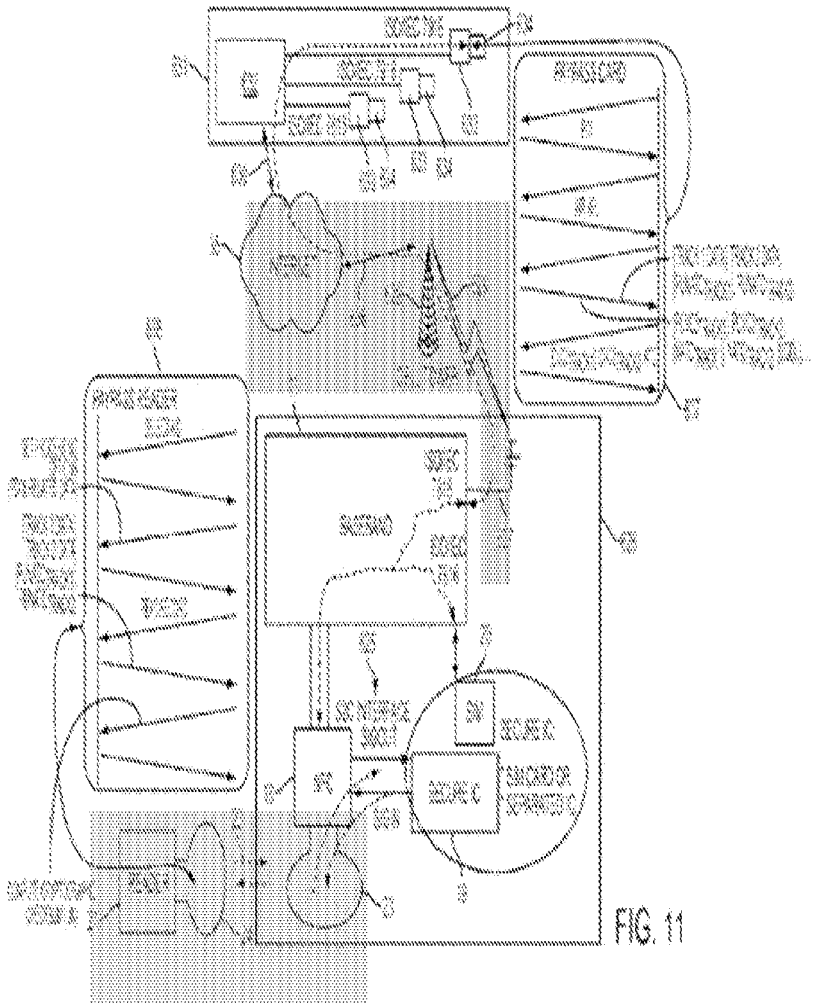
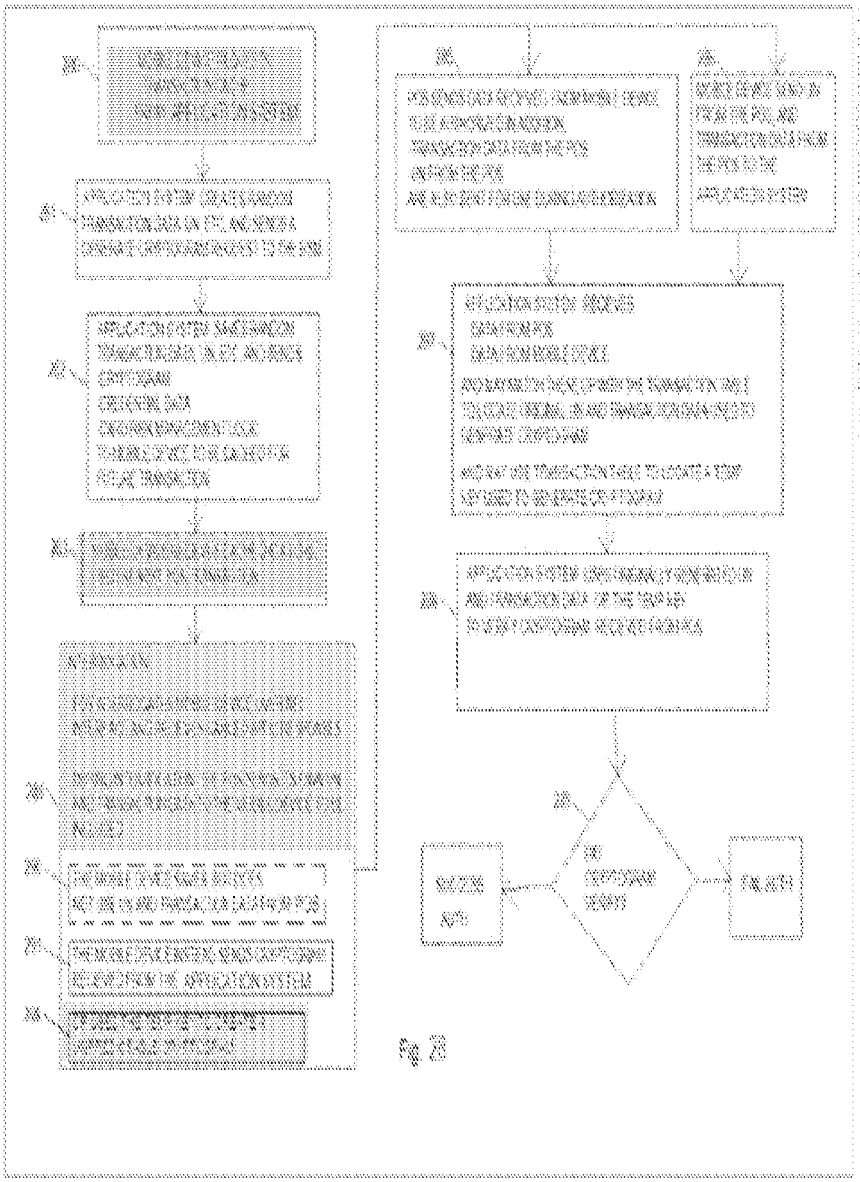


FIG. 11

- Mobile device communicates with remote system via a wireless network. (*See e.g.,* FIG. 11).

- Mobile device communicates with POS via communication channel that is separate from the wireless network.

Application Does Not Access A Permanent Cryptographic Key Associated With the Account During Interrogations



[0213] Element **227**, although it may be less secure, in another embodiment could contain the permanent cryptographic key that is used to create an expected cryptogram.

Application at ¶ [0213]

[0229] As a further alternative to the method of **280**, **281**, **282**, and **283**, a further embodiment may comprise the application system and mobile device sharing a temporary cryptographic key that the mobile devices will use to create an unpredictable cryptogram.

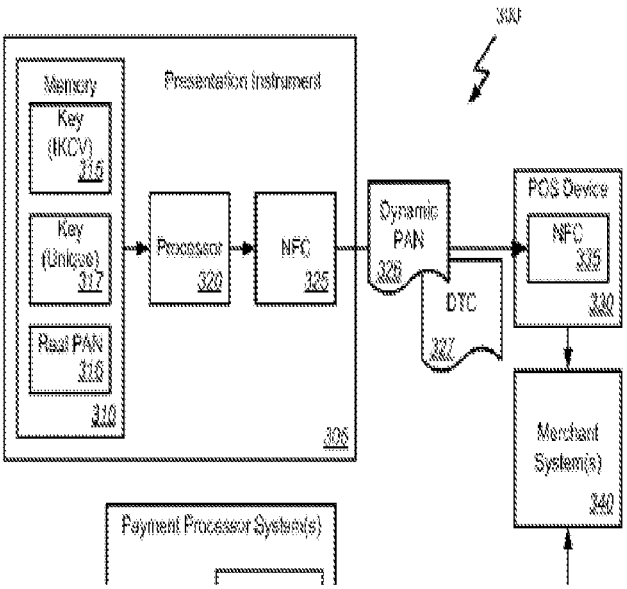
Application at ¶ [0229]

[0236] In a further embodiment of the interrogation **284**, the mobile device creates an unpredictable cryptogram calculated from a temporary cryptographic key and, at least in part, the unpredictable data from the point-of-sale **399**. In this embodiment, elements **290** and **291** are not used.

Application at ¶ [0236]

Royyuru

- Presentation instrument of Royyurru stores an Institution Key Card Variant (IKCV) and unique, card-level key (CK).
- The IKCV and CK are stored on presentation instrument 305 at the time of issuance of presentation instrument 305.



Royyuru Fig. 3 (Portion)

other communication module. The memory **310** includes a variant of the institution key of the issuer of the instrument. That is, the institution key card variant (IKCV) **315** can be generated for the presentation instrument **305** by the payment processor system **350**, financial institution **370** or **375** or other issuer of the instrument at the time of issuance and based on but distinct from an institution key for that issuer. Details of

Royyuru at ¶ [0046]

described below with reference to FIG. **7**. The memory **310** of the presentation instrument **305** can also have stored therein a unique card-level key **317** and the real PAN **316** for the account associated with the presentation instrument **305**. As with the IKCV **315**, the unique card-level key **317** and real PAN **316** can be stored in the memory **310** of the presentation instrument **305** at the time the presentation instrument **305** is issued by the payment processor system **350**, financial institution **370** or **375** or other issuer. Royyuru at ¶ [0046]

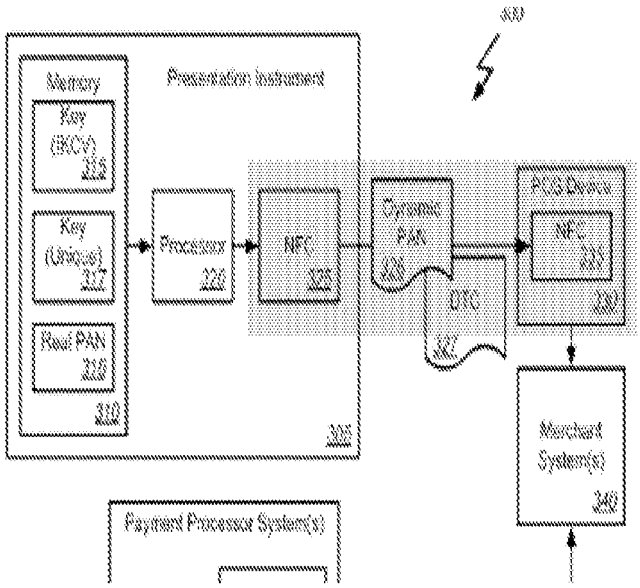
A random CK can be system-generated by payment processor when an institution requests that a card be added to the service.

Royyuru at page 9, Table

Storing the IKCV or the CK on presentation instrument 305 at issuance is not "receiving over a wireless network at a mobile device a first non-permanent cryptographic key associated with an account having a corresponding digital credential."

Royyuru

- The presentation instrument 305 accesses the IKCV and CK during interrogations.



Royyuru, Fig. 3 (Portion)

[0047] When the cardholder wishes to execute a transaction, such as a financial transaction for the purchase of goods and/or services, he presents the presentation instrument **305** to a clerk at a merchant location, and/or passes or taps the presentation instrument **305** on or near the point-of-sale device **330**. The point-of-sale device **330** may have been provided by a payment processor, who acts as an intermediary between merchants and the issuer financial institutions, coordinates transaction routing, and performs a variety of backend processes. Passing or tapping the presentation instrument near the POS device **330** can trigger the processor **320** of the presentation instrument **305** to read the IKCV **315**, the unique card-level key **317** and real PAN **316** from memory **310**. Based on this information, the processor can encrypt the real PAN **316** using the IKCV **315** and one or more inches from the payment device or the POS reader such as unpredictable numbers or counters, e.g., a time of day etc., to generate a dynamic PAN **326**. The dynamic PAN **326** can be considered a dynamic, i.e., good for one use, cryptogram that represents but hides the real PAN **316**. Details of an exemplary process for generating a dynamic PAN **326** are described below with reference to FIG. **5**. The processor **320** can also generate a dynamic transaction cryptogram (DTC) **327** based on the unique card-level key **317** and perhaps other information such as a Personal Identification Number (PIN) provided by the consumer. Details of an exemplary process for generating a DTC **327** are described below with reference to FIG. **6**. The dynamic PAN can be provided to the merchant system **340**, e.g., via the NFC module **325** of the presentation instrument and corresponding NFC module **335** of the POS device **330**. The dynamic PAN **326** and DTC **327** can then be submitted to the payment processor system **350** and/or financial institution **370** and **375** via the payment network **345** for approval and/or processing of the transaction.

Royyuru at ¶ [0047]

Royyuru fails to teach "an application executable in the operating system, the application interrogable for digital credential data corresponding to the account, wherein the application does not access a permanent cryptographic key associated with the account during interrogations."

Manduley

- Manduley seeks to add "remote inspection" capability to cards.

Smart cards are well known and in generally comprise a plastic body having approximately the size, shape and appearance of a typical credit card. Embedded within the body are a microprocessing system including a memory and processor, a power source and an input/output mechanism. When connected to an appropriate card reader a smart card can be used for secure information exchange transactions. In particular, it has frequently been suggested that a smart card can be used as an "electronic purse". In such "electronic purse" applications a smart card would be "filled" or "charged" with electronic tokens representative of a monetary value by an issuing authority such as a bank. Such tokens could then be transferred from the smart card to a vendor having an appropriate card reader as payment for goods or services. A vendor would then download electronic tokens received to an issuing authority, which would then credit the vendor's account.

Manduley, 1:12-28

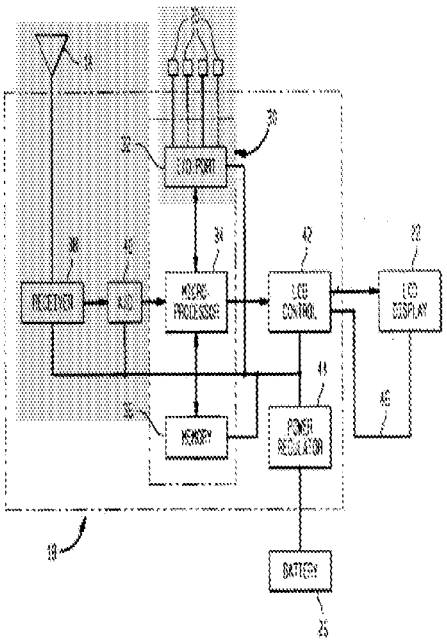
The above object is achieved and the disadvantages of the prior art are overcome in accordance with the subject invention by means of a portable apparatus, which can be a modified smartcard, which includes an antenna and a receiver responsive to the antenna for receiving transmitted messages. A decoder receives the transmitted messages from the receiver and decodes them both to determine the information content of a message and to determine that the message is addressed to a particular apparatus. The appara-

Manduley, 1:59-67

Mastercard, Ex1002, p. 778

Manduley

- Card 10 includes contacts to conduct "information exchange transactions" with a smart card reader, such as for payment of goods and services.
- Card 10 includes an antenna and receiver to receive "messages" for "remote inspection" of the card.



Manduley, Fig. 2

When connected to an appropriate card reader a smart card can be used for secure information exchange transactions. In particular, it has frequently been suggested that a smart card can be used as an "electronic purse". In such "electronic

* * *

Contacts **20** are connected to macro processor **34** through I/O port **32** to conduct information exchange transactions with external devices. Preferably, where card **10** is used as a "electronic purse", these transactions are the input and output of encrypted electronic tokens representing value to and from memory **36**. (Information transaction between smart cards and external devices are well known, and indeed are the reason for which such cards exist, and details of particular types of transactions form no part per se of the subject invention.)

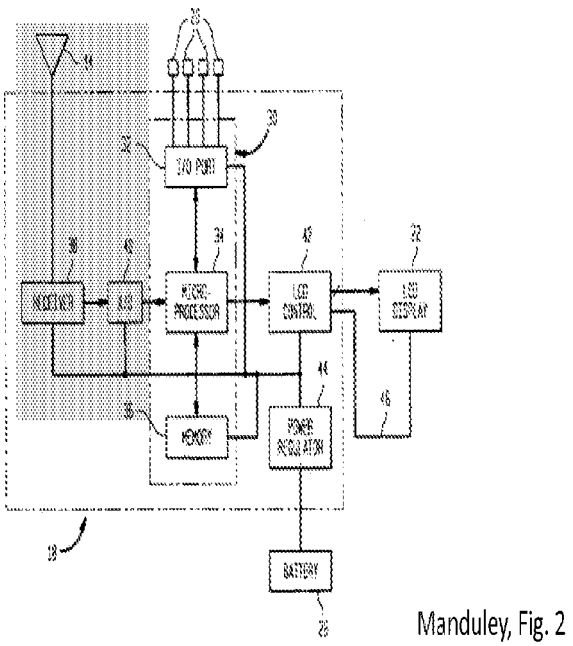
Manduley, 1:17-21, 3:27-35

Circuitry **18** also includes receiver **38** and A/D converter **40**. Antenna **14** is connected to receiver **38** which detects and amplifies RF signals picked up by antenna **14**. The output of receiver **38** is input to A/D converter **40** which generates a stream of digital data for input to microprocessor **34**. Microprocessor **34** decodes the input from A/D converter **40** both to determine if a message is addressed to card **10**, and to determine the content of messages which are addressed to card **10**. In other embodiments of the subject invention this decoding may be carried out by separate decoder circuitry.

Manduley, 3:36-47

Manduley: Remote Inspection

- Card 10 receives a Response Request message via antenna 14/reciever 38 from the issuing authority.
- Card 10 sends a response to the originator.
- If the response is valid, a Response Confirmation message is sent to card 10.



Manduley, Fig. 2

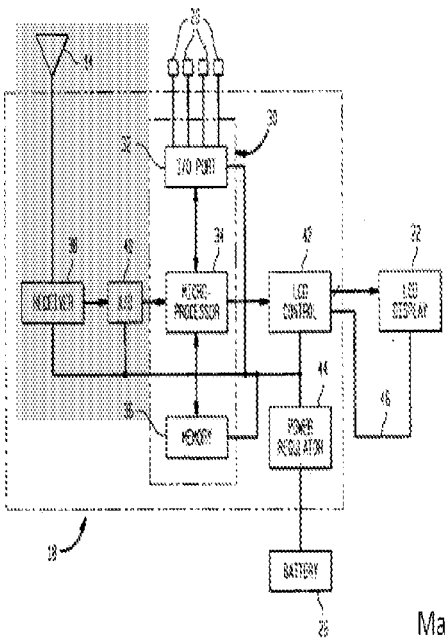
Circuitry **18** also includes receiver **38** and A/D converter **40**. Antenna **14** is connected to receiver **38** which detects and amplifies RF signals picked up by antenna **14**. The output of receiver **38** is input to A/D converter **40** which generates a stream of digital data for input to microprocessor **34**. Microprocessor **34** decodes the input from A/D converter **40** both to determine if a message is addressed to card **10**, and to determine the content of messages which are addressed to card **10**. In other embodiments of the subject invention this decoding may be carried out by separate decoder circuitry.

When a first, response request message is decoded microprocessor **34** will control LCD display **22**, through LCD control **42** to display a secure output message to prompt the possessor of card **10** to send a response reflecting the secure output message to an originator of the response request message. Thereafter, microprocessor **34** will deactivate card

Manduley, 3:37-52

Manduley: Remote Inspection

- Card 10 receives a Response Request message via antenna 14/reciever 38 from the issuing authority.
- Card 10 sends a response to the originator.
- If the response is valid, a Response Confirmation message is sent to card 10.



Manduley, Fig. 2

At **50** the issuing authority transmits a Response Request addressed to card **10**, and at **52** tests to determine if a response has been received. The response may be returned in any convenient manner, but preferably will be transmitted over the telephone network by means of tone signals in a conventional manner by a person in possession of card **10**.

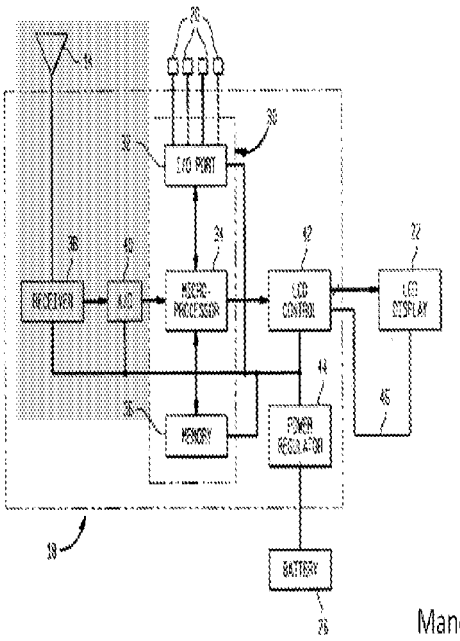
If a response is received, then at **54** the issuing authority decrypts the response, and at **56** determines if the response is valid. The validity of the response is determined by comparing the content of the decrypted response to known information, such as a serial number stored in card **10**. In a preferred embodiment of the subject invention the response will also include a password as evidence that the person returning the response is the person authorized to possess card **10**. In another preferred embodiment of the subject invention the response may also include variable information reflecting the history of transactions made using card **10**. For example, the response can include the amount of current value stored in card **10**. By including such information the issuing authority's ability to control fraudulent use of card **10** will be greatly increased.

If the response is valid, then at **60** a Response Confirmation message is sent to card **10**, completing the inspection. Preferably, the Response Confirmation message will update an encryption key used to encrypt the response so that each encrypted response received will differ from previous responses, thus assuring that the response is provided by a person actually in possession of the card. In one embodiment of the subject invention an updated encryption key may be included in the response confirmation message. To further increase the security of the system the updated key may itself be encrypted with a predetermined key stored in card **10**. In another embodiment of the subject invention, card **10**,

Manduley, 4:1-28

Manduley: Remote Inspection

- Response Confirmation message may update the encryption key used to encrypt the response to the Response Request message received via antenna 14/reciever 38 from the issuing authority.



Manduley, Fig. 2

At **50** the issuing authority transmits a Response Request addressed to card **10**, and at **52** tests to determine if a response has been received. The response may be returned in any convenient manner, but preferably will be transmitted over the telephone network by means of tone signals in a conventional manner by a person in possession of card **10**.

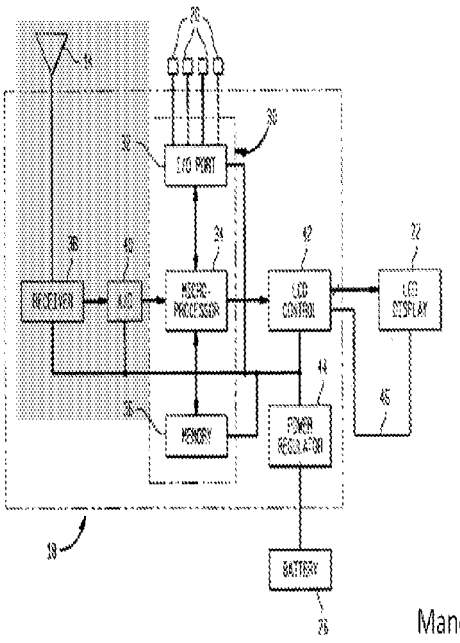
If a response is received, then at **54** the issuing authority decrypts the response, and at **56** determines if the response is valid. The validity of the response is determined by comparing the content of the decrypted response to known information, such as a serial number stored in card **10**. In a preferred embodiment of the subject invention the response will also include a password as evidence that the person returning the response is the person authorized to possess card **10**. In another preferred embodiment of the subject invention the response may also include variable information reflecting the history of transactions made using card **10**. For example, the response can include the amount of current value stored in card **10**. By including such information the issuing authority's ability to control fraudulent use of card **10** will be greatly increased.

If the response is valid, then at **60** a Response Confirmation message is sent to card **10**, completing the inspection. Preferably, the Response Confirmation message will update an encryption key used to encrypt the response so that each encrypted response received will differ from previous responses, thus assuring that the response is provided by a person actually in possession of the card. In one embodiment of the subject invention an updated encryption key may be included in the response confirmation message. To further increase the security of the system the updated key may itself be encrypted with a predetermined key stored in card **10**. In another embodiment of the subject invention, card **10**,

Manduley, 4:1-28

Manduley: Remote Inspection

- Manduley recognizes that there are other keys than those used to encrypt remote inspection communications stored on the card, but does not update those keys.



Manduley, Fig. 2

At **50** the issuing authority transmits a Response Request addressed to card **10**, and at **52** tests to determine if a response has been received. The response may be returned in any convenient manner, but preferably will be transmitted over the telephone network by means of tone signals in a conventional manner by a person in possession of card **10**.

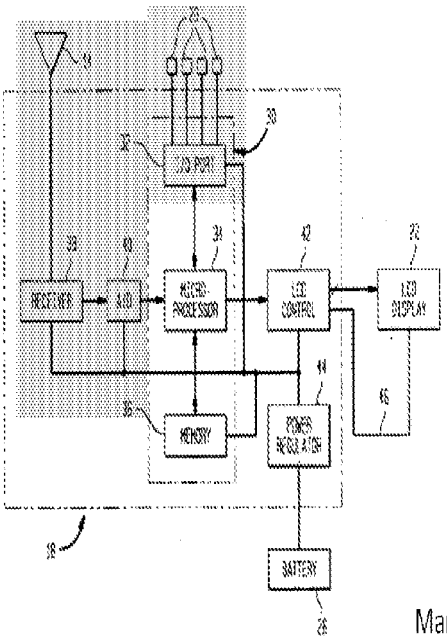
If a response is received, then at **54** the issuing authority decrypts the response, and at **56** determines if the response is valid. The validity of the response is determined by comparing the content of the decrypted response to known information, such as a serial number stored in card **10**. In a preferred embodiment of the subject invention the response will also include a password as evidence that the person returning the response is the person authorized to possess card **10**. In another preferred embodiment of the subject invention the response may also include variable information reflecting the history of transactions made using card **10**. For example, the response can include the amount of current value stored in card **10**. By including such information the issuing authority's ability to control fraudulent use of card **10** will be greatly increased.

If the response is valid, then at **60** a Response Confirmation message is sent to card **10**, completing the inspection. Preferably the Response Confirmation message will update an encryption key used to encrypt the response so that each encrypted response received will differ from previous responses, thus assuring that the response is provided by a person actually in possession of the card. In one embodiment of the subject invention an updated encryption key may be included in the response confirmation message. To further increase the security of the system the updated key may itself be encrypted with a predetermined key stored in card **10**. In another embodiment of the subject invention, card **10**,

Manduley, 4:1-28

Manduley: Remote Inspection

- Manduley does not change the underlying payment transactions with the card reader.
- Reason/Benefit of updating encryption key used to encrypt responses to remote inspection messages not present for information transactions between card and card reader.



Manduley, Fig. 2

Contacts **20** are connected to micro processor **34** through I/O port **32** to conduct information exchange transactions with external devices. Preferably, where card **10** is used as a "electronic purse", these transactions are the input and output of encrypted exctronic tokens representing value to and from memory **36**. (Information transaction between smart cards and external devices are well known, and indeed are the reason for which such cards exist, and details of particular types of transactions form no part per se of the subject invention.)

-Manduley, 3:26-36

If the response is valid, then at **60** a Response Confirmation message is sent to card **10**, completing the inspection. Preferably, the Response Confirmation message will update an encryption key used to encrypt the response so that each encrypted response received will differ from previous responses, thus assuring that the response is provided by a person actually in possession of the card. In one embodiment

Manduley, 4:21-27

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
PROPOSED AMENDMENT (NOT FOR ENTRY)	Atty. Docket No. **STAPP1100-5**

First Named Inventor **C. Douglas Yeager**	
Application Number **13/599,647**	Date Filed **August 30, 2012**
Title **Systems and Methods for Secure Application-Based Participation in an Interrogation by Mobile Device (as amended)**	
Group Art Unit **3695**	Examiner **Puttaiah, Asha**
Confirmation Number: **1919**	

Examiner Puttaiah:

Applicant wishes to discuss the invention as claimed and differences between the invention as claimed and the cited art. To facilitate this discussion, Applicant proposes to amend a representative independent claim as follows. Support for the proposed amendments presented herein can be found in the Specification. Should the proposed changes to the representative independent claim be agreeable, the same or similar changes will be made to other independent claims for the sole purpose of placing the instant application in condition for allowance.

Respectfully submitted,

Sprinkle IP Law Group
Attorneys for Applicants

/John L. Adair/

John L. Adair
Reg. No. 48,828

Date: August 23, 2017

1301 W. 25th Street, Suite 408
Austin, TX 78705
Tel. (512) 637-9220
Fax. (512) 371-9088

PROPOSED AGENDA

I. Overview

a. Permanent Cryptographic Key

i. During patent examination, the pending claims must be "given their broadest reasonable interpretation consistent with the specification."

ii. The broadest reasonable interpretation does not mean the broadest possible interpretation. Rather, the meaning given to a claim term must be consistent with the ordinary and customary meaning of the term (unless the term has been given a special definition in the specification), and must be consistent with the use of the claim term in the specification and drawings.

iii. The Application states, "[a]s used herein the term 'permanent cryptographic key' refers to a cryptographic key that is unchanging (or static) throughout the life of a card, SE, mobile device, or digital credential." United States Patent Publication 2013/0054474 (the "Application") at ¶ [0165].

iv. Discuss examples.

b. The claims recite that a mobile device "comprises an operating system and an application executable in the operating system, the application interrogable for digital credential data corresponding to the account, wherein the application does not access a permanent cryptographic key associated with the account during interrogations." The mobile device receives a non-permanent cryptographic key over a wireless network. During an interrogation, the mobile device uses the non-permanent cryptographic key in generating a response cryptogram that is included in a response to at least one POS command communication sent to the POS over a communications channel with POS (e.g., that is separate from the wireless network over which the non-permanent key was received).

II. Royyuru: the Office Action asserts that Royyuru teaches "receiving over a wireless network at a mobile device a first non-permanent cryptographic key associated with an account having a corresponding digital credential, wherein the mobile device comprises an operating system and an application executable in the operating system, the application interrogable for digital credential data corresponding to the account, wherein the application does not access a permanent cryptographic key associated with the account during interrogations" and "locally storing a first non-permanent cryptographic key associated with the account." Office Action at page 8, citing Royyuru, Fig. 3, ¶¶ [0021], [0033], Page 9 Table, Card-Key, CK.

a. Applicant respectfully requests that the Examiner clarify where Fig. 3, ¶¶ [0021], [0033] of Royurru show receiving the CK over a wireless network.

b. Applicant respectfully requests that the Examiner point out where Fig. 3, ¶¶ [0021], [0033] show "the application interrogable for digital credential data corresponding to the account, wherein the application does not access a permanent cryptographic key associated with the account during interrogations."

i. Royyuru uses at least an IKCV and CK during a transaction:

1. IKCV: "The memory 310 includes a variant of the institution key of the issuer of the instrument. That is, the institution key card variant (IKCV) 315 can be generated for the presentation instrument 305 by the payment processor system 350, financial institution 370 or 375 or other issuer of the instrument **at the time of issuance** and based on but distinct from an institution key for that issuer." Royyuru at ¶ [0046].

2. CK: Royyuru teaches that the CK is generated when "an institution requests that a card be added to the service." Royyuru, page 9, Table, Card-Key, CK. That is, "[a]s with the IKCV 315, the unique card-level key 317 and real PAN 316 can be stored in the memory **310** of the presentation instrument **305 at the time the**

presentation instrument 305 is issued by the payment processor system **350**, financial institution **370** or **375** or other issuer. Royyuru at ¶ [0046].

ii. Royyuru **does** access a permanent cryptographic key associated with the account during interrogations.

c. Royyuru does not teach "locally storing a first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account" where the non-permanent cryptographic key is used to generate the response cryptogram.

III. Manduley: the Office Action argues that Manduley teaches "receiving a second non-permanent cryptographic key at the mobile device . . . replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key."

a. Manduley teaches a card 10 that "[w]hen connected to an appropriate card reader . . . can be used for secure information exchange transactions. In particular, it has frequently been suggested that a smart card can be used as an 'electronic purse'." Manduely at 1:17-18. The card 10 includes "contacts 20" "connected to microprocessor 34 through I/O port 32 to conduct information exchange transactions to external devices." Manduley at 3:26-37.

b. Manduley further teaches that, in addition to the contacts 20 over which "information transactions" occur, the card includes an antenna 14, receiver and microprocessor to receive and decode "messages" received via RF signals. Manduley at 3:36-46. Manduley further teaches that "If the response [to a Response Request message] is received, the issuing authority decrypts the response and, at 56 determines if the response is valid . . . If the response is valid, then at 60 a Response Confirmation message is sent to card 10 . . . Preferably, the Response Confirmation message will update an encryption key used to encrypt the response . . ." Manduley at 4:6-4:21.

i. The encryption key "used to encrypt the response" is used to encrypt the responses to messages received from the issuing authority (e.g., via antenna 14).

ii. Manduley, however, recognizes that there other encryption keys stored on the card, but does not update those keys with Response Confirmation Message. Manduley at 3:31-33 ("To further increase the security of the system the updated key may itself be encrypted with **a predetermined key stored on the card**") (emphasis added).

iii. Manduley recognizes that encryption is used as part of the payment transaction process: "where card 10 is used as an 'electronic purse', these transactions are the input and output of encrypted electronic tokens representing value and from memory 36." Manduley at 3:28-31. Manduley, however, explicitly does not change the underlying payment transactions with the card reader, stating "information transaction between smart cards and external devices are well known, and indeed are the reason such cards exist, and **details of particular type of transactions form no part per se of the subject invention.**" Id. at 3:32-35 (emphasis added).

iv. Manduley does not teach "receiving over a wireless network at a mobile device a first non-permanent cryptographic key associated with an account having a corresponding digital credential" that is used to generate a response cryptogram during an interrogation by a POS, "requesting, by the mobile device, a second non-permanent cryptographic key associated with the account," "receiving [a] the second non-permanent cryptographic key at the mobile device, wherein the second non-permanent cryptographic key is associated with the account," and "replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key as the local cryptographic key associated with the account prior to the application participating in a subsequent interrogation."

PROPOSED ALTERNATIVE AMENDMENTS (NOT FOR ENTRY):

30. (Currently Amended) A method for secure application-based participation in a payment card transaction authorization process by a mobile device, the method comprising:

receiving over a wireless network at a mobile device a first non-permanent cryptographic key associated with an account having a corresponding digital credential, wherein the mobile device comprises an operating system and an application executable in the operating system, the application interrogable for digital credential data corresponding to the account, wherein the application does not access a permanent cryptographic key associated with the account during interrogations;

locally storing a first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;

participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device comprising:

receiving at least one POS command communication sent by the POS terminal over a communications channel separate from the wireless network, wherein the at least one POS command communication comprises a request for digital credential data to authorize a transaction against the account;

generating a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram; and

responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to an electronic reader ~~through the communication channel~~ over the communications channel that is separate from the wireless network, the at least one device response communication comprising at least a portion of the digital credential data, wherein the at least a portion of the digital credential data comprises the response cryptogram and an account identifier for the account;

requesting, by the mobile device, a second non-permanent cryptographic key associated with the account;

receiving [a] the second non-permanent cryptographic key at the mobile device, wherein the second non-permanent cryptographic key is associated with the account; and

replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key as the local cryptographic key associated with the account prior to the application participating in a subsequent interrogation.

31. (New) The method of Claim 1, wherein the communications channel is a baseband communications channel.

32. (New) The method of Claim 30, further comprising, prior to receiving the first non-permanent cryptographic key over the wireless network:

authenticating the mobile device with a remote system;

receiving a shared key from the remote server to encrypt communications over the wireless channel;

requesting the first non-permanent encryption key from the remote system.

30. (Previously Presented) A method for secure application-based participation in a payment card transaction authorization process by a mobile device, the method comprising:

the mobile device requesting, over a wireless network, a transaction cache for a secure element associated with an account from a remote application system that comprises a plurality of secure element representations ~~receiving over a wireless network at a mobile device a first non-permanent cryptographic key associated with an account having a corresponding digital credential,~~ wherein the mobile device comprises an operating system and an application executable in the operating system, the application interrogable for digital credential data corresponding to the account, wherein the application does not access a permanent cryptographic key associated with the account during interrogations;

receiving the transaction cache over the wireless network, the transaction cache containing data to create application program data unit (APDU) responses to APDU commands, said data including a first non-permanent cryptographic key associated with the account;

locally storing [[a]] the first non-permanent cryptographic key at the mobile device as a local non-permanent cryptographic key associated with the account;

participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device comprising:

receiving at least one POS command communication sent by the POS terminal over a communications channel, wherein the at least one POS command communication comprises a request for digital credential data to authorize a transaction

against the account, the at least on POS command communication comprising an APDU command cryptogram request;

the mobile device generating an unpredictable response cryptogram used to authorize the transaction based on a set of inputs and the local non-permanent cryptographic key associated with the account, wherein the response cryptogram does not include the local non-permanent cryptographic key associated with the account used to generate the response cryptogram; and

responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication comprising at least one response APDU from the mobile device to an electronic reader through the communication channel, the at least one device response communication comprising at least a portion of the digital credential data, wherein the at least a portion of the digital credential data comprises the response cryptogram and an account identifier for the account;

prior to the application participating in a subsequent interrogation to authorize another financial transaction against the account, receiving, over the wireless network, a second non-permanent cryptographic key at the mobile device from the remote application system, wherein the second non-permanent cryptographic key is associated with the account; and

replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key as the local non-permanent cryptographic key associated with the account prior to the application participating in [a] subsequent interrogation.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
REPLY TO OFFICE ACTION DATED 06/05/2017	Atty. Docket No. **STAPP1100-5**

First Named Inventor **C. Douglas Yeager**	
Application Number **13/599,647**	Date Filed **August 30, 2012**
Title **SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE** (As Amended)	
Group Art Unit **3695**	Examiner **Puttaiah, Asha**
Confirmation Number: **1919**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission Under 37 C.F.R. § 1.8

I hereby certify that this correspondence is being deposited electronically with the U.S. Patent and Trademark Office using the United States Patent and Trademark Office's EFS-Web system on October 5, 2017.

Margarita Marquez

Dear Sir:

This paper is submitted in response to the Official Action mailed on June 5, 2017, the Examiner Interview held on September 6, 2017, and the Interview Summary mailed on September 25, 2017. Please reconsider the above-identified application in view of the following amendments and remarks.

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 11 of this paper.

AMENDMENTS TO THE CLAIMS:

Please amend the claims as set forth in the following listing. This listing of claims will replace all prior versions, and listings, of claims in the present application:

1-29. Cancelled.

30. (Currently Amended) A method for secure application-based participation in a payment card transaction authorization process by a mobile device, the method comprising:

~~receiving over a wireless network~~ at a mobile device, executing an application in an operating system of the mobile device, ~~a first non-permanent cryptographic key associated with an account having a corresponding digital credential, wherein the mobile device comprises an operating system and an application executable in the operating system,~~ the application interrogable by an electronic reader, over a first communications channel, for digital credential data corresponding to [the] an account having a corresponding digital credential and configured to request, from a remote computer system hosting the corresponding digital credential, over a wireless network that is separate from the first communications channel, data associated with the account and generate cryptograms requested during interrogations over the first communications channel using the data associated with the account received from the remote computer system, wherein the application does not access a permanent cryptographic key issued for the digital credential ~~associated with the account~~ during the interrogations;

requesting by the application, from the remote computer system, over the wireless network, a first set of data associated with the account;

receiving by the application, from the remote computer system, over the wireless network, the first set of data associated with the account, the first set of data associated with the account usable by the application to formulate a first application protocol data unit response, the first set of data comprising a first non-permanent cryptographic key associated with the account;

locally storing [a] the first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;

participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device comprising:

receiving at least one POS command communication sent by the POS terminal over [a] the first communications channel, wherein the at least one POS command

communication comprises a request for digital credential data to authorize a transaction against the account, the request for digital credential data including a cryptogram request;

generating a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram; and

responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to an electronic reader through the communication channel, the at least one device response communication comprising at least one response application data protocol unit containing ~~a portion of the digital credential data, wherein the at least a portion of the digital credential data~~ comprises the response cryptogram and an account identifier for the account;

subsequent to the interrogation, requesting by the application, from the remote computer system, over the wireless network, a second set of data associated with the account;

receiving by the application, from the remote computer system, over the wireless network, the second set of data associated with the account, the second set of data comprising a second non-permanent cryptographic key associated with the account ~~at the mobile device, wherein the second non-permanent cryptographic key is associated with the account~~; and

replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key as the local cryptographic key associated with the account prior to the application participating in a subsequent interrogation.

31. (Currently Amended) The method of Claim 30, wherein the mobile device is an NFC emulating device, wherein the first communications channel is an NFC communications channel and the first set of data associated with the account and the second set of data associated with the account are received via a data connection over the internet.

32. (Previously Presented) The method of Claim 30, wherein the response cryptogram is a hash.

33. (Previously Presented) The method of Claim 30, wherein the interrogation conforms to a card specification, the set of inputs is specified by the card specification and the at least one device response is formulated according to the card specification.

34. (Previously Presented) The method of Claim 33, wherein the request for digital credential data comprises a request for a first cryptogram according to the card specification and the at least one device response communication comprises a second cryptogram, wherein the second cryptogram is the response cryptogram.

35. (Previously Presented) The method of Claim 30, wherein generating the response cryptogram comprises encrypting the set of inputs using the local cryptographic key according to a digital encryption standard (DES) calculation to generate an output, wherein the response cryptogram includes a portion, but not all, of the output.

36. (Previously Presented) The method of Claim 30, wherein the mobile device does not have connectivity to the wireless network during the interrogation.

37. (Currently Amended) The method of Claim 30, further comprising, at [a] the remote computer system:

prior to the interrogation, generating ~~at a remote system~~ the first non-permanent cryptographic key at the remote computer system, associating the first non-permanent cryptographic key with the account, and sending the first non-permanent cryptographic key and the account identifier to the mobile device over the wireless network; and

after the interrogation generating ~~at the remote system,~~ the second non-permanent cryptographic key at the remote computer system, associating the second non-permanent cryptographic key with the account and sending the second non-permanent cryptographic key and the account identifier to the mobile device over the wireless network.

38. (Currently Amended) The method of Claim 37, wherein the digital credential comprises a secure element representation maintained at the remote computer system.

39. (Currently Amended) The method of Claim 30, further comprising, at [a] the remote computer system, performing an authorization process comprising:

receiving an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the response cryptogram and the account identifier;

determining a current non-permanent cryptographic key associated with the account using the account identifier;

calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account;

verifying a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram; and

sending an authorization response to the POS terminal, wherein the data contained in the authorization response is determined, at least in part, by the verifying the correctness of the response cryptogram.

40. (Previously Presented) The method of Claim 39, wherein:

the set of inputs comprises unpredictable data;

the authorization data comprises the unpredictable data; and

the calculated cryptogram is calculated using the unpredictable data.

41. (Previously Presented) The method of Claim 40, wherein the POS command communications comprise the unpredictable data.

42. (Currently Amended) The method of Claim 41, wherein the authorization data further comprises values from the transaction ~~and wherein the POS terminal communicates the values from the transaction, the response cryptogram and the account identifier to the remote system in track 2 format~~.

43. (Cancelled)

44. (Currently Amended) A system for secure application-based participation by a mobile device in point-of-sale interrogations, the system comprising:

a mobile device comprising:

a controller configured to route communications received over a communication channel from an electronic reader;

a wireless interface to connect to a wireless network that is separate from the communications channel;

a processor;

a computer readable storage medium accessible by the processor storing an application executable in an operating system of the mobile device, the application, when executed, interrogable over the communications channel for digital credential data to authorize transactions against an account having a corresponding digital credential hosted at a remote computer system, ~~the application executable in an operating system of the mobile device to participate in interrogations~~ wherein the application does not have access to a permanent cryptographic key issued for the digital credential and the application is executable to:

request from the remote computer system, over the wireless network, a first set of data associated with the account;

receive by the application, from the remote computer system, over the wireless network, the first set of data associated with the account, the first set of data associated with the account usable by the application to formulate a first application protocol data unit response, the first set of data comprising a first non-permanent cryptographic key associated with the account;

store the first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;

during an interrogation:

receive at least one point-of-sale (POS) command communication sent by a POS terminal to the mobile device over the communications channel, wherein the at least one POS command communication comprises a request for digital credential data, the request for digital credential data including a cryptogram request;

access [a] the locally stored cryptographic key associated with the account, ~~wherein the mobile device does not have access to a permanent cryptographic key associated with the account and the locally stored cryptographic key associated with the account is a non-permanent cryptographic key that does not last a life of a digital credential for an account~~;

generate a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram

does not include the local cryptographic key associated with the account used to generate the response cryptogram; and

respond to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response to the electronic reader through the communication channel, the at least one device response communication comprising at least one response application data protocol unit containing ~~a portion of the digital credential data, wherein the at least a portion of the digital credential data comprises~~ the response cryptogram and an account identifier for the account;

subsequent to the interrogation, request from the remote computer system, over the wireless network, a second set of data associated with the account;

receive by the application, from the remote computer system, over the wireless network, the second set of data associated with the account, the second set of data associated with the account comprising a second non-permanent cryptographic key ~~keys~~ associated with the account ~~transmitted to the mobile device over the wireless network by a remote source~~; and

store the received second non-permanent cryptographic key ~~keys~~ as the locally stored cryptographic key associated with the account to change the locally stored cryptographic key associated with the account between at least two interrogations.

45. (Currently Amended) The system of Claim 44, wherein the mobile device is an NFC emulating device, the first communication channel is an NFC channel, and the application is further executable to request and receive the first set of data associated with the account and the second set of data associated with the account via a data connection over the internet to the remote computer system.

46. (Previously Presented) The system of Claim 44, wherein the response cryptogram is a hash.

47. (Previously Presented) The system of Claim 44, wherein the interrogations conform to a card specification, the set of inputs is specified by the card specification and the at least one device response is formulated according to the card specification.

48. (Previously Presented) The system of Claim 47, wherein the request for digital credential data requests digital credential data comprising a first cryptogram and the at least one device response communication comprises a second cryptogram, wherein the second cryptogram is the response cryptogram.

49. (Previously Presented) The system of Claim 44, wherein generating the response cryptogram comprises encrypting the set of inputs using the local cryptographic key according to a digital encryption standard (DES) calculation to generate an output, wherein the response cryptogram includes a portion, but not all, of the output.

50. (Previously Presented) The system of Claim 44, wherein the mobile device does not have connectivity to the wireless network during the interrogation.

51. (Previously Presented) The system of Claim 44, wherein the mobile device is programmed to request a new non-permanent cryptographic key after the interrogation.

52. (Currently Amended) The system of Claim 44, further comprising [a] the remote computer system, the remote computer system configured to generate [the] non-permanent cryptographic keys associated with the account and send each of the non-permanent cryptographic keys and the account identifier to the mobile device over the wireless network.

53. (Previously Presented) The system of Claim 52, wherein the remote computer system is configured to maintain a secure element representation for the account, wherein the digital credential comprises the secure element representation.

54. (Previously Presented) The system of Claim 44, further comprising, a remote computer system programmed to:

receive an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the response cryptogram and the account identifier;

determine a current non-permanent cryptographic key associated with the account using the account identifier;

calculate a calculated cryptogram using the current non-permanent cryptographic key associated with the account;

verify a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram; and

send an authorization response to the POS terminal, wherein the data contained in the authorization response is determined, at least in part, by the verifying the correctness of the response cryptogram.

55. (Previously Presented) The system of Claim 54, wherein:

the set of inputs comprises unpredictable data;

the authorization data comprises the unpredictable data; and

the calculated cryptogram is calculated using the unpredictable data.

56. (Previously Presented) The system of Claim 55, wherein the POS command communications comprise the unpredictable data.

57. (Currently Amended) The system of Claim 55, wherein the authorization data further comprises values from the transaction ~~and wherein the POS terminal communicates the values from the transaction, the response cryptogram and the account identifier to the remote system in track 2 format~~.

58. (Cancelled).

59. (New) The method of Claim 30, wherein the first non-permanent cryptographic key and second non-permanent cryptographic key are shared by a remote payment authorization process.

60. (New) The system of Claim 44, wherein the first non-permanent cryptographic key and second non-permanent cryptographic key are shared by a remote payment authorization process.

61. (New) The method of Claim 30, wherein the application is configured to generate the response cryptogram according to a card specification.

62. (New) The system of Claim 44, wherein the application is executable to generate the responsive cryptogram according to a card specification.

63. (New) The method of Claim 30, wherein the first and second non-permanent cryptographic key are associated with an issuer master key.

64. (New) The system of Claim 44, wherein the first and second non-permanent cryptographic key are associated with an issuer master key.

REMARKS

Applicant appreciates the time taken by the Examiner to review Applicant's present application. This application has been carefully reviewed in light of the Official Action mailed on June 5, 2017 ("Office Action"), the Examiner Interview held on September 6, 2017, and the Examiner's Interview Summary mailed on September 25, 2017. Applicant respectfully requests reconsideration and favorable action in this case.

Interview Summary

A telephonic interview was conducted on September 6, 2017 between Examiner Puttaiah, inventor Yeager and Attorney Adair. During the interview, the Proposed Agenda, Alternative Amendments to Claim 30 and the Slides attached to Examiner Puttaiah's Applicant-Initiated Interview Summary were discussed. Royyuru and Manduley were discussed. No agreement was reached, but the Examiner suggested amending the claims to further clarify that the non-permanent keys used to generate the cryptograms that are returned in the interrogation responses are received by the mobile device over a communications channel that is distinct from the payment communications channel.

Applicant appreciates the time and effort taken by Examiner Puttaiah to review Applicant's present application and discuss the pending claims and the cited prior art. Applicant has amended the claims accordingly.

Rejections under 35 U.S.C. § 112

The Examiner objects to Claims 42, 57, 43 and 58 as being indefinite for specifying an standard format which can change upon updates. Applicant disagrees with the Examiner's rejection for at least the reasons discussed in the prior response, but has amended claims 42 and 57 and cancelled claims 43 and 48 to further prosecution.

Rejections under 35 U.S.C. § 103

Claims 30, 31, 33, 34, 35, 37, 38, 39, 40, 41, 42 44, 45, 47, 48, 49, 51, 52, 53, 54, 55, 56 and 57 stand rejected as obvious over U.S. Patent Application Publication No. 2010/0185545 ("Royyuru") in view of U.S. Patent No. 5,737,423 ("Manduley").

Before addressing the claims and cited art, some background information may be helpful. In traditional "smartcard" payment technologies, a microchip referred to as a "Secure Element" (SE) is embedded into a payment card, a payment fob (medallion), a cell phone, or other mobile

device that may be used for making payments. *See*, United States Patent Publication 2013/0054474 (the "Application") at ¶ [0003]. As described in the Specification, conventional secure element payment systems require that the user have physical possession of a "card" (e.g., card or mobile device with a secure element microchip) that matches the authorization capabilities of a merchant's system where a purchase is made. *See*, Application at ¶ [0003].

Prior to card issuance, an SE is typically injected with personalization or "credential" data that is generated from a "Hardware Security Module" (HSM). The HSM securely contains the cryptographic keys and algorithms that relate to a particular banking application and more specifically may contain a set of individual digital credentials. *See,* Application at ¶ [0041]. Conventionally, the HSM injects a permanent cryptographic key into the SE that is used throughout the life of the SE. The permanent cryptographic key injected into an SE prior to issuance is derived from a card issuer's master key as is known in the art. For example, SEs in Mastercard Paypass MSD v3.3 smartcards are injected with a KDcvc3 permanent cryptographic key derived from the card issuer's master key (IMK). *See,* Application at ¶¶ [0041], [0165], [0172]-[0174]. In a typical interrogation, a POS terminal sends at least one command communication to the secure element requesting a cryptogram and the SE generates a responsive cryptogram using the permanent cryptographic key that was injected into the SE prior to issuance. *See e.g.,* Application at ¶¶ [0165], [0256]. Many mobile devices, however, do not have a secure element microchip for electronic payment or, if they do, the secure element microchip may be limited to a single or limited number of card specifications and accounts. Embodiments described in the Application provide systems and methods that allow a mobile device to participate in secure element payment authorization systems without requiring that the mobile device have a matching secure element chip installed on the mobile device.

As described in the Application, a mobile device may include an application that runs in the operating system of the mobile device that is capable of being interrogated by an electronic reader for digital credential data associated with a payment card account. *See e.g.,* Application at ¶ [0262]. However, according to some embodiments described in the specification, the matching secure element is not maintained at the mobile device. Instead, a remote system may host digital credentials (secure element representations) associated with payment card accounts. Prior to an interrogation, the mobile device can request data associated with the account from the remote system over a first communications channel (*e.g.*, a data connection over the Internet), cache the data associated with account and use the data the associated with the account to

generate application protocol data unit responses to a subsequent interrogations by an electronic reader over a second communications channel. For example, as illustrated in FIG. 28 (reproduced below), the mobile device can request a "transaction cache" from the remote system over the Internet (steps 280-283). The transaction cache can include data usable by the mobile device to generate application protocol data unit responses during an interrogation. In one example provided, the transaction cache includes a temporary cryptographic key associated with the account. *See* Application at ¶¶ [0229], [0225].

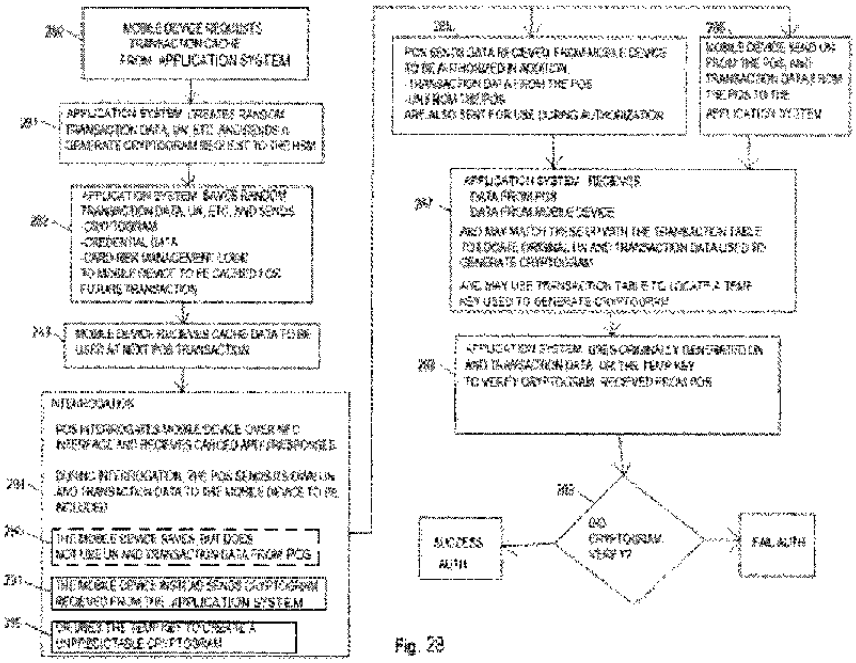


Fig. 29

During an interrogation, which occurs over a different communications channel than the channel over which the mobile device communicated with remote system to request and receive the transaction cache, a point-of-sale terminal may request data from the digital credential. This may including requesting that a cryptogram be generated according to a payment card specification (e.g., Mastercard Paypass MSD v3.3) (step 284). The mobile device can generate the requested cryptogram using the temporary cryptographic key from the transaction cache, rather than a permanent cryptographic key that was stored in a secure element at issuance, and provide the cryptogram formatted according to the card specification to the point-of-sale terminal in an APDU response (step 399). *See* Application at ¶¶ [0234], [0236].

Turning to the claims, Claim 30, as amended, recites:

> at a mobile device, executing an application in an operating system of the mobile device, the application interrogable by an electronic reader, over a first communications channel, for digital credential data corresponding to an account having a corresponding digital credential and configured to[:] request, over a wireless network that is separate from the first communications channel, from a remote computer system hosting the corresponding digital credential, data associated with the account[;] and generate cryptograms requested during interrogations over the first communications channel using the data associated with the account received from the remote computer system, wherein the application does not access a permanent cryptographic key issued for the digital credential during the interrogations

An application running in the operating system of a mobile device can request data associated with the account from a remote system that hosts a digital credential corresponding to the account, receive the data associated with the account from the remote system over a wireless network (for example, via a data connection over the Internet) and use the data associated with the account to generate cryptograms requested as part of interrogations by electronic readers which occur on a separate communications channel than the communications channel over which the application communicates with the remote system hosting the digital credential. The data associated with the account received from the remote system may be usable by the application to formulate application protocol data unit responses to the interrogations.

More particularly, the application receives, over the wireless network (*e.g.*, via an data connection over the Internet with the remote system that hosts the digital credential), "a first set of data associated with the account the first set of data associated with the account usable by the application to formulate a first application protocol data unit response, the first set of data comprising a first non-permanent cryptographic key associated with the account" and during an interrogation by a point-of-sale terminal over a separate communications channel, uses the non-permanent cryptographic key to "generat[e] a response cryptogram based on a set of inputs and the [first non-permanent] cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram" and responds to a POS command communication that includes a cryptogram request with "at least one response application data protocol unit containing the response cryptogram" generated using the first non-permanent cryptographic key.

The application does not access a permanent cryptographic key issued for the digital credential during the interrogation.

The Office Action asserts "[i]n the instant case, Royyuru discloses a method and system of handling information related to financial transactions including mobile devices/card utilizing dynamic cryptograms including a single use cryptographic key" and appears to point to the unique card key (CK) as the alleged single use key of Royyuru. *See* Office Action at 8, 11. Applicant respectfully disagrees. While Royyuru does teach generating a dynamic cryptogram, the dynamic cryptogram is generated using the unique card key (CK), which, as discussed below, is a permanent cryptographic key, not a single use key as apparently asserted in the Office Action. Thus, contrary to the claimed application, the payment instrument of Royyuru does "access a permanent cryptographic key issued for the digital credential during the interrogations."

During patent examination, the pending claims must be "given their broadest reasonable interpretation consistent with the specification." MPEP § 2111 (internal citations omitted). However, "the broadest reasonable interpretation does not mean the broadest possible interpretation. Rather, the meaning given to a claim term must be consistent with the ordinary and customary meaning of the term (unless the term has been given a special definition in the specification), and must be consistent with the use of the claim term in the specification and drawings." *Id.* With respect to the term "permanent cryptographic key" the Application states, "[a]s used herein the term 'permanent cryptographic key' refers to a cryptographic key that is unchanging (or static) throughout the life of a card, SE, mobile device, or digital credential." The CK of Royyuru is a "permanent cryptographic key," as is the IKCV of Royyuru.

The payment instrument of Royyuru accesses at least the IKCV and CK during a transaction. Royyuru at ¶ [0047] ("Passing or tapping the presentation instrument near a POS device 330 can trigger processor 320 of the presentation instrument 305 to read the IKCV 315, the unique card-level key 317 and real PAN 316 from memory"). With respect to the IKCV, Royyuru teaches that "the memory 310 includes a variant of the institution key of the issuer of the instrument. That is, the institution key card variant (IKCV) 315 can be generated for the presentation instrument 305 by the payment processor system 350, financial institution 370 or 375 or other issuer of the instrument **at the time of issuance** and based on but distinct from an institution key for that issuer." Royyuru at ¶ [0046] (emphasis added). With respect to the CK, Royyuru teaches that the CK is generated "**when** an institution requests that a card be **added to the service**." Royyuru, page 9, Table, Card-Key, CK (emphasis added). That is, "[a]s with the

IKCV 315, the unique card-level key 317 and real PAN 316 can be stored in the memory **310** of the presentation instrument **305 at the time the presentation instrument 305 is issued** by the payment processor system 350, financial institution 370 or 375 or other issuer." Royyuru at ¶ [0046] (emphasis added). One of ordinary skill in the art would thus understand that the IKCV and CK are "permanent cryptographic key(s)" stored in the presentation instrument at the time issue and are not single use keys. The payment instrument of Royyuru thus does "access a permanent cryptographic key issued for the digital credential" during a transaction.

Applicant respectfully submits that Royyuru fails to teach *inter alia*:

- an application interrogable by an electronic reader, over a first communications channel, for digital credential data corresponding to an account having a corresponding digital credential, where the application is "configured to request, from a remote computer system hosting the corresponding digital credential, over a wireless network that is separate from the first communications channel, data associated with the account and generate cryptograms requested during interrogations over the first communications channel using the data associated with the account received from the remote computer system [over the wireless network that is separate from the first channel], wherein the application does not access a permanent cryptographic key issued for the digital credential during the interrogations;"
- "requesting by the application, from the remote computer system, over the wireless network, a first set of data associated with the account" and "receiving by the application, from the remote computer system, over the wireless network, the first set of data associated with the account, the first set of data associated with the account usable by the application to formulate a first application protocol data unit response, the first set of data comprising a first non-permanent cryptographic key associated with the account;"
- "responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to an electronic reader through the communication channel, the at least one device response communication comprising at least one response application data

protocol unit containing the response cryptogram [generated using the first non-permanent cryptographic key];"

- "subsequent to the interrogation, requesting by the application, from the remote computer system, over the wireless network, a second set of data associated with the account" and "receiving by the application, from the remote computer system, over the wireless network, the second set of data associated with the account, the second set of data comprising a second non-permanent cryptographic key associated with the account;"
- "replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key as the local cryptographic key associated with the account prior to the application participating in a subsequent interrogation."

Manduley does not make up for the deficiencies of Royyuru. Manduley teaches a card 10 that "[w]hen connected to an appropriate card reader . . . can be used for secure information exchange transactions. In particular, it has frequently been suggested that a smart card can be used as an 'electronic purse'." Manduely at 1:17-18. The card 10 includes "contacts 20" "connected to microprocessor 34 through I/O port 32 to conduct information exchange transactions to external devices." Manduley at 3:26-37.

Manduley further seeks to add "remote inspection" capability to cards. *See* Manduley at 1:12-28, 1:59-67. To this end, the card of Manduley includes an antenna, receiver and microprocessor to receive and decode "remote inspection" messages. Manduley at 3:36-47. If the card receives a "Response Request" message from the issuing authority, the card sends a response to the originator and, if the response is valid, a "Response Confirmation" message is sent to the card. Manduley at 4:1-28. The Response Confirmation message may update the encryption key used to encrypt the response to the Response Request message. Manduley at 4:21-29.

Manduley simply uses a changing shared key to encrypt back and forth communications between card and originator for remote inspection. It can be noted that Manduley recognizes that there may be other keys stored on the card than those used for encrypting remote inspection but does not teach updating those keys. For example, Manduley teaches, "[t]o further increase security of the system the updated key may itself be encrypted with a predetermined key stored in card 10," yet makes no mention of updating the predetermined key. Manduley at 4:30-32.

More importantly, Manduley recognizes that encryption is used as part of the payment transaction process that occurs between the card and card reader on the payment communications channel, explaining "where card 10 is used as an 'electronic purse', these transactions are the input and output of encrypted electronic tokens representing value and from memory 36," but explicitly **does not change** the underlying payment transactions with the card reader (the transactions over the payment channel), stating "information transactions between smart cards and external devices are well known, and indeed are the reason such cards exist, and **details of particular type of transactions form no part per se of the subject invention**." Manduley at 3:32-35 (emphasis added).

Manduley, like Royyuru, fails to teach:

- an application interrogable by an electronic reader, over a first communications channel, for digital credential data corresponding to an account having a corresponding digital credential, where the application is "configured to request, from a remote computer system hosting the corresponding digital credential, over a wireless network that is separate from the first communications channel, data associated with the account and generate cryptograms requested during interrogations over the first communications channel using the data associated with the account received from the remote computer system [over the wireless network that is separate from the first channel], wherein the application does not access a permanent cryptographic key issued for the digital credential during the interrogations;"
- "requesting by the application, from the remote computer system, over the wireless network, a first set of data associated with the account" and "receiving by the application, from the remote computer system, over the wireless network, the first set of data associated with the account, the first set of data associated with the account usable by the application to formulate a first application protocol data unit response, the first set of data comprising a first non-permanent cryptographic key associated with the account;"
- "responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to an

electronic reader through the communication channel, the at least one device response communication comprising at least one response application data protocol unit containing the response cryptogram [generated using the first non-permanent cryptographic key];"

- "subsequent to the interrogation, requesting by the application, from the remote computer system, over the wireless network, a second set of data associated with the account" and "receiving by the application, from the remote computer system, over the wireless network, the second set of data associated with the account, the second set of data comprising a second non-permanent cryptographic key associated with the account;"
- "replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key as the local cryptographic key associated with the account prior to the application participating in a subsequent interrogation."

Furthermore, the Examiner's reasons for combining Royyuru and Manduley are based on the flawed conclusion that Royyuru "discloses a method and system of handling information related to financial transactions including mobile devices/card utilizing dynamic cryptograms including a single use cryptographic key" and Manduley is merely another method updating /re-keying of encryption keys. Office Action at 11. Royyuru, however, does not teach "utilizing dynamic cryptograms including a single use cryptographic key" and Manduley not change the underlying payment transaction between the card and card reader, which in Royyuru uses multiple permanent cryptographic keys of the payment instrument. Applicant therefore submits that there is no apparent reason to modify Royyuru in light of Manduley to achieve the claimed invention.

Applicant respectfully submits the Royyuru and Manduley, either alone or combination, fail to teach or reasonably suggest the combination of limitations in Claim 30. Applicant therefore submits that Claim 30 is allowable. For reasons readily apparent from the foregoing, Applicant submits that Claim 44 is also allowable. Applicant further submits that the dependent claims are allowable at least by virtue of their dependency.

New Claims

New claims 59-64 have been added without the addition of new matter. Claims 59-60 are supported at least at paragraph [0225]. Claims 61-62 are supported throughout the specification. Claims 53-64 are supported at least at FIG. 22 and the accompanying discussion.

Conclusion

Applicant has now made an earnest attempt to place this case in condition for allowance. Other than as explicitly set forth above, this reply does not include an acquiescence to statements, assertions, assumptions, conclusions, or any combination thereof in the Office Action. For the foregoing reasons and for other reasons clearly apparent, Applicant respectfully requests full allowance of Claims 30-58. The Examiner is invited to telephone the undersigned at the number listed below for prompt action in the event any issues remain.

An extension of one (1) month is requested and a Notification of Extension of Time Under 37 C.F.R. § 1.136 with the appropriate fee is enclosed herewith.

The Director of the U.S. Patent and Trademark Office is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

Sprinkle IP Law Group
Attorneys for Applicant

/John L. Adair/

John L. Adair
Reg No. 48,828

Date: October 5, 2017

1301 W. 25th Street, Suite 408
Austin, TX 78705
Tel. (512) 637-9220
Fax. (512) 371-9088

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
NOTIFICATION OF EXTENSION OF TIME UNDER 37 C.F.R § 1.136	Atty. Docket No. **STAPP1100-5**

First Named Inventor **C. Douglas Yeager**	
Application Number **13/599,647**	Filed **August 30, 2012**
Title **SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE** (As Amended)	
Group Art Unit **3695**	Examiner **Puttaiah, Asha**
Confirmation No. **1919**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

CERTIFICATION UNDER 37 C.F.R. §1.8

I hereby certify that this document is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on October 5, 2017.

Margarita Marquez

Applicant hereby takes an Extension of Time for responding to the **Office Action** mailed **June 5, 2017** for a period of **1** month.

		Small Entity	*Large Entity*
X	First Month	$ 100.00	$ 200.00
	Second Month	$ 300.00	$ 600.00
	Third Month	$ 700.00	$ 1,400.00
	Fourth Month	$ 1,100.00	$ 2,200.00
	Fifth Month	$ 1,500.00	$ 3,000.00
	TOTAL	**$ 100.00**	**$**

The Commissioner is hereby authorized to deduct the above-noted fee from Deposit Account 50-3183 of Sprinkle IP Law Group. If any fees are inadvertently omitted, additional fees are required, or if any amounts have been overpaid, please appropriately charge or credit those fees to Deposit Account No. 50-3183 of SPRINKLE IP LAW GROUP.

Respectfully submitted,
Sprinkle IP Law Group

Attorneys for Applicant

John L. Adair
Reg. No. 48,828

Dated: October 5, 2017
1301 W. 25th Street, Suite 408
Austin, Texas 78705
(512) 637.9220 - Telephone
(512) 371.9088 - Facsimile

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. (Opt.) **STAPP1100-5**

First Named Inventor **C. Douglas Yeager**	
Application Number **13/599,647**	Date Filed **August 30, 2012**
Title **SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE (as amended)**	
Group Art Unit **3695**	Examiner **Asha Puttaiah**
Confirmation Number **1919**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATION OF TRANSMISSION UNDER 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on October 5, 2017.

Margarita Marquez

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. A copy of foreign patent documents as well as the information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

☐ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☐ This Information Disclosure Statement is being submitted before the mailing of a first Office action on the merits; or

☐ This Information Disclosure Statement is being submitted before the mailing of a first Office action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

☒ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(b) and before the mailing date of any of a Final Action under 37 C.F.R. § 1.113, a Notice of Allowance under 37 C.F.R. § 1.311, or an Action that otherwise closes prosecution in the application, and is accompanied by one of:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); or
- ☒ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(c) and on or before payment of the issue fee and is accompanied by:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); and
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

Pursuant to 37 C.F.R. § 1.97(e), Applicant hereby states:

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. § 1.56(c) more than three months prior to the filing of the information disclosure statement.

Pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application.

Respectfully submitted,

SPRINKLE IP LAW GROUP
Attorneys for Applicant

John L. Adair
Reg. No. 48,828

Dated: October 5, 2017

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 371-9088

INFORMATION DISCLOSURE STATEMENT				Application Number	13/599,647
				Filing or 371 (c) Date:	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	Puttaiah, Asha
Sheet	1	of	1	Attorney Docket Number	STAPP1100-5

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C18	Examination Report issued for European Patent Application No. 12 827 026.1, mailed June 23, 2017, 9 pages.	
	C19	Examiner's Report issued for Canadian Patent Application No. 2,846,462, mailed August 1, 2017, 5 pages.	

Examiner Signature		Date Considered	

Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
Postbus 5818
2280 HV Rijswijk
NETHERLANDS
Tel: +31 70 340 9040
Fax: +31 70 340 3016

Boult Wade Tennant
Verulam Gardens
70 Gray's Inn Road
London WC1X 8BT
ROYAUME-UNI

Formalities Officer
Name: Dahl, Pia
Tel: +31 70 340 - 4449
or call
+31 (0)70 340 45 00

Substantive Examiner
Name: Horst, David
Tel: +31 70 340 - 3112

Application No.	Ref.	Date
12 827 026.1 - 1871	PEH/P131279EP00	23.06.2017
Applicant: SimplyTapp, Inc.		

Communication pursuant to Article 94(3) EPC

The examination of the above-identified application has revealed that it does not meet the requirements of the European Patent Convention for the reasons enclosed herewith. If the deficiencies indicated are not rectified the application may be refused pursuant to Article 97(2) EPC.

You are invited to file your observations and insofar as the deficiencies are such as to be rectifiable, to correct the indicated deficiencies within a period

of 4 months

from the notification of this communication, this period being computed in accordance with Rules 126(2) and 131(2) and (4) EPC. One set of amendments to the description, claims and drawings is to be filed within the said period on separate sheets (R. 50(1) EPC).

If filing amendments, you must identify them and indicate the basis for them in the application as filed. Failure to meet either requirement may lead to a communication from the Examining Division requesting that you correct this deficiency (R. 137(4) EPC).

Failure to comply with this invitation in due time will result in the application being deemed to be withdrawn (Art. 94(4) EPC).

Registered letter

Horat, David
Primary Examiner
For the Examining Division

Enclosure(s): 7 page/s reasons (Form 2906)

1 Executive Summary

1.1 The examiner has considered the applicant's arguments but is of the opinion that a patent cannot be granted on the basis of the documents currently on file. Moreover, the division has once more re-assessed the application as a whole, including the embodiments as presented in the description, and it considers that there are no good prospects of bringing the proceedings to a positive conclusion (EPC Guidelines C-IV, 3).

The examination is being carried out on the **following application documents**

Description, Pages

1, 3, 4, 6-82	as published	
5, 5a-5k	filed in electronic form on	10-11-2014
2	filed in electronic form on	23-03-2016

Claims, Numbers

1-18	filed in electronic form on	24-03-2017

Drawings, Sheets

1/24-24/24	as published

Mastercard, Ex1002, p. 821

2 Cited Documents

2.1 Reference is made to the following documents; the numbering will be adhered to in the rest of the procedure.

D1 US 2011/099079 A1 (WHITE SPENCER NEIL [US])
28 April 2011 (2011-04-28)

D2 WO 01/08113 A1 (VISA INT SERVICE ASS [US]; DAVIS VIRGIL M [US]; CUTINO SUZANNE C [US];)
1 February 2001 (2001-02-01)

D3 US 2010/153721 A1 (MELLQVIST ANDERS [SE])
17 June 2010 (2010-06-17)

D4 WO 2009/017754 A1 (EBAY INC [US]; MURPHY TIMOTHY [US]) 5 February 2009 (2009-02-05)

D5 US 2002/026414 A1 (NAKAJIMA MITSURU [JP] ET AL)
28 February 2002 (2002-02-28)

3 Amendments (Art. 123(2) EPC)

3.1 With the letter received on 24-03-2017, the applicant has filed amendments that appear to meet Article 123(2) EPC for the reasons presented in the letter.

4 Clarity and Conciseness (Art. 84 EPC)

4.1 The application does not meet the requirements of Article 84 EPC, because claim 1 is not clear. Claim 1 states "... the mobile device participating mobile device ..." which leaves the reader in doubt as to the actual meaning of such sentence.

Mastercard, Ex1002, p. 822

5 Novelty and Inventive Step (Art. 52(1), 54 and 56 EPC)

5.1 The present application (see [0007], [0105], [0137]-[0139]) is about a method for authorizing a financial transaction including a mobile device, a Point of Sale/POS and a remote application system.

5.2 Document D1, which is considered as the closest prior art, is about (see D1 abstract) securing payments, the system comprising a mobile device, a POS and a payment server.

5.3 Document D1 discloses in terms of claim 1:

A method for an interrogation between a point-of-sale and a mobile device for digital credential data to authorize a transaction ("methods for securing payments", [0009]; "... mobile communication device ... point of sale ... payment server ... one-time digital key ...", [0028], ref. 100, 120, 140 in figure 1; "... authorization is required ...", [0033]):

for a mobile device that comprises an operating system and an application that runs in the operating system and an application that has the capability of being interrogated by a point-of-sale (POS) for digital credential data used to authorize approval of transaction ("mobile wallet application 670 on a mobile communications device 600", [0035]; since there is an application running on the mobile device, the operating system is considered as implicit; "... point of sale device communicates amount to mobile communication device ... one-time digital key ... If the numbers or codes match, payment server 140 deducts the amount from an account associated with mobile communications device 100, and sends a confirmation to point-of-sale device 120", [0028]), performing a device preparation comprising:

requesting, from a remote application system that comprises a plurality of secure element representations, a transaction cache for a particular secure element ("a payment server 440 issues a one-time digital key S450 to mobile communications device 400", [0032], ref. S450 in figure 4);

receiving transaction cache data at the mobile device, ~~the transaction cache data containing data required to formulate application program data unit APDU responses to APDU commands~~, the transaction cache data including a temporary cryptographic key associated with an account to be used during a POS interrogation ("a payment server 440 issues a one-time digital key S450 to mobile communications device 400. The one-time digital key is stored on mobile communications device 400 until it is used. Mobile communications device 400 uses the one-time digital key to submit a payment S451 to a point-of-sale (POS) device 420", [0032], ref. S450, S451 in figure 4);

Mastercard, Ex1002, p. 823

wherein the application does not have access to a permanent cryptographic key for the digital credential ("The one-time digital key is stored on mobile communications device 400 until it is used, until it is replaced by a new one-time digital key, for a period of time, etc.", [0032], therefore the one-time digital key is not permanent, hence the application does not have access to a permanent cryptographic key for the digital credential); and

after the mobile device receives the transaction cache data, the mobile device participating mobile device in an interrogation according to a card specification between a POS terminal and the mobile device ("Mobile communications device 400 uses the one-time digital key to submit a payment S451 to a point-of-sale (POS) device 420, the payment including a payment number and an amount", [0032], ref. S451 in figure 4) comprising:

receiving at least one POS command communication sent by the POS terminal to the mobile device over a communications channel the at least one POS command communication comprising an ~~APDU~~ command to request a cryptogram and unpredictable data ("the mobile communications device receives a one-time digital key S560. The one-time digital key may be sent by a point-of-sale POS device", [0034], ref. S560 in figure 4; "using near field communication NFC to communicate with the point-of-sale device", [0010], NFC is considered a type of card specification);

formulating an unpredictable cryptogram response containing an unpredictable cryptogram calculated from the temporary cryptographic key and, at least in part, the unpredictable data from the POS terminal ("The mobile communications device uses the one-time digital key and a random number from a random number generator algorithm to generate a payment number S561", [0034], ref. S561 in figure 5); and

responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending through the communication channel at least one device response communication comprising an account identifier and a response ~~APDU~~ containing the unpredictable cryptogram ("The mobile communications device then sends the payment number to the POS device S562", [0034], ref. S562 in figure 5, the payment number is considered to also comprise the account identifier since the system knows which account to deduct as seen in [0032]); and

updating or replacing the temporary cryptographic key associated with the account for a subsequent transaction (S455 in figure 4, S560 in figure 5).

5.3.1 The differences between claim 1 and D1 are that the communications use application program data unit APDU commands.

5.3.2 Nevertheless, the use of APDU commands is just a normal design procedure to the skilled person.

5.3.3 Therefore, the subject-matter of claim 1 is not inventive under Article 56 EPC.

5.4 The subject-matter of dependent claims 2-18 is not inventive under Article 56 because they are either a normal design procedure to the skilled person or disclosed by the available prior art. For more information see the previous communications.

6 Arguments of the applicant

6.1 First of all, the examiner would like to apologize to the applicant for the previous' communication mistakes and would thank the applicant's representative for the extensive letter received on 24-03-2017 which addresses all the points previously made by the examiner. In response, the examiner has raised the objections in the present communication to address the points stated by the applicant in the letter. Notwithstanding the objections presented by the examiner, the following should be noted:

6.2 With the electronic form received on 24-03-2017, the applicant argues that D1 does not disclose a "temporary cryptographic key" used to generate an "unpredictable cryptogram" that is sent to a POS terminal.

6.2.1 The examiner disagrees. D1 discloses in [0034] that the mobile communications device uses the one-time digital key and a random number from a random number generator algorithm to generate a payment number. This generation is indeed an "unpredictable cryptogram" since it uses a random number generator. Such generation is considered to be of a cryptographic nature because it is used to secure the payment (see D1 [0032] and [0034]) and because both the generation algorithm and the input parameters are needed in order to verify the message (see D1 [0028]).

6.3 The applicant also argues that this combination is obfuscation and not encryption.

6.3.1 The examiner disagrees for the following reasons:

6.3.2 Obfuscation is the willful obscuring of the intended meaning of communication by making the message difficult to understand.

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries.

An obfuscation method may or may not be a cryptographic method and a cryptographic method may or may not be an obfuscation method. Therefore, implying that a method is obfuscation and therefore not encryption is an incorrect assessment.

6.3.3 Moreover, D1 [0028] discloses that combining may include multiplying the numbers, appending one number to the other, mixing the numbers, adding the numbers, subtracting the numbers, etc.

Adding the numbers is a type of the Caesar's cipher algorithm which takes an input text and a key which acts as a shift to the input text.

Hence, the combination used in D1 is in fact an encryption algorithm.

7 Procedure

7.1 It is not at present apparent which part of the application could serve as a basis for a new, allowable claim. Should the applicant nevertheless regard some particular matter as patentable, an independent claim should be filed taking account of Rule 43(1) EPC. The applicant should also indicate how the subject-matter of the new claim differs from the state of the art and the significance thereof.

7.2 When filing amended claims the applicant should at the same time bring the description into conformity with the amended claims. Care should be taken during revision, especially of the introductory portion and of any statements of problem or advantage, not to add subject-matter which extends beyond the content of the application as originally filed (Article 123(2) EPC).

7.3 In order to comply with the requirements of Rule 137(4) EPC, the applicant should clearly identify the amendments made, irrespective of whether they concern amendments by addition, replacement or deletion, and indicate the passages of the application as filed on which these amendments are based (Guidelines H-III, 2.1).

7.4 According to the application of Rule 50(1) EPC in combination with Rule 49(8) EPC, no hand-written amendments by the applicant are accepted (Office Journal of the EPO 2013, 603-604).

Mastercard, Ex1002, p. 826

7.5 The independent claim is not in the two-part form in accordance with Rule 43(1) EPC, which in the present case would be appropriate, with those features known in combination from the prior art being placed in the preamble (Rule 43(1)(a) EPC) and the remaining features being included in the characterising part (Rule 43(1)(b) EPC).

7.6 The features of the claims should be provided with reference signs placed in parentheses to increase the intelligibility of the claims (Rule 43(7) EPC). This applies to both the preamble and characterising portion (see Guidelines F-IV, 4.19).

Mastercard, Ex1002, p. 827

1 August 2017 (01-08-2017)

GOWLING WLG (CANADA) LLP
2600 - 160 Elgin Street
OTTAWA Ontario
K1P 1C3

Application No.	:	**2,846,462**
PCT No.	:	**US2012053129**
Owner	:	SIMPLYTAPP, INC.
Title	:	**SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM**
Classification	:	G06Q 20/40 (2012.01)
Your File No.	:	**08927357CA**
Examiner	:	Kazem Ziaie

YOU ARE HEREBY NOTIFIED OF A REQUISITION BY THE EXAMINER IN ACCORDANCE WITH SUBSECTION 30(2) OF THE *PATENT RULES*. CONSISTENT WITH THE OBJECTIVES OF SECTION 28 OF THE *PATENT RULES*. IN ORDER TO AVOID ABANDONMENT UNDER PARAGRAPH 73(1)(a) OF THE *PATENT ACT*, A WRITTEN REPLY MUST BE RECEIVED WITHIN **THREE (3)** MONTHS AFTER THE ABOVE DATE.

This application has been examined taking into account the applicant's correspondence received in this office on 4 May 2017 (04-05-2017).

The number of claims in this application is 134.

After a careful review and examination of the newly submitted claimed dated 04-05-2017, the Examiner is of the opinion that the application is directed to a plurality of inventions, as detailed below. As such, the search and substantive examination of the claimed subject matter have been deferred pending the applicant's response to the present requisition.

The examiner has identified the following defects in the application:

Lack of unity

The application does not comply with subsection 36(1) of the *Patent Act*. The claims are directed to a plurality of alleged inventions as follows:

Group A - Claims 1-63 are directed to a method for acquiring digital credential data by a point-of-sale terminal from a mobile device for authorization of a financial transaction comprising: using a remote permanent cryptographic key to calculate an expected cryptogram, wherein the expected cryptogram is expected to comprise at least a portion of the digital credential data, wherein the remote permanent cryptographic key is persistently stored at a remote source that is remote from the mobile device and wherein there is no duplicate local permanent cryptographic key persistently stored locally to the mobile device; performing an interrogation between the point-of-sale terminal and the mobile device comprising: sending through a communication channel at least one POS command communication from the point-of-sale terminal to the mobile device requesting the digital credential data wherein the at least one POS command communication conforms to a card specification; and sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal comprising the expected cryptogram as the at least a portion of the digital credential data; wherein the financial transaction is authorized;

Group B - Claims 64-105 are directed to a method for an interrogation between a point-of-sale and a mobile device for digital credential data to authorize a transaction: for a mobile device that comprises an operating system and an application that runs in the operating system that has the capability of being interrogated by a point-of-sale (POS) for digital credential data used to authorize approval of a transaction, performing a device preparation, the device preparation comprising: requesting over a network, from a remote application system that comprises a plurality of secure element representations, a transaction cache for a particular secure element; receiving transaction cache data at the mobile device, the transaction cache data containing data required to formulate application program data unit (APDU) responses to APDU commands, the transaction cache data including a temporary cryptographic key associated with an account to be used during a POS interrogation, wherein the application does not have access to a permanent cryptographic key for the digital credential; and the mobile device participating in the interrogation according to a card specification between a POS terminal and the mobile device after the device preparation, participating in the interrogation comprising: receiving at least one POS command communication sent by the POS terminal to the mobile device over a communications channel, the at least one POS command communication comprising (a) an APDU command to request a cryptogram and (b) unpredictable data; generating an unpredictable cryptogram using the temporary cryptographic key and, at least in part, the unpredictable data from the POS terminal and formulating a response APDU containing the unpredictable cryptogram; and responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending through the communication channel at least one device response communication from the mobile device to the POS terminal, the at least one device response communication comprising an account identifier and the response APDU containing the unpredictable cryptogram; and updating or replacing temporary cryptographic key associated with the account for a subsequent transaction; and

Group C - Claims 106-134 are directed to method for secure application-based participation in a payment card transaction authorization process by a mobile device, the method comprising: receiving over a wireless network at a mobile device a first non-permanent cryptographic key associated with an account having a corresponding digital credential, wherein the mobile device comprises an operating system and an application executable in the operating system, the application interrogable for digital credential data corresponding to the account, wherein the application does not access a permanent cryptographic key associated with the account during interrogations; locally storing a first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account; participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device comprising: receiving at least one POS command communication sent by the POS terminal over a communications channel, wherein the at least one POS command communication comprises a request for digital credential data to authorize a transaction against the account; generating a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram; and responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to an electronic reader through the communication channel, the at least one device response communication comprising at least a portion of the digital credential data, wherein the at least a portion of the digital credential data comprises the response cryptogram and an account identifier for the account; receiving a second non-permanent cryptographic key at the mobile device, wherein the second non-permanent cryptographic key is associated with the account; and replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key as the local cryptographic key associated with the account prior to the application participating in a subsequent interrogation.

According to subsection 36(2) of the *Patent Act*, after limiting the claims of the present application to one invention only, the applicant may make any other invention disclosed the subject of a divisional application. The applicant is advised that once an election has been made, further prosecution of the present application will be limited to the invention so elected.

In accordance with subsection 28(2) of the *Patent Rules*, this application will no longer qualify for advanced examination requested by the applicant if the application is deemed to be abandoned in accordance with subsection 73(1) of the *Patent Act* or if an extension of time under subsection 26(1) of the *Patent Rules* is granted.

In view of the foregoing defects, the applicant is requisitioned, under subsection 30(2) of the *Patent Rules*, to amend the application in order to comply with the *Patent Act* and the *Patent Rules* or to provide arguments as to why the application does comply.

Under section 34 of the *Patent Rules*, any amendment made in response to this requisition must be accompanied by a statement explaining the nature thereof, and how it corrects each of the above identified defects.

Kazem Ziaie
Patent Examiner
819-639-8376

As per CIPO Client Service Standards, a response to a telephone enquiry or voice mail should be provided by the end of the next business day. In the event that attempts to reach the examiner are unsuccessful, the examiner's Section Head, Eric Lafontaine, can be reached at 819-635-3356.

For general inquiries: 1-866-997-1936 or for more options see http://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/wr00006.html.

CIPO values your feedback and invites you to complete a short and anonymous ongoing survey on patent examination products and services. You can access the survey at the following link: http://ic.sondages-surveys.ca/s/SCB-OPS/langeng.

2846462B kzz.docm

The Examination Search Report is provided for reference only and is not part of any requisition made by the examiner in accordance with the *Patent Act* or *Rules*. The applicant is not required to respond to the information contained in the Examination Search Report.

Examination Search Report

Box I: General Information

Application No.	2,846,462	Search Report Date	2017-07-24
Title	SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM		
Examiner	Kazem Ziaie	Search Conducted?	No

No search was conducted for the following reasons :	
- Search deferred - see report for reasoning (lack of unity, excluded subject matter etc.)	Yes
- Relied on previous search results (CIPO and/or by Foreign Office)	N/A

Box II: Family Prosecution

Family Member	File Wrapper Reviewed	Status of Prosecution
US2012317628 A1	2016-08-02	In Progress
EP 2 751 754 A4	2016-08-02	In Progress

Box IV: Search History

No Search Conducted

Version 9

Electronic Patent Application Fee Transmittal

Application Number:	13599647
Filing Date:	30-Aug-2012
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Filer:	John L. Adair/Margarita Marquez
Attorney Docket Number:	STAPP1100-5

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 1 month with $0 paid	2251	1	100	100
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	90	90
		Total in USD ($)		**190**

Electronic Acknowledgement Receipt	
EFS ID:	30581267
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Customer Number:	44654
Filer:	John L. Adair/Margarita Marquez
Filer Authorized By:	John L. Adair
Attorney Docket Number:	STAPP1100-5
Receipt Date:	05-OCT-2017
Filing Date:	30-AUG-2012
Time Stamp:	18:28:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$190
RAM confirmation Number	100617INTEFSW00005632503183
Deposit Account	503183
Authorized User	Margarita Marquez
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		STAPP1100-5_ROA_10-05-2017.pdf	1476237 ac3854b059b44e79ce557e4616ad07c611e2efdc40	yes	20

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	10
Applicant Arguments/Remarks Made in an Amendment	11	20

Warnings:

Information:

2	Extension of Time	STAPP1100-5_Time_Extension.pdf	778771 e6ca5a08bab3f52c0572f0acc6ce772a10bdcc57	no	2

Warnings:

Information:

3		STAPP1100-5_IDS_10-05-2017.PDF	999812 a2e0e8159380cbe5aa1e15dffe08c15c18fc1aa0	yes	4

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Transmittal Letter	1	3
Information Disclosure Statement (IDS) Form (SB08)	4	4

Warnings:

Information:

4	Non Patent Literature	STAPP1100_Ref_C18.pdf	7881895 0c9ff9f095cfa702578b78aff91ae2b22e51f571	no	9
Warnings:					
Information:					
5	Non Patent Literature	STAPP1100_Ref_C19.pdf	5884931 3a3a77a185127673820ec4799882fd8d9571b526	no	5
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	32791 0a2ab5ac4aa1fe4722177755f3121f8202968233e	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	17054437		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Patent Application Fee Transmittal

Application Number:	13599647
Filing Date:	30-Aug-2012
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Filer:	John L. Adair/Margarita Marquez
Attorney Docket Number:	STAPP1100-5

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	2202	4	40	160
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	160

Electronic Acknowledgement Receipt	
EFS ID:	30618553
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Customer Number:	44654
Filer:	John L. Adair/Margarita Marquez
Filer Authorized By:	John L. Adair
Attorney Docket Number:	STAPP1100-5
Receipt Date:	10-OCT-2017
Filing Date:	30-AUG-2012
Time Stamp:	20:31:08
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$160
RAM confirmation Number	101117INTEFSW00007105503183
Deposit Account	503183
Authorized User	Margarita Marquez
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Fee Worksheet (SB06)	fee-info.pdf	30683 4ac943d5452a4a4d0a28dc53e645bd177f3ec2e9c	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	30683		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/599,647	Filing Date 08/30/2012	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 = *		X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 = *		X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	10/05/2017	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 33	Minus	** 29	= 4	X $40 =	160
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $210 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	**160**

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
PAULA MCCRAY STANLEY

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

INFORMATION DISCLOSURE STATEMENT				Application Number	13/599,647
				Filing or 371 (c) Date:	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	Puttaiah, Asha
Sheet	1	of	1	Attorney Docket Number	STAPP1100-5

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C20	Examination Report issued for Malaysian Patent Application No. PI2014000569, mailed October 13, 2017, 3 pages.	

Examiner Signature		Date Considered	

PERBADANAN HARTA INTELEK MALAYSIA
INTELLECTUAL PROPERTY CORPORATION OF MALAYSIA
(Agensi di bawah KPDNKK)
Unit 1-7 & Mezzanine, Aras 12–19
Tower B, Menara UOA Bangsar
No. 5, Jalan Bangsar Utama 1
59000 KUALA LUMPUR
MALAYSIA

Tel : +603 - 2299 8400
Faks (Fax) : +603 - 2299 8989
Laman Web (Web) : www.myipo.gov.my

APPLICATION NO	: PI 2014000569
APPLICANT	: SIMPLYTAPP, INC.
FILING DATE	: 30 AUGUST 2012
APPLICANT'S /AGENT'S FILE REF	: P-025191
DATE OF MAILING	: 13 OCTOBER 2017

~~SUBSTANTIVE / MODIFIED SUBSTANTIVE*~~ EXAMINATION
ADVERSE REPORT (Section 30(1) / 30(2))

The examiner has examined / ~~further examined~~* the above application and has reported as follows:

(a) ☒ The application does not comply with the substantive requirements under section 30(1) of the Patents Act 1983.The examiner's report is attached, **OR**

(b) ☐ The application does not comply with the modified substantive requirements under section 30(2) of the Patents Act 1983. The examiner's report is attached.

(c) search under Regulation 27C / 27D of the Patents Act 1983 :

☒ The search report is attached.

You are invited to respond to this report. In accordance with Regulation 27C / 27D, a response should be filed at the above Office or Branch Offices within **TWO (2) MONTHS** from the date of mailing, otherwise this application may be refused under Section 30(3) of the Patents Act 1983.

Date : 13 OCTOBER 2017

(Khairul Syafiq Bin Mohd Shukri)
for Registrar of Patents
✉khairulsyafiq@myipo.gov.my
☎03-2299 8849

To : BOEY WENG CHOONG
C/O HENRY GOH & CO. SDN. BHD
217, JALAN IMBI
55100 KUALA LUMPUR
MALAYSIA

SUBSTANTIVE / MODIFIED SUBSTANTIVE* EXAMINATION
EXAMINER'S REPORT TO THE REGISTRAR
UNDER SECTION 30(1) / 30(2)

Specification Details
The examination was carried out on the following application documents:

Description :	Pages	1 - 79	filed on	27 February 2014
Claims :	Pages	80 - 91(claims no.:1 - 29)	filed on	27 February 2014
Drawings :	Figure	1 - 30	filed on	27 February 2014
Abstract :	Page	92	filed on	27 February 2014
	Figure	1	filed on	27 February 2014

Documents Cited or Considered Relevant

Reference is made to AU 2012301897 B2.

Basis of Examination

1. Your corresponding Australia patent no. **AU 2012301897 B2** has been granted with claims which are narrower in scope than the present claims of your Malaysian application, and certain prior art listed on the patent was considered relevant during prosecution. It therefore appears, **prima facie**, that your present claims are not novel and / or inventive as required by sections 14 and 15 having regard to that prior art.

The claims should therefore be amended, and if they are brought into conformity with those of the above patent further examination will be expedited.

2. The technical features of the claim(s) is (are) not followed by appropriate reference signs in parentheses [Reg. 13(4)].

To increase the intelligibility, the technical features of the claims should be provided with reference signs placed in parentheses [Reg. 13(4)]. This applies to both the preamble and characterizing portion. These reference signs are not however, to be construed as limiting the scope of the claims, but merely as aids to an easier understanding of the defined subject matter.

3. Each main feature of the abstract is not followed by a reference sign in parentheses [Reg. 16(6)].

4. Amendments to the specification should be effected by filing replacement pages in duplicate.

[end of report]

Date of Report :

Examiner :
Nursyuhada Mohd Shafawi

Email : nursyuhada@myipo.gov.my

SEARCH REPORT
EXAMINER'S REPORT TO THE REGISTRAR

DOCUMENT CONSIDERED TO BE RELEVANT			
Category	Document details, with indication, where appropriate, of relevant passages	Relevant to Claim(s)	CLASSIFICATION OF THE APPLICATION (IPC)
	Reference is made to AU 2012301987 B2		G06Q 20/00
			CORRESPONDING FOREIGN SEARCH
			AU 2012301987 B2
			TECHNICAL FIELDS SEARCHED
			G06Q

Date of Report :	Examiner : Nursyuhada Mohd Shafawi	Email : nursyuhada@myipo.gov.my

CATEGORY OF CITED DOCUMENTS

X : Relevant if taken alone
Y : Relevant if combined with another cited document
A : Technological background
P : Document published on or after declared priority date but before filing date of the present application
E : Conflict with earlier Malaysian patent/utility innovation

Electronic Acknowledgement Receipt

EFS ID:	30772579
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Customer Number:	44654
Filer:	John L. Adair/Margarita Marquez
Filer Authorized By:	John L. Adair
Attorney Docket Number:	STAPP1100-5
Receipt Date:	26-OCT-2017
Filing Date:	30-AUG-2012
Time Stamp:	15:50:03
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		STAPP1100-5_IDS_10-26-2017.pdf	1049659 872d11c0f75d092a5cd6f5cd92c4e513872fff216	yes	4

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	3	
	Information Disclosure Statement (IDS) Form (SB08)		4	4	
Warnings:					
Information:					
2	Non Patent Literature	STAPP1100_Ref_C20.pdf	237677 abbf2f7f3f3f3a9f3c0d3b72161c3727fd6bd2ecc6	no	3
Warnings:					
Information:					
		Total Files Size (in bytes):	1287336		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. (Opt.) **STAPP1100-5**

First Named Inventor **C. Douglas Yeager**	
Application Number **13/599,647**	Date Filed **August 30, 2012**
Title **SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE (as amended)**	
Group Art Unit **3695**	Examiner **Asha Puttaiah**
Confirmation Number **1919**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATION OF TRANSMISSION UNDER 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on December, 2017.

M. Marquez

Margarita Marquez

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. A copy of foreign patent documents as well as the information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

☐ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☐ This Information Disclosure Statement is being submitted before the mailing of a first Office action on the merits; or

☐ This Information Disclosure Statement is being submitted before the mailing of a first Office action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

☒ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(b) and before the mailing date of any of a Final Action under 37 C.F.R. § 1.113, a Notice of Allowance under 37 C.F.R. § 1.311, or an Action that otherwise closes prosecution in the application, and is accompanied by one of:

☒ The statement specified in 37 C.F.R. § 1.97(e); or

☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(c) and on or before payment of the issue fee and is accompanied by:

☐ The statement specified in 37 C.F.R. § 1.97(e); and

☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

Pursuant to 37 C.F.R. § 1.97(e), Applicant hereby states:

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. § 1.56(c) more than three months prior to the filing of the information disclosure statement.

Pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application.

Applicant does not believe any fees are due and owing at this time. If Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

SPRINKLE IP LAW GROUP
Attorneys for Applicant

John L. Adair
Reg. No. 48,828

Dated: Oct 25, 2017

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 371-9088

INFORMATION DISCLOSURE STATEMENT				Application Number	13/599,647
				Filing or 371 (c) Date:	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	Puttaiah, Asha
Sheet	1	of	1	Attorney Docket Number	STAPP1100-5

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C21	Office Action issued for Chinese Patent Application No. 201280053080.6, mailed October 18, 2017, 19 pages.	

Examiner Signature		Date Considered	

CPEL1450577P

State Intellectual Property Office, P.R. China

Address : Receiving Section of the Chinese Patent Office, No. 6 Tucheng Road West, Haidian District, Beijing, Postal code: 100088

Applicant	SIMPLYTAPP，INC.			**Date of Issue**
Agent	China Patent Agent (H.K.) Ltd.			October 18, 2017
Patent Application No.	201280053080.6	**Application Date**	August 30, 2012	
Title of Invention	SYSTEMS AND METHOD FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM			

3rd *Office Action*

1. ☑ The examiner has received the Observations, submitted by the applicant on July 20, 2017 in response to the 2nd Office Action issued by the Patent Office, and on this basis continued to conduct examination as to substance of the captioned patent application.
   ☐ On the basis of the Reexamination Decision made by the Reexamination Board of the Chinese Patent Office on _____ , the examiner has continued to conduct examination as to substance of the captioned patent application.
   ☐

2.Further examination has been conducted in the light of the following application document(s):
   ☐ the amended application document(s) attached to the said observations.
   ☑ the application document(s) at which the previous Office Action is directed, and the replacement sheet(s) of the amended application document(s) attached to the said Observations.
   ☐ the application document(s) at which the previous Office Action is directed.
   ☐ the application document(s) confirmed in the said Reexamination Decision.
   ☐

3. ☑ In this Office Action no new reference documents have been cited.
   ☐ The following reference document(s) is/are cited in this Office Action. (Its/Their serial number(s) shall come after those previously cited and will continue to be used throughout the examination procedure):

Mastercard, Ex1002, p. 853

Serial No.	Number or Title(s) of Reference Document(s)	Date of Publication (or filing date of interfering appl.)

4. Concluding comments of the examiner:

☐ On the description:
- ☐ The amendment to the description is not in conformity with the provision of Art. 33 of the Patent Law.
- ☐ The content of the application comes within the scope where no patent right shall be granted as prescribed in Art. 5 of the Patent Law.
- ☐ The description is not in conformity with the provision of Art. 26, para. 3 of the Patent Law.
- ☐ The drafting of the description is not in conformity with the provision of Rule 18 of the Implementing Regulations.

☑ On the claims:
- ☐ The amendment to Claim(s) _____ is not in conformity with the provision of Art. 33 of the Patent Law.
- ☐ Claim(s) _____ come(s) within the scope where no patent right shall be granted as prescribed in Art. 25 of the Patent Law.
- ☐ Claim(s) _____ is/are not in conformity with the definition of invention in Rule 2, para. 1 of the Implementing Regulations.
- ☐ Claim(s) _____ possess(es) no novelty as prescribed in Art. 22, para. 2 of the Patent Law.
- ☑ Claim(s) 1-18 possess(es)no inventiveness as prescribed in Art. 22, para. 3 of the Patent Law.
- ☐ Claim(s) _____ possess(es) no practical applicability as prescribed in Art. 22, para. 4 of the Patent Law.
- ☐ Claim(s) _____ is/are not in conformity with the provision of Art. 26, para. 4 of the Patent Law.
- ☐ Claim(s) _____ is/are not in conformity with the provision of Art. 31, para. 1 of the Patent Law.
- ☐ Claim(s) _____ is/are not in conformity with the provisions of Rule 20 of the Implementing Regulations.
- ☐ Claim(s) _____ is/are not in conformity with the provision of Art. 9 of the Patent Law.
- ☐ Claim(s) _____ is/are not in conformity with the provision of Rule 23 of the Implementing Regulations.

Mastercard, Ex1002, p. 854

See the text portion of this Office Action for a detailed analysis of the above concluding comments.

5. In view of the above concluding comments, the examiner deems that

☐ the applicant should make amendment to the application document(s) according to the requirements raised in the text portion of this Office Action.

☐ the applicant should expound in his/its observations the reason why the captioned patent application is patentable and make amendment to what is not in conformity with the provisions as pointed out in the text portion of this Office Action, otherwise the said application will be rejected.

☑ the patent application has no substantive content(s) for which the patent right may be obtained, if the applicant has no sufficient reason to demonstrate that the captioned application may be granted a patent right, said the application will be rejected.

6. **The applicant should pay attention to the following matters**:

(1) According to the provision of Art. 37 of the Patent Law, the applicant should submit his/its observations within **two** months from the date of receipt of this Office Action; if, without any justified reason(s), the time limit for making a response is not met, the said application shall be deemed to have been withdrawn.

(2) The amendment(s) made by the applicant to the application should be in conformity with the provisions of Art. 33 of the Patent Law and Rule 51 of the Implementing Regulations thereof, the amended text should be in duplicate and its form should conform to the relevant provisions of the Guidelines for Examination.

(3) The observations and/or amended text of the applicant should be submitted to the Receiving Section of the Chinese Patent Office by mail or by personal delivery, if not submitted Receiving Section by mail or by personal delivery, the document(s) will have no legal effect.

(4) If no appointment is made in advance, the applicant and/or the agent shall not come to the Chinese Patent Office to hold an interview with the examiner.

7. This Office Action consists of the text portion totaling __7___ page(s) and of the following attachment(s):

☐ ____ copy(copies) of the reference document(s) cited totaling ____ page(s).

Examination Dept. No. _____ Examiner _____

2206

Mastercard, Ex1002, p. 855

Your Ref: STAPP1101-CN
Our Ref: CPEL1450577P
Application No: 201280053080.6

TEXT OF THIRD OFFICE ACTION

The applicant submitted an Observation and the amended application text on July 20, 2017. Upon further examination of said documents, the examiner has the following comments.

I. Claims 1-18 do not possess inventiveness as prescribed in Article 22(3) of the Patent Law.

1. Claim 1 seeks to protect a method for interrogation between a point-of-sale (POS) terminal and a mobile device for digital credential data to authorize a financial transaction. D1 discloses secure mobile-based financial transactions, and particularly discloses the following features (see paragraphs [0021]-[0033] of the description): the payment server sends a one-time digital key to the mobile terminals (equivalent to prior to an interrogation, the mobile device requesting, over a network, a transaction cache from a remote application system; receiving the transaction cache data at the mobile device, the transaction cache data containing data required to formulate responses to commands, and a temporary cryptographic key); the sale terminal sends the amount to the mobile terminal to acquire the corresponding payment number and etc., the one-time digital key is input to a number generator algorithm to generate the payment number (equivalent to during the interrogation: performing an interrogation according to a card specification between the point-of-sale terminal and the mobile device, sending through a communication channel at least one POS command communication according to a card specification from the point-of-sale terminal to the mobile device, the at least one POS command communication requesting digital credential data, the at least one POS command communication comprising (a) a cryptogram request

Mastercard, Ex1002, p. 856

and (b) unpredictable data); the mobile terminal inputs a one-time digital key to the number generator algorithm to generate the payment number, also may generate in combination with a random number, and sends the payment number to the sale terminal (equivalent to the mobile device generating a cryptogram using the temporary cryptographic key and formulating a response containing the cryptogram generated using the temporary cryptographic key and at least in part the unpredictable data from the POS terminal); the mobile terminal submits a payment request including the payment number and the amount (equivalent to sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal, the at least one device response communication comprising at least one part of the digital credential data, the digital credential data comprising the response, the response containing the cryptogram); the payment server verifies the payment number and confirms the transaction to the POS device.

As the technical solution claimed by claim 1 is compared to the content disclosed by D1, the distinguishing features are the following: (1) a transaction cache for a particular secure element from a remote application system that comprises a plurality of secure element representations; wherein the mobile device comprises an application running in an operating system of the mobile device that is capable of being interrogated by a POS; wherein the application does not have access to a permanent cryptographic key for the digital credential; the cryptographic key is associated with an account to be used during a POS interrogation, the response sent from the mobile device to the point of sale terminal comprising an account identifier; APDU commands and response; (2) using unpredictable data for generating an unpredictable cryptogram; (3) updating or replacing the temporary cryptographic key associated with the account for a subsequent transaction. Based on the distinguishing features, it can be determined that the problems actually solved by claim 1 are: (1) how to

Mastercard, Ex1002, p. 857

make transactions based on secure element; (2) how to generate an expected cryptogram; (3) how to perform subsequent transactions.

Regarding distinguishing feature (1), D3 (US2010153721A1) discloses a method for accessing remote secure elements, and particularly discloses the following feature (see paragraphs [0006]-[0007] and [0029]-[0042] of the description): the secure element (equivalent to an HSM) is located on the remote secure element server, the virtual secure element module is configured to communicate with one or more remote secure element servers. A secure transaction may be established using the virtual secure element module and the remote securing element (equivalent to a remote application system that comprises a plurality of secure element representations); customers can pay by simply waving their portable electronic device at a point-of-sale reader (equivalent to wherein the mobile device comprises an application running in an operating system of the mobile device that is capable of being interrogated by a POS). The feature performs the same function in D3 as it performs in claim 1, both making transactions using remote secure elements, that is, those skilled in the art can get inspiration and apply the method of using remote secure element in D3 to the payment transaction process of D1. In addition, generating payment cryptogram using the permanent cryptogram of a secure element is a common way of a secure element. Therefore, on D3 has disclosed storing secure elements using a remote server for payment, those skilled in the art will easily conceive remotely storing permanent cryptogram corresponding to the secure element and sending the permanent cryptogram of the secure element to the mobile device, to thereby generate the payment cryptogram. On the basis that D1 discloses the payment server sending a one-time key, in order to realize security of payments, those skilled in the art conceive that the application does not have access to a permanent cryptographic key for the digital credential, which is a common technical means in the art of secure

Mastercard, Ex1002, p. 858

payment. Transaction operations are related to accounts, hence, that the cryptographic key is associated with an account to be used during a POS interrogation, and that the response sent from the mobile device to the point of sale terminal comprises an account identifier, can be easily conceived by those skilled in the art. In addition, an APDU command is a common data interaction for secure element transactions. Therefore, the response is APDU responses.

Regarding distinguishing feature (2), D2 (CN101048794A) discloses a method for authorizing a transaction using a dynamic authorization code, and particularly discloses the following feature (see line 1 on page 4 to line 28 on page 5 and line 1 on page 8 to line 19 on page 9 of the description): the unpredictable data includes the transaction amount and etc., the device uses the unpredictable data together with other secret data to generate a dynamic authorization code (equivalent to using unpredictable data for generating an unpredictable cryptogram). The feature performs the same function in D2 as it performs in claim 1, both generating an unpredictable cryptogram using unpredictable data, that is, those skilled in the art can get inspiration and apply the method of generating a cryptogram in D2 to the payment number generation process of D1.

Regarding distinguishing feature (3), D1 (see paragraphs [0021]-[0033] of the description): the payment server automatically sends the next digital key to the mobile terminal to be stored there until the next transaction is processed. On the basis of this, those skilled in the art will easily conceive updating or replacing the temporary cryptographic key associated with the account for a subsequent transaction, which is a common technical means in the art.

Thus it can be seen that it is obvious to those skilled in the art to obtain the technical solution claimed by claim 1 on the basis of D1 in combination with D2, D3 and common technical means in the art. Therefore, claim 1 does not possess prominent substantive feature and notable progress, i.e. does not

Mastercard, Ex1002, p. 859

possess inventiveness as prescribed in Article 22(3) of the Patent Law.

Comments upon claims 2-18 can be referred to in the previous Office Actions.

II. Reply to the applicant's observations.

The applicant deems: D1 does not describe key as a "cryptographic key" nor does it refer to encryption. "Payment number" is not a cryptogram; (2) D1 does not disclose: prior to an interrogation, ""request over a network a transaction cache for a particular secure element from a remote application system that comprises a plurality of secure element representations and receive the transaction cache data at the mobile device, the transaction cache data containing data required to formulate APDU responses to APDU commands, and a temporary cryptographic associated with the particular secure an account to be used during a POS interrogation. . ." and during the interrogation "generate an unpredictable cryptogram using the unpredictable data and the temporary cryptographic key and formulating a response APDU containing the unpredictable cryptogram generated using the temporary cryptographic key and at least in part the unpredictable data from the POS terminal and sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal, the at least one device response communication comprising an account identifier and the response APDU containing the unpredictable cryptogram". Therefore, D1 does not teach the invention to be protected; (3) D3 teaches neither a transaction cache nor temporary cryptographic keys; (4) Claim 18 recites that the cryptogram is a hash.

However, the examiner deems: (1) D1 discloses (see paragraphs [0021]-[0033] of the description): the payment number includes a one-time digital key and a random number, the one-time digital key is sent automatically from the payment server to the mobile terminal, the one-time digital key, in the form of a

Mastercard, Ex1002, p. 860

multi-digit number, is effectively multiplied by the number generator algorithm to create a payment number. Thus it can be seen that D1, like the present application, also generates the payment number (equivalent to cryptogram) by using one-time digital key (equivalent to key). And D3 has given the hint of making transaction payments with remote secure element. And during the process of the secure transactions of secure elements, generating cryptograms using permanent keys to authorize the transaction is a common technical means in the art. For example, D2 has disclosed: the software or circuitry on the mobile device has substantially all of the functionality of a typical smart card, although (equivalent to a secure element); the mobile processing device generates a dynamic authentication code 130 using a key 120, such as an encryption key. The key 120 may be a DES key, a private key, a public key, some combination thereof, or any other data used for encryption or generating a secure message for subsequent authentication.

(2) Please refer to the comments upon claim 1. A part of the distinguishing features is disclosed by D1, D2 and D3, and the rest part can be easily conceived by those skilled in the art on the basis of the disclosures of D1, D2 and D3, which is common technical means in the art.

(3) D1 discloses: a one-time digital key (equivalent to a temporarily used key); D2 discloses: the encryption key or one or more of the keys in a key pair may be encrypted, such as with triple-DES, using the PIN and a Mobile Device Identifier, previously entered by the user, as the temporary key to create the personalization data. the application cryptogram is generated based on the unpredictable data in addition to the key 120 and transaction counter (equivalent to generating the cryptogram using the unpredictable data and the temporary cryptographic key). Besides, on the basis that D3 has disclosed making transaction payments using a remote secure element, those skilled in the art will easily conceive sending keys related to the secure element from the

Mastercard, Ex1002, p. 861

remote to the mobile device.

(4) Hash is a common way of data encryption. On the basis that D2 has disclosed that the key 120 may be a DES key, a private key, a public key, some combination thereof, those skilled in the art will easily conceive using Hash for encryption.

In conclusion, the applicant's reasons are not persuasive.

For the abovementioned reasons, neither the independent claims nor the dependent claims of the present application possess inventiveness; meanwhile, the description does not possess any other patentable substantive contents. The present application does not have a prospect to be granted the patent right. If the applicant fails to provide weighty reasons within the time limit for making a response as prescribed in this Office Action, the present application will be rejected.

Mastercard, Ex1002, p. 862

100035
北京市西城区裨皮厂胡同2号国际商会大厦16层 中国专利代理（香港）有限公司
臧霁晨 刘春元

发文日：
2017年10月18日

申请号或专利号：201280053080.6　　发文序号：20171014003208 90

申请人或专利权人：易太普公司

发明创造名称：用于授权利用不可预期密码的交易的系统和方法

第三次审查意见通知书

1. ☒审查员已经收到申请人于2017年7月20日提交的意见陈述书，在此基础上审查员对上述专利申请继续进行实质审查。

☐根据国家知识产权局专利复审委员会于_____年_____月_____日作出的复审决定，审查员对上述专利申请继续进行实质审查。

☐_____

2. ☐经审查，申请人于　　提交的修改文件，不符合专利法实施细则第51条第3款的规定，不予接受。

3. 继续审查是针对下列申请文件进行的：

☐上述意见陈述书中所附的经修改的申请文件。

☒前次审查意见通知书所针对的申请文件以及上述意见陈述书中所附的经修改的申请文件替换文件。

☐前次审查意见通知书所针对的申请文件。

☐上述复审决定所确定的申请文件。

☐_____

4. ☒本通知书未引用新的对比文件。

☐本通知书引用下列对比文件（其编号续前，并在今后的审查过程中继续沿用）：

编号	文件号或名称	公开日期（或抵触申请的申请日）

5. 审查的结论性意见：

关于说明书：

☐申请的内容属于专利法第5条规定的不授予专利权的范围。

☐说明书不符合专利法第26条第3款的规定。

☐说明书的修改不符合专利法第33条的规定。

☐说明书的撰写不符合专利法实施细则第17条的规定。

☐_____

关于权利要求书：

☐权利要求_____不符合专利法第2条第2款的规定。

☐权利要求_____不符合专利法第9条第1款的规定。

纸件申请，回函请寄：100088 北京市海淀区蓟门桥西土城路6号 国家知识产权局专利局受理处收
电子申请，应当通过电子专利申请系统以电子文件形式提交相关文件。除另有规定外，以纸件等其他形式提交的文件视为未提交。

☐权利要求_____不具备专利法第 22 条第 2 款规定的新颖性。
☒权利要求 1-18 不具备专利法第 22 条第 3 款规定的创造性。
☐权利要求_____不具备专利法第 22 条第 4 款规定的实用性。
☐权利要求_____属于专利法第 25 条规定的不授予专利权的范围。
☐权利要求_____不符合专利法第 26 条第 4 款的规定。
☐权利要求_____不符合专利法第 31 条第 1 款的规定。
☐权利要求_____的修改不符合专利法第 33 条的规定。
☐权利要求_____不符合专利法实施细则第 19 条的规定。
☐权利要求_____不符合专利法实施细则第 20 条的规定。
☐权利要求_____不符合专利法实施细则第 21 条的规定。
☐权利要求_____不符合专利法实施细则第 22 条的规定。
☐_____

☐申请不符合专利法第 26 条第 5 款或者实施细则第 26 条的规定。
☐申请不符合专利法第 20 条第 1 款的规定。
☐分案申请不符合专利法实施细则第 43 条第 1 款的规定。
上述结论性意见的具体分析见本通知书的正文部分。
6.基于上述结论性意见，审查员认为：
☐申请人应当按照通知书正文部分提出的要求，对申请文件进行修改。
☐申请人应当在意见陈述书中论述其专利申请可以被授予专利权的理由，并对通知书正文部分中指出的不符合规定之处进行修改，否则将不能授予专利权。
☒专利申请中没有可以被授予专利权的实质性内容，如果申请人没有陈述理由或者陈述理由不充分，其申请将被驳回。
☐_____

7. 申请人应注意下列事项：

（1）根据专利法第 37 条的规定，申请人应当在收到本通知书之日起的 2 个月内陈述意见，如果申请人无正当理由逾期不答复，其申请将被视为撤回。

（2）申请人对其申请的修改应当符合专利法第 33 条的规定，不得超出原说明书和权利要求书记载的范围，同时申请人对专利申请文件进行的修改应当符合专利法实施细则第 51 条第 3 款的规定，按照本通知书的要求进行修改。

（3）申请人的意见陈述书和/或修改文本应当邮寄或递交国家知识产权局专利局受理处，凡未邮寄或递交给受理处的文件不具备法律效力。

（4）未经预约，申请人和/或代理人不得前来国家知识产权局与审查员举行会晤。

8. 本通知书正文部分共有 7 页，并附有下列附件：
☐引用的对比文件的复印件共_____份_____页。
☐

审查员：陈巧艳　　联系电话：028-62967620　　审查部门：专利审查协作四川中心电学发明审查部

Mastercard, Ex1002, p. 864

第三次审查意见通知书

申请号:2012800530806

申请人于2017年7月20日提交了意见陈述书和经过修改的申请文件，审查员在阅读了上述文件后，对本申请继续进行审查，现提出如下审查意见：

一、权利要求1-18不具备专利法第22条第3款所规定的创造性

1、权利要求1请求保护一种用于在销售点(POS)终端和移动设备之间针对数字凭证数据进行询问以便授权财务交易的方法，对比文件1公开了一种基于移动终端的安全金融交易，并具体公开了如下特征（参见说明书第[0021]-[0033]段）：支付服务器向移动终端发送一次性数字密钥（相当于在询问前，所述移动设备通过网络从远程应用程序系统请求交易缓存；在所述移动设备处接收交易缓存数据，所述交易缓存数据包含为制定对命令的响应所需的数据以及临时的使用密码的密钥）；销售终端将数量发送给移动终端，以获取相应的支付码等，将一次性数字密码输入数字生成算法以生成支付码（相当于在询问期间：根据卡规范执行销售点终端和移动设备之间的询问，根据卡规范通过通信信道将至少一个POS命令通信从销售点终端发送到移动设备，所述至少一个POS命令通信请求数字凭证数据，所述至少一个POS命令通信包括（a）密码请求；以及（b）不可预知数据）；移动终端将一次性数字密码输入数字生成算法以生成支付码，同时可结合随机数生成，并将支付码发送给销售终端（相当于所述移动设备使用所述临时的使用密码的密钥来生成密码，且制定包含使用所述临时的使用密码的密钥生成的密码以及来自POS终端的至少部分所述不可预知数据的响应）；移动终端向POS提交支付请求，支付请求包括支付码及数量（相当于通过所述通信信道将至少一个设备响应通信从移动设备发送到销售点终端，所述至少一个设备响应通信包括数字凭证数据的至少一部分，所述数字凭证数据包括所述响应，所述响应包括密码）；支付服务器鉴定支付码并向POS确认交易。

权利要求1所请求保护的技术方案与对比文件1所公开的内容相比，区别特征为：（1）从包括多个安全元件表示的远程应用程序系统请求用于特定安全元件的交易缓存，其中所述移动设备包括在能够被POS询问的所述移动设备的操作系统中运行的应用程序；其中所述应用程序不能访问所述数字凭证的永久的使用密码的密钥；该密钥与将在POS询问期间所使用的帐户相关联；从移动设备发送到销售点终端的所述响应包括帐户标识符；APDU命令和响应；（2）使用不可预知数据来生成不可预知密码；（3）更新或替换与所述帐户相关联的所述临时的使用密码的密钥以用于后续交易。基于上述区别特征，可以确定权利要求1实际解决的问题是：（1）如何基于安全元件进行交易；（2）如何生成密码；（3）如何进行后续交易。

对于区别特征（1），对比文件3（US 2010153721A1）公开了一种用于访问远程安全元件的方法，并具体公开了如下特征（参见说明书第[0006]-[0007]、[0029]-[0042]段）：安全元件（相

Mastercard, Ex1002, p. 865

当于HSM）被设置在远程安全元件服务器，虚拟安全元件模块被配置成与一个或更多个远程安全元件服务器进行通信，利用远程安全元件服务器和虚拟安全模块来建立安全业务（相当于包括多个安全元件表示的远程应用程序系统）；顾客可以通过简单地在销售点的读取器处晃动他们的便携式电子装置来付款（相当于其中所述移动设备包括在能够被POS询问的所述移动设备的操作系统中运行的应用程序）。上述特征在对比文件3中所起的作用与其在权利要求3中所起的作用相同，都是利用远程安全元件进行交易，也就是说，本领域技术人员能够获得启示，将对比文件3中利用远程安全元件的方法应用到对比文件1的支付交易过程中。此外，利用安全元件的永久密码生成支付密码，这是安全元件的常见处理方式，因此，在对比文件3公开了利用远程服务器存储安全元件进行支付的基础上，本领域技术人员容易想到远程存储安全元件对应的永久密码，并将安全元件的永久密码发送给移动设备，以生成支付密码，因此，在对比文件3公开了利用远程服务器存储安全元件进行支付的基础上，本领域技术人员容易想到远程存储安全元件对应的永久密码，并将安全元件的永久密码发送给移动设备，以生成支付密码，在对比文件1公开了支付服务器发送一次性密码的基础上，为了实现支付的安全性，本领域技术人员容易想到所述应用程序不能访问所述数字凭证的永久的使用密码的密钥，这是安全支付领域的常用技术手段。交易操作与账户有关，因此，该密钥与将在POS询问期间所使用的帐户相关联，从移动设备发送到销售点终端的所述响应包括帐户标识符，这都属于本领域技术人员容易想到的。此外，APDU命令是安全元件交易的常用数据交互方式，因此，其响应为APDU响应。

对于区别特征（2），对比文件2（CN 101048794A）公开了一种使用动态授权码授权交易的方法，并具体公开了如下特征（参见说明书第4页第1行-第第5页第28行、第8页第1行-第9页第19行）：不可预测数据包括交易额等，设备使用不可预测数据及其它保密数据来生成动态授权码（相当于使用不可预知数据来生成不可预知密码）。上述特征在对比文件2中所起的作用与其在权利要求1中所起的作用相同，都是利用不可预测数据生成不可预知密码，也就是说，本领域技术人员能够获得启示，将对比文件2中生成密码的方法应用到对比文件1的支付码生成过程中。

对于区别特征（3），对比文件1公开了（参见说明书第[0021]-[0033]段）：支付服务器自动发送下一个数字密钥到移动终端，并将其保存在移动终端以便下次交易使用，在此基础上，本领域技术人员容易想到，更新或替换与所述帐户相关联的所述临时的使用密码的密钥以用于后续交易，这属于本领域常用技术手段。

由此可知，在对比文件1的基础上结合对比文件2、对比文件3及本领域的常用技术手段得到权利要求1所要求保护的技术方案，对本领域的技术人员来说是显而易见的，因此权利要求1

Mastercard, Ex1002, p. 866

不具有突出的实质性特点和显著的进步，不具备专利法第 22 条第 3 款所规定的创造性。

2、权利要求 2-3 是权利要求 1 的从属权利要求，其附加技术特征被对比文件 2 公开（参见说明书第 4 页第 1 行-第第 5 页第 28 行、第 8 页第 1 行-第 9 页第 19 行）：不可预测的数据可以是随机数、可以基于当前时间、预测交易额的单项散列、上述的某些组合。因此，在其引用的权利要求不具备创造性的情况下，权利要求 2-3 不具备专利法第 22 条第 3 款所规定的创造性。

3、权利要求 4 是权利要求 1 的从属权利要求，其附加技术特征被对比文件 1 公开（参见说明书第[0021]-[0033]段）：支付服务器自动发送下一个数字密钥到移动终端，并将其保存在移动终端以便下次交易使用。因此，在其引用的权利要求不具备创造性的情况下，权利要求 4 不具备专利法第 22 条第 3 款所规定的创造性。

4、权利要求 5 是权利要求 4 的从属权利要求，其附加技术特征被对比文件 1 公开（参见说明书第[0021]-[0033]段）：支付服务器自动发送下一个数字密钥到移动终端，并将其保存在移动终端以便下次交易使用，移动终端基于一次性数字密钥生成相应的支付码。因此，在其引用的权利要求不具备创造性的情况下，权利要求 5 不具备专利法第 22 条第 3 款所规定的创造性。

5、权利要求 6 是权利要求 4 的从属权利要求，对比文件 3 公开了（参见说明书第[0006]-[0007]、[0029]-[0042]段）：便携式电子装置包括虚拟安全元件模块，虚拟安全元件模块被配置成与一个或更多个远程安全元件服务器进行通信，安全元件（相当于 HSM）被设置在远程安全元件服务器。对比文件 2 公开了（参见说明书第 4 页第 1 行-第第 5 页第 28 行、第 8 页第 1 行-第 9 页第 19 行）：用户将输入到他或她的移动处理设备中去的不可预测的数据，该数据随后被用于（典型地与诸如加密密钥之类的其它数据一起）生成动态认证码。在此基础上，当利用对比文件 3 中的安全元件进行交易时，本领域技术人员容易想到利用不可预测的数据临时创建密钥，并与安全元件关联，这是利用安全元件进行交易时的常用技术手段。因此，在其引用的权利要求不具备创造性的情况下，权利要求 6 不具备专利法第 22 条第 3 款所规定的创造性。

6、权利要求 7 是权利要求 1 的从属权利要求，对比文件 2 公开了（参见说明书第 4 页第 1 行-第第 5 页第 28 行、第 8 页第 1 行-第 9 页第 19 行）：移动处理设备使用密钥生成动态认证码，密钥可以是 DES 密钥，密钥可以保存在受保护的存储器中（相当于其中使用所述使用密码的密钥生成所述密码包括按照数字加密标准计算使用所述本地存储的使用密码的密钥来加密所述输入的组以生成输出）。上述技术特征被对比文件 2 公开，且其在对比文件 2 中所起作用与其在本申请权利要求 7 中所起作用相同，均是使用所述使用密码的密钥生成所述密码包括按照数字加密标准计算使用所述本地存储的使用密码的密钥来加密所述输入的组以生成输出，也即对比文件 2 给出了将上述技术特征应用于对比文件 1 以解决其技术问题的启示。密码包括输出的一部

Mastercard, Ex1002, p. 867

分是进行加密信息输出时的常见方式。因此，在其引用的权利要求不具备创造性的情况下，权利要求 7 不具备专利法第 22 条第 3 款所规定的创造性。

7、权利要求 8 是权利要求 1 的从属权利要求，由于实际交易过程中，安全元件主要用于生成交易相关的密码，因此在交易询问期间不联系远程应用程序系统，这是本领域的常用技术手段。因此，在其引用的权利要求不具备创造性的情况下，权利要求 8 不具备专利法第 22 条第 3 款所规定的创造性。

8、权利要求 9 是权利要求 1 的从属权利要求，对比文件 1 公开了（参见说明书第[0021]-[0033]段）：POS 终端可以将数量直接发送给支付服务器，并传送支付码，支付服务器分解支付码，比较一次性数字密码及随机数，验证其正确性，验证通过后，向 POS 确认交易（相当于从所述销售点终端接收授权请求，所述授权请求包括所述密码；由所述系统验证所述响应密码的正确性，其中将所接收的密码进行比较；以及从所述系统向所述销售点发送授权响应，其中至少部分地通过验证所接收的密码的正确性来确定包含在所述授权响应中的数据）。对比文件 2 公开了（参见说明书第 4 页第 1 行-第第 5 页第 28 行、第 8 页第 1 行-第 9 页第 19 行）：授权过程可能需要使用与移动设备所执行的相同的数据和算法在授权端计算动态认证码，并将计算的结果与接收到的动态码作比较以确定计算的结果与接收到的码相匹配（相当于其中将所接收的密码与密码计算的结果进行比较，所述结果基于与交易相关联的所述临时的使用密码的密钥而生成）。上述技术特征被对比文件 2 公开，且其在对比文件 2 中所起作用与其在本申请权利要求 9 中所起作用相同，均是将所接收的密码与密码计算的结果进行比较，所述结果基于与交易相关联的所述临时的使用密码的密钥而生成，也即对比文件 2 给出了将上述技术特征应用于对比文件 1 以解决其技术问题的启示。因此，在其引用的权利要求不具备创造性的情况下，权利要求 9 不具备专利法第 22 条第 3 款所规定的创造性。

9、权利要求 10 是权利要求 9 的从属权利要求，其附加技术特征被对比文件 2 公开（参见说明书第 4 页第 1 行-第第 5 页第 28 行、第 8 页第 1 行-第 9 页第 19 行）：不可预测数据包括交易额等，设备使用不可预测数据及其它保密数据来生成动态授权码，授权过程可能需要使用与移动设备所执行的相同的数据和算法在授权端计算动态认证码，并将计算的结果与接收到的动态码作比较以确定计算的结果与接收到的码相匹配。因此，在其引用的权利要求不具备创造性的情况下，权利要求 10 不具备专利法第 22 条第 3 款所规定的创造性。

10、权利要求 11 是权利要 10 的从属权利要求，在交易授权过程中，发送交易的值是本领域的常用技术手段，ISO8583 是常用的数据格式。因此，在其引用的权利要求不具备创造性的情况下，权利要求 11 不具备专利法第 22 条第 3 款所规定的创造性。

Mastercard, Ex1002, p. 868

11、权利要求 12 是权利要求 1 的从属权利要求，对比文件 1 公开了（参见说明书第[0021]-[0033]段）：POS 终端可以将数量直接发送给支付服务器，并传送支付码，移动终端将数量等发送给支付服务器，支付服务器分解支付码，比较一次性数字密码及随机数，验证其正确性，验证通过后，向 POS 确认交易。在对比文件 1 公开了销售点终端及移动终端都能发送不可预知数据的基础上，为了避免数据被篡改，本领域技术人员容易想到在服务器端比较两数据是否相同，这是信息验证领域的常用技术手段。因此，在其引用的权利要求不具备创造性的情况下，权利要求 12 不具备专利法第 22 条第 3 款所规定的创造性。

12、权利要求 13 是权利要求 12 的从属权利要求，对比文件 1 公开了（参见说明书第[0021]-[0033]段）：将交易数量发送到支付服务器。对比文件 2 公开了（参见说明书第 4 页第 1 行-第第 5 页第 28 行、第 8 页第 1 行-第 9 页第 19 行）：该认证码输出设备可将生成的动态认证码呈现给用户，诸如通过 LCD 屏幕或其它显示器，并将其随后发送至受权端。在此基础上，当对交易数据进行验证时，本领域技术人员容易想到将其显示到移动设备的显示器，此外，验证交易量数据是交易验证时的常用技术手段。因此，在其引用的权利要求不具备创造性的情况下，权利要求 13 不具备专利法第 22 条第 3 款所规定的创造性。

13、权利要求 14 是权利要求 1 的从属权利要求，其附加技术特征被对比文件 1 公开（参见说明书第[0021]-[0033]段）：移动终端将交易数量发送到支付服务器。因此，在其引用的权利要求不具备创造性的情况下，权利要求 14 不具备专利法第 22 条第 3 款所规定的创造性。

14、权利要求 15 是权利要求 1 的从属权利要求，然而，ISO7816-4 数据协议是常用的数据通信协议，因此，POS 命令通信及设备响应通信遵守 ISO7816-4 数据协议是数据通信领域的常用技术手段。因此，在其引用的权利要求不具备创造性的情况下，权利要求 15 不具备专利法第 22 条第 3 款所规定的创造性。

15、权利要求 16 是权利要求 1 的从属权利要求，其附加技术特征被对比文件 1 公开（参见说明书第[0021]-[0033]段）：支付可以采用近场通信。因此，在其引用的权利要求不具备创造性的情况下，权利要求 16 不具备专利法第 22 条第 3 款所规定的创造性。

16、权利要求 17 是权利要求 1 的从属权利要求，其附加技术特征被对比文件 1 公开（参见说明书第[0021]-[0033]段）：移动终端保存一次性数字密码以便下次交易使用，基于一次性数字密码生成支付码。因此，在其引用的权利要求不具备创造性的情况下，权利要求 17 不具备专利法第 22 条第 3 款所规定的创造性。

17、权利要求 18 是权利要求 1 的从属权利要求，哈希是常用的数据加密方式。因此，在其引用的权利要求不具备创造性的情况下，权利要求 18 不具备专利法第 22 条第 3 款所规定的创

Mastercard, Ex1002, p. 869

造性。

二、针对申请人意见陈述的答复

申请人认为：（1）尽管对比文件 1 确实提到“密钥”，但其不是使用密码的密钥，并且也不是用于生成密码；“支付号码”不是密码；（2）对比文件 1 未公开：在询问前：“通过网络从包括多个安全元件表示的远程应用程序系统请求用于特定安全元件的交易缓存，并且，在移动设备处接收交易缓存数据，所述交易缓存数据包含响应于 APDU 命令制定 APDU 所需的数据，以及临时的使用密码的密钥，其与将在 POS 询问期间所使用的帐户相关联……”以及在询问期间：“使用所述不可预知数据和所述临时的使用密码的密钥来生成不可预期密码，且制定包含使用所述临时的使用密码的密钥生成的不可预期密码以及来自 POS 终端的至少部分所述不可预知数据的响应 APDU；通过所述通信信道将至少一个设备响应通信从移动设备发送到销售点终端，所述至少一个设备响应通信包括帐户标识符和包含所述不可预期密码的所述响应 APDU”，因此，对比文件 1 并没有教导所要求保护的发明；（3）对比文件 3 既没有教导交易缓存也没有教导临时的使用密码的密钥；（4）权利要求 18 记载了密码是哈希。

审查员认为：（1）对比文件 1 公开了（参见说明书第[0021]-[0033]段）：支付码包括一次性数字密钥及随机数，一次性数字密钥从支付服务器自动发送到移动终端，一次性数字密钥能通过与随机数相乘等方式计算得到支付码。由此可知，对比文件 1 与本申请一样，都是通过一次性数字密钥（相当于密钥）生成支付码（相当于密码）。且对比文件 3 中给出了利用远程安全元件进行交易支付的启示，而在安全元件进行安全交易的过程中，利用永久的密钥生成密码以授权交易，这是本领域的常用技术手段，例如对比文件 2 中公开了：移动设备上的软件生成电路具有典型智能卡几乎全部的功能（相当于安全元件）；移动处理设备使用（诸如加密密钥之类的）密钥 120 来生成动态认证码 130，密钥 120 可以是 DES 密钥、私钥、公钥、上述的某些组合、或者用于加密或生成用于后续认证的保密消息的任何其它数据。

（2）参见权利要求 1 的评述，上述区别特征部分被对比文件 1、2、3 公开，其余部分为在对比文件 1、2、3 公开的内容基础上，本领域技术人员容易想到的，属于本领域常用技术手段。

（3）对比文件 1 公开了：一次性数字密钥（相当于临时使用的密钥）；对比文件 2 公开了：加密密钥或密钥对中的一个或多个密钥通过使用之前由用户输入的 PIN 和移动设备标识符来加密（如通过三重 DES 技术）作为临时密钥以生成个人化数据，除密钥 120 和交易计数器以外还基于该不可预测数据来生成应用密文（相当于使用所述不可预知数据和所述临时的使用密码的密钥来产生密码）；此外，在对比文件 3 公开了利用远程安全元件进行交易支付的基础上，本领域技术人员容易想到将安全元件相关的密钥等由远程发送到移动设备。

Mastercard, Ex1002, p. 870

（4）哈希是常见的数据加密方式，在对比文件2公开了密钥120可以是DES密钥、私钥、公钥、上述的某些组合的基础上，本领域技术人员容易想到利用哈希进行加密。

综上，申请人陈述的理由不具有说服力。

基于上述理由，本申请的独立权利要求以及从属权利要求都不具备创造性，同时说明书中也没有记载其他任何可以授予专利权的实质性内容，本申请也不具备被授予专利权的前景。如果申请人不能在本通知书规定的答复期限内提出充分的理由，本申请将被驳回。

审查员姓名：陈巧艳　　审查员代码：638962

Mastercard, Ex1002, p. 871

Electronic Patent Application Fee Transmittal

Application Number:	13599647
Filing Date:	30-Aug-2012
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Filer:	John L. Adair/Margarita Marquez
Attorney Docket Number:	STAPP1100-5

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION INFORMATION DISCLOSURE STMT	2806	1	120	120
		Total in USD ($)		**120**

Electronic Acknowledgement Receipt	
EFS ID:	31654894
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Customer Number:	44654
Filer:	John L. Adair/Margarita Marquez
Filer Authorized By:	John L. Adair
Attorney Docket Number:	STAPP1100-5
Receipt Date:	31-JAN-2018
Filing Date:	30-AUG-2012
Time Stamp:	09:54:58
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$120
RAM confirmation Number	013118INTEFSW00008063503183
Deposit Account	503183
Authorized User	Margarita Marquez
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		STAPP1100-5_IDS_01-31-2018.pdf	89271 0eee708a6d1ed3ded611319e8bf3ea7435f5171f	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	2
	Information Disclosure Statement (IDS) Form (SB08)	3	3

Warnings:					
Information:					
2	Non Patent Literature	STAPP1100_Ref_C21.pdf	852494 b95455bde1ea013cb8412fcfcacf5d6d0ee69f4	no	19
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30704 a4dfb5ac1edf15da71c97c4d5de5494bea2e9a4955	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	972469		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. (Opt.) **STAPP1100-5**

First Named Inventor **C. Douglas Yeager**	
Application Number **13/599,647**	Date Filed **August 30, 2012**
Title **SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE (as amended)**	
Group Art Unit **3695**	Examiner **Asha Puttaiah**
Confirmation Number **1919**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATION OF TRANSMISSION UNDER 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on January 31, 2018.

M. Marquez
Margarita Marquez

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. A copy of foreign patent documents as well as the information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

☐ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☐ This Information Disclosure Statement is being submitted before the mailing of a first Office action on the merits; or

Pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application.

Applicant does not believe any fees are due and owing at this time. If Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

SPRINKLE IP LAW GROUP
Attorneys for Applicant

/John L. Adair/

John L. Adair
Reg. No. 48,828

Dated: January 25, 2018

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 371-9088

INFORMATION DISCLOSURE STATEMENT				Application Number	13/599,647
				Filing or 371 (c) Date:	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	~~Puttaiah, Asha~~ Prinslow, Garrison
Sheet	1	of	1	Attorney Docket Number	STAPP1100-5

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C20	Examination Report issued for Malaysian Patent Application No. PI2014000569, mailed October 13, 2017, 3 pages.	

Examiner Signature	/GARRISON PRINSLOW/	Date Considered	02/08/2018	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /G.P./

INFORMATION DISCLOSURE STATEMENT				Application Number	13/599,647
				Filing or 371 (c) Date:	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	Puttalah, Asha Prinslow, Garrison
Sheet	1	of	1	Attorney Docket Number	STAPP1100-5

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C18	Examination Report issued for European Patent Application No. 12 827 026.1, mailed June 23, 2017, 9 pages.	
	C19	Examiner's Report issued for Canadian Patent Application No. 2,846,462, mailed August 1, 2017, 5 pages.	

Examiner Signature	/GARRISON PRINSLOW/	Date Considered	02/08/2018	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /G.P./

2010 IEEE Symposium on Security and Privacy

Chip and PIN is Broken

Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond
University of Cambridge
Computer Laboratory
Cambridge, UK
http://www.cl.cam.ac.uk/users/{sjm217,sd410,rja14,mkb23}

***Abstract*—EMV is the dominant protocol used for smart card payments worldwide, with over 730 million cards in circulation. Known to bank customers as "Chip and PIN", it is used in Europe; it is being introduced in Canada; and there is pressure from banks to introduce it in the USA too. EMV secures credit and debit card transactions by authenticating both the card and the customer presenting it through a combination of cryptographic authentication codes, digital signatures, and the entry of a PIN. In this paper we describe and demonstrate a protocol flaw which allows criminals to use a genuine card to make a payment without knowing the card's PIN, and to remain undetected even when the merchant has an online connection to the banking network. The fraudster performs a man-in-the-middle attack to trick the terminal into believing the PIN verified correctly, while telling the card that no PIN was entered at all. The paper considers how the flaws arose, why they remained unknown despite EMV's wide deployment for the best part of a decade, and how they might be fixed. Because we have found and validated a practical attack against the core functionality of EMV, we conclude that the protocol is broken. This failure is significant in the field of protocol design, and also has important public policy implications, in light of growing reports of fraud on stolen EMV cards. Frequently, banks deny such fraud victims a refund, asserting that a card cannot be used without the correct PIN, and concluding that the customer must be grossly negligent or lying. Our attack can explain a number of these cases, and exposes the need for further research to bridge the gap between the theoretical and practical security of bank payment systems. It also demonstrates the need for the next version of EMV to be engineered properly.**

***Keywords*-EMV; Chip and PIN; card fraud; bank security; protocol failure; security economics; authentication**

I. Introduction

Smart cards have gradually replaced magnetic strip cards for point-of-sale and ATM transactions in many countries. The leading system, EMV [1], [2], [3], [4] (named after Europay, MasterCard, and Visa), has been deployed throughout most of Europe, and is currently being rolled out in Canada. As of early 2008, there were over 730 million EMV-compliant smart cards in circulation worldwide [5]. In EMV, customers authorize a credit or debit card transaction by inserting their card and entering a PIN into a point-of-sale terminal; the PIN is typically verified by the smart card chip, which is in turn authenticated to the terminal by a digital certificate. The transaction details are also authenticated by a cryptographic message authentication code (MAC), using a symmetric key shared between the payment card and the bank that issued the card to the customer (the issuer).

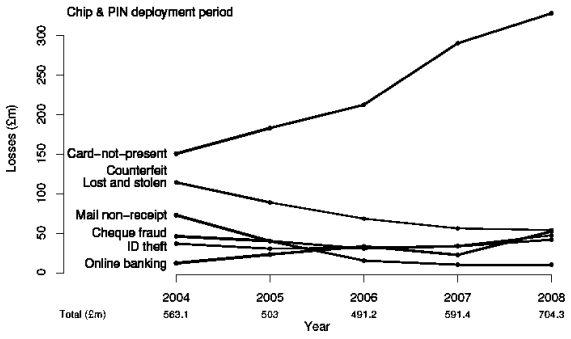


Figure 1. Fraud statistics on UK-issued cards [6]

EMV was heavily promoted under the "Chip and PIN" brand during its national rollout in the UK. The technology was advertised as a solution to increasing card fraud: a chip to prevent card counterfeiting, and a PIN to prevent abuse of stolen cards. Since its introduction in the UK the fraud landscape has changed significantly: lost and stolen card fraud is down, and counterfeit card fraud experienced a two year lull. But no type of fraud has been eliminated, and the overall fraud levels have actually risen (see Figure 1). The likely explanation for this is that EMV has simply moved fraud, not eliminated it.

One goal of EMV was to externalise the costs of dispute from the issuing bank, in that if a disputed transaction has been authorised by a manuscript signature, it would be charged to the merchant, while if it had been authorised by a PIN then it would be charged to the customer. The net effect is that the banking industry, which was responsible for the design of the system, carries less liability for the fraud. The industry describes this as a 'liability shift'.

Security economics teaches us that such arrangements create "moral hazard," by insulating banks from the risk of their poor system design, so it is no surprise when such plans go awry. Several papers have documented technical attacks on EMV. However, it is now so deeply entrenched that changes can be very hard to make. Fundamental pro-

1081-6011/10 $26.00 © 2010 IEEE
DOI 10.1109/SP.2010.33

IEEE computer society

Mastercard, Ex1002, p. 881

tocol changes may now require mutual agreement between banks, merchants, point-of-sale hardware manufacturers, and international card schemes (Visa, MasterCard, and American Express), all of which lobby hard to protect their interests. As with the Internet communications protocols, we are stuck with suboptimal design decisions made a decade ago. So few system changes have been made, and meanwhile the volume of customer complaints about disputed transactions continues to rise. A June 2009 survey revealed that one in five UK victims of fraud are left out of pocket [7].

In the past few years, the UK media have reported numerous cases where cardholders' complaints have been rejected by their bank and by government-approved mediators such as the Financial Ombudsman Service, using stock excuses such as 'Your card was CHIP read and a PIN was used so you must have been negligent.' Interestingly, an increasing number of complaints from believable witnesses indicate that their EMV cards were fraudulently used shortly after being stolen, despite there having been no possibility that the thief could have learned the PIN.

In this paper, we describe a potential explanation. We have demonstrated how criminals can use stolen "Chip and PIN" (EMV) smart cards without knowing the PIN. Since "verified by PIN" – the essence of the system – does not work, we declare the Chip and PIN system to be broken.

II. Protocol Failure

EMV is both a protocol suite and a proprietary protocol framework: a general toolkit from which protocols can be built. In practice, it works as follows. A bank that issues EMV cards selects a subset of the EMV protocols, choosing for instance between digital signature methods, selecting a MAC algorithm, and deciding on hundreds of customisable options regarding authentication and risk management. Their selection must comply with card scheme rules as well as the EMV framework. Meanwhile merchants and acquiring banks (who receive payments on behalf of merchants) simply procure EMV-compliant hardware and software and connect it to the payment networks (operated by card schemes).

Since we cannot enumerate the many possible protocols, we mainly describe the protocol as it is deployed within the UK. However, it is implemented similarly in many other countries. In particular, the attack we introduce in this paper results both from a protocol failure of the EMV framework, and a failure of the proprietary MAC protocols that are used by issuing banks (and approved by the card schemes).

As Figure 2 shows in detail, the EMV protocol can be split into three phases:

Card authentication:
: Assures the terminal which bank issued the card, and that the card data have not been altered

Cardholder verification:
: Assures the terminal that the PIN entered by the customer matches the one for this card

Transaction authorization:
: Assures the terminal that the bank which issued the card authorizes the transaction

1) Card authentication: EMV smart cards may contain multiple separate applications with different cryptographic keys, such as a debit or credit card for use at shops, ATM functionality, and MasterCard Chip Authentication Programme (CAP) applications for online banking. Thus when a card is inserted into a point of sale terminal, the terminal first requests a list of supported applications (by reading the file "1PAY.SYS.DDF01") and selects one of them. The actual transaction is then initiated by sending the Get Processing Options command to the card.

Next, the terminal reads cardholder information from the card by sending a Read Record command with the appropriate file identifiers. These records include card details (e.g. primary account number, start and expiry date), backwards compatibility data (e.g. a copy of the magnetic strip), and control parameters for the protocol (e.g. the cardholder verification method list, and card data object lists, which will be discussed later).

The records also include an RSA digital signature over a subset of the records, together with a certificate chain linking the signing key to a card scheme root key known to the terminal. In one variant of EMV, known as SDA (static data authentication), the card itself is not capable of performing RSA operations, so it can only present the terminal with a static certificate. Cards employing the DDA (dynamic data authentication) variant additionally contain RSA private keys which are used to sign a nonce sent by the terminal and whose corresponding public keys are authenticated by the certificate chain.

SDA cards (which prior to 2009 all UK banks issued) are vulnerable to a trivial and well-known replay attack in which the certificate is read from a card and written to a counterfeit one (these are often called "yes cards" because they will respond "yes" to a PIN verification request, no matter what PIN is entered). The card is then used at a point-of-sale terminal which has no online connection to the banking network, and because there is no real-time interaction, the MAC produced during transaction authorization cannot be checked before the goods are handed over.

However, the vast majority of UK point-of-sale terminals maintain a permanent online connection, so yes cards could normally be detected[1]. Since 2009, some UK banks have started issuing DDA cards, which resist counterfeiting even in offline transactions, by giving the cards the capability to sign a terminal-provided nonce under an asymmetric key. However the attack presented in this paper does not rely on the yes card attack; it is entirely independent of card authentication, whether by SDA or DDA.

[1]There are viable criminal attack scenarios involving yes cards, and criminal business models, but these are beyond the scope of this paper.

Mastercard, Ex1002, p. 882

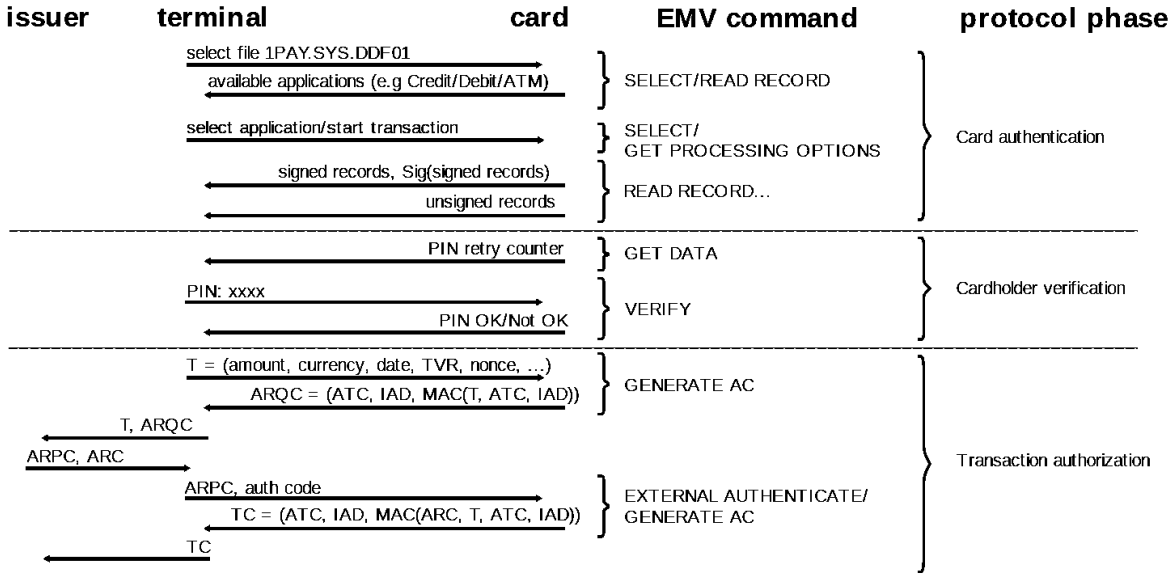


Figure 2. A complete run of a Chip and PIN protocol.

2) Cardholder verification: The cardholder verification step starts with a mechanism negotiation, performed between the card and the terminal, to establish what cardholder authentication method they can (or must) use. This is driven by a data element called the cardholder verification method (CVM) list. The CVM list states the card's policy on when to use a PIN, or a signature, or nothing at all, to authenticate the cardholder.

Protocols for negotiating an authentication mechanism are notoriously hard to get right. EMV specifies a complex negotiation algorithm by which the terminal can decide the appropriate method depending on the value of the transaction, its type (e.g. cash, purchase), and the terminal's capabilities. The CVM list also specifies what action should be taken if cardholder verification fails, i.e., whether the next method should be tried or the transaction rejected.

In practice, however, only a small subset of these capabilities is used. UK cards we have examined specify, in descending order of preference, *PIN verification*, *signature verification*, and *no verification*. A terminal may skip an option of which it is not capable; for example, unattended terminals cannot do signature verification, and some vending machines are not equipped with PIN entry devices/keypads. There may also be scope for operator discretion. For example, the card may permit the terminal to attempt signature verification if PIN verification fails, but in practice merchants will normally reject such a transaction. In the UK there also exists a type of card known as a "Chip & Signature" card, which does not support PIN verification at all. These cards are issued to customers who request them, normally because they are unable to remember a PIN or are visually impaired. Some customers also request such cards because they are concerned about the additional liability that PIN-based transactions would place on them.

However, the vast majority of transactions are 'PIN verified', which means the customer enters the PIN on a PIN entry device. The PIN is sent to the card, and the card compares it to the PIN it stores. If they match, the card returns `0x9000`, and if it fails the card returns `0x63C`x, where x is the number of further PIN verification attempts the card will permit before locking up. Note that the card's response is not directly authenticated.

ATM cardholder verification works differently, and uses a method known as "online PIN", as opposed to "offline PIN" described above. Here, the PIN is encrypted by the ATM, and sent to the issuer over a payment network. The issuer then verifies the PIN centrally, and sends the result back to the ATM. The attack we present in this paper only applies to offline PIN cardholder verification.

We have observed variations between countries. While cards from Belgium and Estonia work like British cards, we have tested cards from Switzerland and Germany whose CVM lists specify either chip and signature or online PIN, at least while used abroad. The attack described here is not applicable to them. However, because UK point-of-sale terminals do not support online PIN, a stolen card of such a type could easily be used in the UK, by forging the cardholder's signature.

Mastercard, Ex1002, p. 883

3) Transaction authorization: In the third step, the terminal asks the card to generate a cryptographic MAC over the transaction details, to be sent to the issuing bank. The terminal calls the Generate AC command, to request an ARQC (authorization request cryptogram) from the card. The payload of this command is a description of the transaction, created by concatenating data elements specified by the card in the CDOL 1 (card data object list 1). Typically this includes details like the transaction amount, currency, type, a nonce generated by the terminal, and the TVR (terminal verification results), which will be discussed later.

The cryptogram sent to the bank includes a type code, a sequence counter identifying the transaction (ATC – application transaction counter), a variable length field containing data generated by the card (IAD – issuer application data), and a message authentication code (MAC), which is calculated over the rest of the message including a description of the transaction. The MAC is computed, typically using 3DES, with a symmetric key shared between the card and the issuing bank.

If the card permits the transaction, it returns an ARQC; otherwise, it returns an AAC (application authentication cryptogram) which aborts the transaction. The ARQC is then sent by the terminal to the issuing bank, via the acquirer and payment network. The issuer will then perform various cryptographic, anti-fraud and financial checks: such as whether the card has been listed as stolen, whether there are adequate funds, and whether the risk analysis algorithm considers the transaction acceptable. If the checks pass, the issuer returns a two byte ARC (authorization response code), indicating how the transaction should proceed, and the ARPC (authorization response cryptogram), which is typically a MAC over ARQC $\oplus$ ARC. Both items are forwarded by the terminal to the card with the External Authenticate command.

The card validates the MAC contained within the ARPC, and if successful updates its internal state to note that the issuer authorized the transaction. The terminal then calls Generate AC again, but now using the CDOL 2, requesting that the card issues a TC (transaction certificate) cryptogram, signifying that it is authorizing the transaction to proceed. Finally, the terminal sends the TC to the issuer, and stores a copy in its own records in case there is a dispute. At this point it will typically print a receipt, which may contain the legend 'Verified by PIN' if the response to Verify indicated success. One copy of the receipt is given to the cardholder and a second copy is retained. We have also seen different receipts with 'confirmed' for the cardholder and 'PIN verified' on the merchant copy (perhaps to assure the merchant that the liability for disputes is no longer on them).

The above description assumes that the terminal chose to perform an online transaction and contacted the issuer. In the event of an offline transaction, the terminal requests that the card return TC on the first call to Generate AC. The card may then either decide to accept the transaction offline by returning a TC, force the transaction online by returning an ARQC, or reject the transaction entirely by returning an AAC. Our attack applies just as well to the offline case.

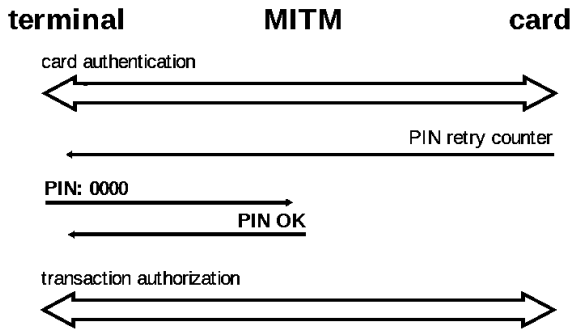


Figure 3. The man-in-the-middle suppresses the PIN Verify command to the card, and tells the terminal that the PIN has been verified correctly. A complete transaction is detailed in Appendix A.

Table I
TERMINAL VERIFICATION RESULTS (TVR) BYTE 3.

Bit	Meaning when bit is set
8	Cardholder verification was not successful
7	Unrecognized CVM
6	PIN Try Limit exceeded
5	PIN entry required and PIN pad not present or not working
4	PIN entry required, PIN pad present, but PIN was not entered
3	Online PIN entered
2	Reserved for future use
1	Reserved for future use

III. The Attack

The central flaw in the protocol is that the PIN verification step is never explicitly authenticated. Whilst the authenticated data sent to the bank contains two fields which incorporate information about the result of the cardholder verification – the Terminal Verification Results (TVR) and the Issuer Application Data (IAD), they do not together provide an unambiguous encoding of the events which took place during the protocol run. The TVR mainly enumerates various possible failure conditions for the authentication, and in the event of success does not indicate *which particular method was used* (see Table I).

Therefore a man-in-the-middle device, which can intercept and modify the communications between card and terminal, can trick the terminal into believing that PIN verification succeeded by responding with `0x9000` to Verify, without actually sending the PIN to the card. A dummy PIN must be entered, but the attack allows any PIN to be accepted. The card will then believe that the terminal did not support PIN verification, and has either skipped cardholder

Mastercard, Ex1002, p. 884

Table II
IAD FORMAT, BYTE 5 (BITS 4–1) FROM A VISA VERSION 10 CRYPTOGRAM [8, APPENDIX A-13, P222].

Bit	Meaning when bit is set
4	Issuer Authentication performed and failed
3	Offline PIN performed
2	Offline PIN verification failed
1	Unable to go online

verification or used a signature instead. Because the dummy PIN never gets to the card, the PIN retry counter is not altered. The modified protocol flow is shown in Figure 3.

Neither the card nor terminal will spot this subterfuge because the cardholder verification byte of the TVR is only set if PIN verification has been attempted *and* failed. The terminal believes that PIN verification succeeded (and so generates a zero byte), and the card believes it was not attempted (so will accept the zero byte).

The IAD (Table II) does often indicate whether PIN verification was attempted. However, it is in an issuer-specific proprietary format, and not specified in EMV. Therefore the terminal, which knows the cardholder verification method chosen, cannot decode it. The issuer, which can decode the IAD, does not know which cardholder verification method was used, and so cannot use it to prevent the attack. Because of the ambiguity in the TVR encoding, neither party can identify the inconsistency between the cardholder verification methods they each believe were used. The issuer will thus believe that the terminal was incapable of soliciting a PIN – an entirely plausible yet inaccurate conclusion.

For offline transactions, the issuer will not be contacted until after the transaction has been completed, so has even less ability to detect the attack. Some cards may refuse to authorize an offline transaction without having successfully verified the PIN. This however is no obstacle to the attack, because the man-in-the-middle can simply change the cryptogram type field in the response to the Generate AC call, turning an ARQC or AAC into a TC. This modification will possibly cause the cryptogram verification to fail, but this would only be detected after the cardholder has left with the goods.

In the UK, PIN-based cardholder verification is mandatory and all cards support offline PIN verification. Although the CVM list permits merchants to fall back to signature, they rarely offer this (they become liable for fraud if they do). Therefore, unless a thief can somehow discover the PIN, using a stolen card is difficult. Here, our attack could be used by criminals to carry out a point-of-sale transaction.

In fact, the authors are regularly contacted by bank customers who have had fraudulent transactions carried out shortly after their card has been stolen, and who state that they did not write down their PIN, but found that their bank accused them of negligence and refused to refund the losses. The attack we describe in this paper may explain some of these cases.

IV. ATTACK DEMONSTRATION

We successfully executed the attack using several different Chip and PIN cards at a live terminal. The schematic and a photograph of the equipment used is shown in Figure 4. Stills from a video of us carrying this attack out are in Figure 5; a film by BBC Newsnight of us carrying out the attack is also available [9]. The hardware for the attack was made of cheap off-the-shelf components and required only elementary programming and engineering skills.

The man-in-the-middle circuit connects to the terminal through a fake card. This card has thin wires embedded in the plastic substrate, which connect the card's contact pads to an interface chip ($2 Maxim 1740 [10]) for voltage level-shifting. This is connected to a general-purpose FPGA board ($189 Spartan-3E Starter Kit [11]) that drives the card and converts between the card and PC interfaces. Through a serial link, the FPGA is connected to a laptop, which is in turn connected to a standard smart card reader from Alcor Micro ($8) into which the genuine card is inserted. A Python script running on the laptop relays the transaction while waiting for the Verify command being sent by the terminal; it then suppresses it to the card, and responds with `0x9000`:

```
if VERIFY_PRE and command[0:4] == "0020":
    debug("Spoofing VERIFY response")
    return binascii.a2b_hex("9000")
```

The rest of the communication is unaltered.

Where the merchant colludes with the attacker for a cut of the profit, the hardware bulk is not a factor. When the merchant is unwitting, the security measures introduced to protect the customer from a corrupt merchant skimming the magnetic strip work in the attackers' favour. Cardholders are instructed not to hand their card to the merchant, and the merchant is under social pressure to look away during a transaction while the cardholder enters their PIN. The attack could easily be miniaturized: it can be ported to smaller hardware devices, and would not require a PC at all if the FPGA or microcontroller is programmed to parse the transaction and interface with the card. Miniaturized hardware could be entirely hidden in a coat sleeve and used immediately after the card is stolen.

Finally, we can envision a carrier card that hosts a cutout of the original card, which interfaces with a microcontroller that communicates with the terminal. This way, the attack is entirely encapsulated in a card form factor and can be moderately industrialized. Miniturized "shims" with an embedded microcontroller have already been created for SIM cards for unlocking phones from a particular network [12]; the simple code required for our attack can be ported to

Mastercard, Ex1002, p. 885

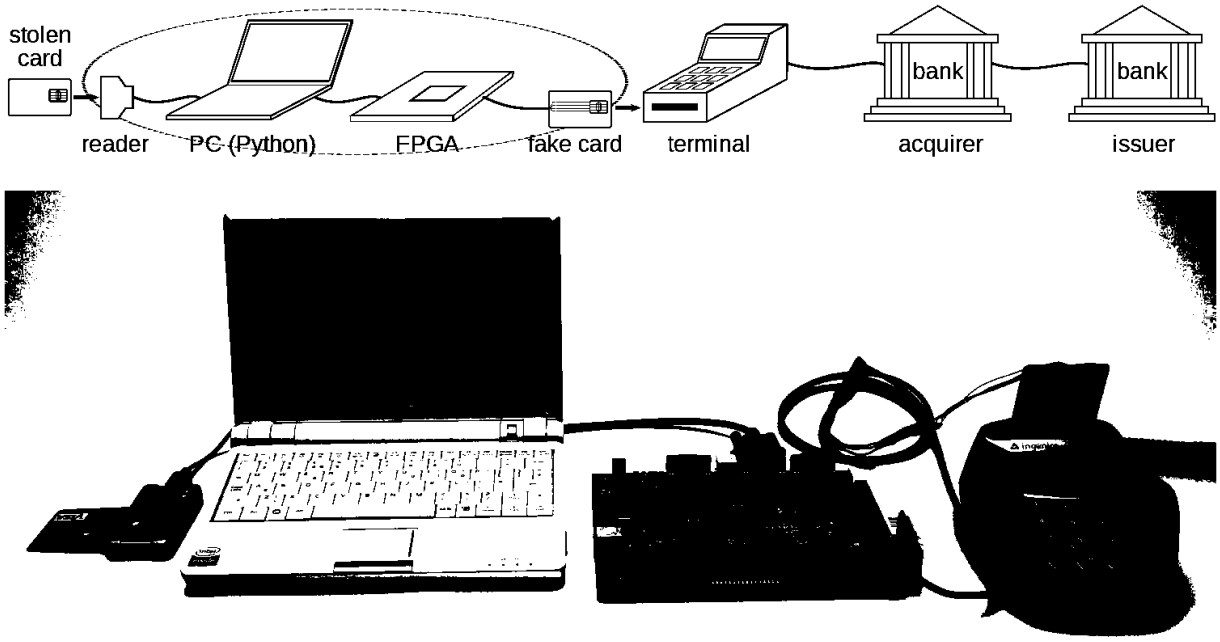


Figure 4. Components of the attack.

run on a similar device. Miniaturization is mostly a mechanical challenge, and well within the expertise of criminal gangs: such expertise has already been demonstrated in the miniaturised transaction interceptors that have been used to sabotage point of sale terminals and skim magnetic strip data. Miniaturization is not critical, though, as criminals can target businesses where a card can be used with wires running up the cashout operative's sleeve, while a laptop and FPGA board can be hidden easily in his backpack. There are firms such as supermarkets and money changers whose terminals are located on the other side of a barrier from the checkout staff, who therefore do not scrutinise the cards their customers use.

V. Causes

The failure we identify here might be patched in various ways which we will discuss later. But at heart there is a protocol design error in EMV: it compartmentalises the issuer-specific MAC protocol too distinctly from the negotiation of the cardholder verification method. Both of the parties who rely on transaction authentication – the merchant and the issuing bank – need to have a full and trustworthy view of the method used to verify the cardholder; and because the relevant data cannot be collected neatly by either party, the framework itself is flawed.

A key misconception of the designers was to think of the TVR and card verification results primarily as separate lists of possible failures represented by a bit mask, rather than as a report of the authentication protocol run.

This is not to say that issuing banks cannot in future implement secure proprietary schemes within the EMV framework: because the internal protocols are proprietary anything is possible, and some potential options will be discussed in Section VI. But such schemes must make ever more complex and intricate analysis of the transaction data returned, driving up the complexity and fragility of the existing EMV card authorization systems. Essentially, they will have to ignore the framework, and without a change in the framework itself, the authorization calculations will remain so complex and dependent on external factors that further mistakes are very likely. Also, as the protocol becomes more customized by the issuer, the introduction of new system-wide features sought for other purposes will become progressively more difficult and expensive.

The failure of EMV has many other aspects which will be familiar to security engineers. There was a closed design process, with no open external review of the architecture and its supporting protocols. The protocol documentation appeared eventually in the public domain – nothing implemented by 20,000 banks could have been kept secret – but too late for the research community to give useful feedback before a lot of money was spent on implementation.

The economics of security work out not just in the interaction between banks, customers and merchants – with

Mastercard, Ex1002, p. 886

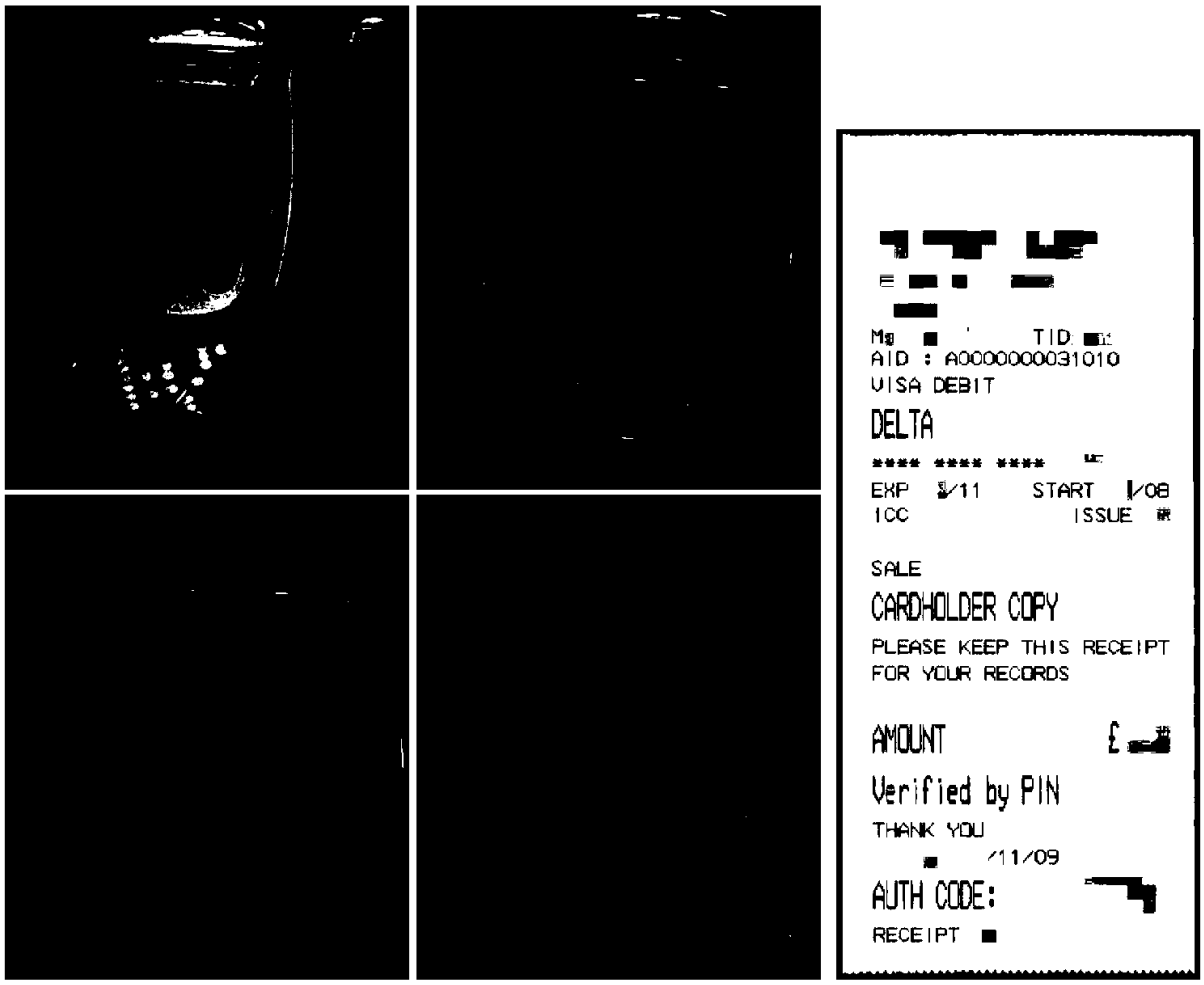


Figure 5. Carrying out the attack. Although we entered the wrong PIN, the receipt indicates that the transaction was "Verified by PIN".

the banks using their control of the system to dump liability, and thus undermining their own incentive to maintain it. There are also mismatches between acquirer and issuer banks, with only the latter feeling any real incentive to remediate security failures; between banks and suppliers, with the latter being squeezed on costs to the point that they have little incentive to innovate; and between banks and the facilities management firms to whom much of the business of card personalisation, network operation, and so on gets outsourced. The industry as a whole suffers from a significant collective action problem. It will be interesting to see which of the dozens of national bank regulators, or which of the three card schemes, will initiate action to deal with those aspects of the problems described here that cannot be tackled by issuer banks acting alone. It may be worth bearing in mind that the smart card industry spent some twenty years pitching its products to the banks before it managed to overcome the collective action problem and get the industry to move. In the absence of a catastrophe, changes that require everyone to act together are going to be slow at best.

A major contributing factor to the fact that these protocol flaws remained undiscovered is the size and complexity of the specification, and its poor structure. The core EMV protocols are now 707 pages long, there are a further 2 126 pages of testing documentation, and card schemes also specify extensions (Visa publishes 810 pages of public documentation, and there is more which is secret). Many options are given, and a typical implementation mixes some of the functionality from the published manuals with some issuer-specific enhancements. Security critical details are scattered throughout, and there is no one section which is

Mastercard, Ex1002, p. 887

sufficient to understand the protocol, the threat model, or the security policy. In fact, much detail is not specified at all, being left to implementation decisions by individual issuers.

For example, to confirm the existence of the security vulnerability discussed in this paper, we needed to establish:

- Lack of authentication in transport layer (EMV Book 1 [1])
- Encoding of Verify (EMV Book 3 [3, p71])
- Encoding of the TVR (EMV Book 3, Annex C [3, p171])
- Recommended generation algorithm for the ARPC (EMV Book 2 [2, p89])
- Recommended transaction data items to be included in the ARQC and TC (EMV Book 2 [2, p88])
- Absence of cardholder verification result in ARQC and TC requests (EMV Book 2 [2, p73], EMV Book 3 [3, p58])
- Encoding of the CVM list (EMV Book 3, Annex C [3, p168])
- Algorithm for selecting cardholder verification method (EMV Book 3 [3, p103])
- Transaction flow (EMV Book 3 [3, p83])
- Values of the TVR for signature transaction (EMV Book 4 [4, p49])
- Whether the actual cardholder verification method used is included in the CDOL (unspecified, found by experiment)
- Whether the issuer checks value of IAD in online transactions (unspecified, found by experiment)
- Whether the terminal attempts to decode the IAD (unspecified, found by experiment)
- Encoding of the IAD (proprietary, specified in Visa Integrated Circuit Card Specification, Appendix A [8, p222])

Ultimately EMV is a compatibility system and protocol toolkit. It allows interoperable protocols to be built, but following the specification – even including the optional recommendations – does not ensure a secure protocol. This may explain why there has been little analysis of EMV. The specification does not contain enough detail to support any claims about the security of implementations, as they depend on proprietary, and often unpublished, details. It is necessary to do experiments, as we did. But researchers, and merchants who assist them, may be afraid of retribution from the banking industry, which makes experimentation difficult.

VI. Solutions and Non-Solutions

Core protocol failures are difficult to fix. None of the security improvements already planned by banks will help: moving from SDA to DDA will not have any effect, as these are both methods for card authentication, which occurs before the cardholder verification stage. Neither will a further proposed enhancement – CDA (combined data authentication) – in which the transaction authorization stage additionally has a digital signature under a private key held by the card. This is because the attack we present does not interfere with either the input or output of transaction authentication, so replacing a transaction MAC with a digital signature will not help.

One possible work-around is for the terminal to parse the IAD, which does include the result of PIN verification (Table II). This will only be effective for online transactions, and offline transactions where CDA is used, otherwise the man-in-the-middle device could tamper with the IAD as it is returned by the card. It would also be difficult to implement because the IAD was intended only for the issuer, and there are several different formats, without any reliable method to establish which one is used by a particular card. However a solution along these lines would require the acquiring banks and the terminal vendors to act together, which for the incentive reasons discussed above would be both slow and difficult.

The realities of security economics mean that we have to look for a fix which requires changes only to customer cards or to the issuer's back-end systems. Such a repair may in fact be possible: the card can change its CDOL to request that the CVMR (cardholder verification method results) be included in the payload to the Generate AC command. This specifies which cardholder verification method the terminal believes was used, and so should allow the card and issuer to identify the inconsistency. Out of many, we have only seen one EMV card which requests this field, and it is not clear that the issuer actually validates the CVMR against the IAD. Whether this fix works for a given bank will depend on its systems; we have not been able to test it, and given that it involves reissuing the card base it would take years to roll out.

In addition to the global EMV specifications, and ones from card-scheme operators such as Visa and MasterCard, there are also country-specific standards. In the UK, the standard for communications between merchant terminal and acquirer is APACS 70, Book 2 [13], which specifies that both the IAD and CVMR must be sent. This is sufficient information for the issuer to detect the attack, but our results clearly show that they are not currently doing so. One possible reason is that the data items are dropped or corrupted between the acquirer and issuer (industry experts disagree over whether this is the case). Another possibility is that some terminals do not set the CVMR correctly, resulting in too many false positives if it were compared against the IAD. In any case, unless the CVMR is included in the CDOL it may not be integrity-protected, so a second man-in-the-middle between terminal and acquirer (perhaps installed with co-operation of a corrupt merchant staff member) could tamper with it too.

These workarounds should resolve the particular flaw discussed in this paper, but there are likely to be more. A more prudent approach would be to follow established

Mastercard, Ex1002, p. 888

design principles for robust security protocols. For example, adopting the "Fail-stop" [14] principles would prevent this attack; so would the explicitness principle, of ensuring you authenticate all data that might be relied on. Either approach would be likely to prevent other attacks too, and it would also make the protocols easier to analyze. Alternatively an industry standard transport-layer confidentiality and authenticity standard, such as TLS [15], could be wrapped around the existing command set. However, it's important that a fix should not just be an ad-hoc hack. The next version of EMV needs a proper security engineering exercise; regulators should insist that a threat model, security policy and protocol specification are published for open review.

VII. Evidence in Chip and PIN Disputes

Even if it turns out to be too expensive in the short term to prevent the attack we present in this paper, it is important to detect whether it occurred when resolving cases where a customer disputes a transaction. While assisting fraud victims who have been refused a refund by their bank, we have requested the IAD so as to discover whether the card believes PIN verification succeeded, but have almost always been refused. This paper illustrates that while the IAD can be considered trustworthy (after its MAC has been verified), the TVR and merchant receipt must not.

In fact, dispute resolution processes we have seen in the UK are seriously flawed, even excluding the protocol failure described here. In one disputed transaction case we assisted in, the customer had his card stolen while on holiday, and then used in an EMV transaction. The issuer refused to refund this customer on the basis that their records showed the PIN was used. Luckily, the customer managed to obtain the merchant receipts, and these contained the TVR. This indicated that the PIN was not used, and the merchant opted to fall back to signature. We decoded the TVR and informed the customer, who was then able to get a refund.

Other customers are less fortunate: it is unusual for the TVR to be included on the receipt, and often the merchant receipt has been destroyed by the time the dispute is being considered. In these cases we have not been able to obtain the TVR, IAD, or even a statement by the bank as to how they established that the cardholder was verified through the correct PIN being entered.

Our demonstration therefore exposes a deeper flaw in EMV and the associated systems: they fail to produce adequate evidence for dispute resolution or litigation. Procedures are also a mess. For example, once a transaction is disputed a typical bank either destroys the card or asks the customer to do so, preventing information from being extracted which might show whether the card was actually used. Transaction logs are commonly only kept for 120 days, and by the time the dispute is being heard the bank may have destroyed most of the records. (This was the case in the well-known Job v. Halifax trial: even though the Halifax had been notified that the transaction was being disputed, the logs were then destroyed in defiance of Visa guidelines [16].)

These general issues are discussed by Murdoch [17], but the vulnerability described in this paper poses a problem for such banks. If they have indeed destroyed all record of the IAD, they will be unable to show that disputed transactions actually used the correct PIN. So our findings might help banks understand that it is in their interest to retain evidence rather than destroy it.

Another evidential issue is that even if the issuer were able to establish whether the attack we present here had occurred, this may not help customers because the typical receipt still states that the PIN was verified. Although this may be false, many people evaluating evidence (adjudicators, judges, and jury members) will not know this. In one particular case, from 2009, the issuing bank, and government-approved adjudicator, explicitly relied upon the "Verified by PIN" indicator on the merchant receipt, in concluding that the transaction was PIN-verified and therefore the customer was liable. For this reason we propose that terminals no longer print "Verified by PIN" unless the protocol actually supports this assertion.

VIII. Related Work

EMV has been available for 14 years and is now widely deployed despite little published research on its security. In 1999, Herreweghen and Wille [18] evaluated the suitability of EMV for Internet payments and identified the problem of not being able to determine if the Verify command was ever executed because it is not authenticated. In their proposed Internet-based payment scheme, they suggested that the ARQC should only be generated if the Verify command has been successful. But their paper did not consider that the result of PIN verification is included in the IAD, nor that the Verify message could be tampered with by a man-in-the-middle in a point-of-sale transaction.

More recently, interest in EMV has increased since it was widely deployed in 2005, but perhaps due to the specification's complexity and incompleteness, the closed user community, and difficulties in carrying out experiments, researchers have not done much work on it. Anderson *et al.* [19] described how bank customers might have difficulty in obtaining refunds once transactions were authorized by PIN. That paper also outlined some potential attacks against Chip and PIN, such as cloning SDA cards for use in offline transactions, and the likelihood that criminals would migrate towards cross-border fraud if and when legacy magnetic strip transactions were disabled at domestic ATMs. It also briefly considered the attack line described in this paper, but did not follow though at the time with detailed analysis or performing experiments.

Another potential EMV weakness outlined in [19] was the relay attack, which was refined and demonstrated by Drimer and Murdoch [20]. Here, the criminal sets up a tampered

Mastercard, Ex1002, p. 889

Chip and PIN terminal, which the victim uses to make a small transaction (e.g. buying a meal at a restaurant). Rather than placing the transaction, the terminal relays the session to a fake card which is being used for a far larger transaction elsewhere (e.g. buying diamonds at a jewelery shop). The authors also described a defence against this attack, in which the terminal and card engage in a cryptographic exchange which not only establishes authenticity but also a maximum distance bound, either eliminating or greatly limiting the applicability of the attack.

Another attack is to tamper a terminal to merely record card details, and then use them for a fraudulent transaction later. Drimer *et al.* [21] demonstrated that current Chip and PIN payment terminals have inadequate tamper resistance, and a tapping device can be surreptitiously added to record the customer's PIN and enough details to allow a cloned magnetic strip card to be created. Criminals are now known to have carried out variants of this attack, so banks are now taking action: the chip no longer has a copy of the magnetic strip (one data field is replaced), and magnetic strip fallback transactions are gradually being phased out.

The work presented in this paper is a significant advance in our understanding of attacks against EMV because it is applicable to online transactions (unlike cloned SDA "yes cards"); it does not require criminals to synchronise their fraudulent purchase with that of an unwitting customer (as the relay attack does); and it does not depend on magnetic strip fallback (unlike the payment terminal tampering attacks). As a consequence, it may be one of the most realistic and attractive attacks for criminals, if and when magnetic strip transactions are no longer permitted. It could even be used at the moment, by criminals who wish to make purchases in countries which now mandate EMV transactions at point of sale. It may explain a number of the transaction dispute cases reported to us.

If this attack becomes more widely used, its net effect will be that criminals can use stolen cards in shops without the cardholder being negligent – exactly as was the case with magnetic strip cards before the introduction of EMV. However, so long as the public is not aware of this, the banks will be able to get away with blaming cardholders for fraud. We have therefore decided on a policy of responsible disclosure, of publishing this paper some time after informing bank regulators in the UK, Europe and North America of the vulnerability.

At present, we understand that there is a lot of pressure on the US Federal Reserve from the banks it regulates to countenance a move from magnetic strip cards to EMV. This paper shows that such a move may be premature. It's not reasonable for the smart card industry to foist a broken framework on the US banking industry and then leave it to individual issuer banks to come up with patches. The EMV consortium should first publish its plans for fixing the framework, presumably with the next version (v 5) of the EMV specification. The Fed should then satisfy itself of three things.

First, will the fix work technically? For this, only open peer review will do. Second, will the high level of consumer protection so far enjoyed by US cardholders be preserved? Third, will the introduction of the remediated system introduce any systemic risks, because of moral hazard effects? For these last two questions to be answered in the affirmative, we believe that there must be no associated 'liability shift' as there has been in Europe and Canada.

IX. Response

The response to our paper has been largely positive, with most knowledgeable respondents agreeing that the attack works. However there was substantial discord regarding our conclusion that "Chip and PIN is broken", which can mainly be explained by differences in the way that respondents define and measure success. In this section we summarise and comment only on the discordant responses: the positive responses speak for themselves.

Respondents who measure success differently have argued that Chip and PIN is *de facto* successful because its deployment has reduced lost and stolen card fraud; others argued that it is successful because the chip itself still has not been fully cloned by criminals.

We measure the success of Chip and PIN by its two core goals: first, to prevent counterfeit card fraud using the chip, and second to prevent lost and stolen card fraud using the PIN. Because stolen cards can be used without knowing the PIN, by our definition, Chip and PIN is broken. We do not believe that the system is broken beyond repair, but neither is it the case that a simple fix will suffice, due to the unmanageable complexity of EMV. This has been demonstrated by the spirited disagreement among experts discussing the attack on our blog [22] and proposing different favoured solutions, and by the continued absence of a fix at the time of writing, almost three months since the industry was notified.

Some of our respondents argued that Chip and PIN was a success on economic grounds, claiming that it saved more money from fraud than it cost to deploy. However they did not present figures to back up this claim. And counterfactual history is hard: how would one show that in the absence of EMV, fraud would have increased even more than it in fact has? Other respondents agreed that Chip and PIN simply pushed fraud to other areas such as card-not-present fraud, undermining the argument of economic success.

Some respondents argued that our attack would be difficult to deploy, for instance because of the bulk of the equipment and because of the narrow window of opportunity between theft of a card and its cancellation once the cardholder reports it stolen. Some even insisted on characterising it as theoretical, despite the fact it was deployed against live terminals at real merchants at three different sites. Whilst our demonstration equipment was indeed bulky, miniaturization

Mastercard, Ex1002, p. 890

is straightforward and well within the capabilities of criminals who already miniaturize hi-tech point-of-sale skimmers and ATM skimmers. Skimmers perform far more complex actions than blocking a single command from a protocol run. Those who argued that the window of opportunity for abuse is small fail to recognise that the very reason the PIN is used is to prevent abuse of lost/stolen cards, so clearly the threat must have been substantial enough to justify investment in PIN technology in the first place. A larger window for abuse can also be achieved by postal interception of replacement cards, by stealing the victim's mobile phone at the same time as a card, or by pickpocketing rather than mugging: there really is no shortage of opportunity to abuse stolen cards.

Other respondents argued that the problem was not significant because systems could be patched to prevent it. Commenters proposed various cross-checking measures that might be performed by the issuing banks: checking the correspondence between CVMR and IAD (we also proposed this ourselves), or checking terminal capabilities and various acquirer fields such as POS data entry mode (defined in standard ISO 8583) against the IAD. But definite suggested fixes are generally remarkable by their absence. Indeed, some respondents claimed that card schemes were aware of this attack as far back as 2002; so if any straightforward cross-checks could fix the problem, surely they would have been implemented either now, or within the three months during which our paper circulated privately in the industry. Others argued that banks might simply move to online PIN at point-of-sale – in essence to abandon Chip and PIN in favour of an older approach – or move to CDA, where proprietary card checks such as the "terminal erroneously considers PIN OK" flag might help detect the subterfuge. Unfortunately none of these patches are easy. They require either a card re-issue, or re-engineering of the POS acquirer networks in those countries not set up to support online PIN. Both would be expensive. In particular, CDA has not been widely adopted because it is very sensitive to cryptographic errors: because more data are authenticated, it is more likely that a bug or incompatibility will cause an authentication failure. Many countries simply do not have the quality of engineering in their payment networks to be able to use CDA – a symptom of the excessive complexity of EMV.

A third class of respondents admitted the attack worked, but argued that because the IAD would be the most trusted source, and since this would not record PIN use, customers would never be liable for the losses. Unfortunately, in nearly all the disputes where we have assisted, banks have been extremely reluctant to provide any cryptographic evidence at all. Instead they have relied upon summary records of the transaction (not on any raw transaction data), or even on the printed receipts from the merchant, which we have proven to be untrustworthy.

Finally, some respondents agreed there was a problem but felt we had misattributed the blame. They argued that it was not EMV that was at fault, or the card schemes' specifications, but the issuing banks. When contacted for comment, these same issuing banks referred us back to central bodies such as card schemes or trade associations. No-one wants to take responsibility. It is true that EMV is a protocol framework, and that its scope does not extend to issuer checks. We would argue that for any protocol specification to be valid, it must necessarily include statements of checks that must be performed by each party on the protocol messages. In the absence of named specification authors who accept responsibility, we feel it is fair to attribute responsibility to the "Chip and PIN" system, which is after all a marketing term that covers a whole specification stack.

X. Conclusion

We have shown how the PIN verification feature of the EMV protocol is flawed. A lack of authentication on the PIN verification response, coupled with an ambiguity in the encoding of the result of cardholder verification as included in the TVR, allows an attacker with a man-in-the-middle to use a card without the correct PIN. This attack can be used to make fraudulent purchases on a stolen card. We have shown that the live banking network is vulnerable by placing a transaction using the wrong PIN, with every major UK bank and foreign banks too. The records indeed falsely show that the PIN was verified, and the money was actually withdrawn from an account.

Attacks such as this could help explain the many cases in which a card has supposedly been used with the PIN, despite the customer being adamant that they have not divulged it. So far, banks have refused to refund such victims, because they assert that a card cannot be used without the correct PIN. This paper shows that their claim is false.

We have discussed how this protocol flaw has remained undetected; not only are the public specifications complex, but they also fail to specify security-critical details. Finally, we have discussed ways in which this vulnerability may be fixed by issuer banks, while maintaining backwards compatibility with existing systems. However, it is clear that the EMV framework is seriously flawed. Rather than leaving its member banks to patch each successive vulnerability, the EMV consortium must start planning a redesign and an orderly migration to the next version. In the meantime, the EMV protocol should be considered broken. We recommend that the Federal Reserve should resit pressure from banks to allow its deployment in the USA until it is fixed.

Acknowledgments

We thank the anonymous reviewers, Colin Whittaker, and the contributors to the Light Blue Touchpaper blog for their comments. We also thank the merchants and cardholders who allowed us to carry out experiments, and Markus Kuhn for photography assistance. Steven Murdoch is funded by the Tor Project and employed part-time by Cronto Ltd.

Mastercard, Ex1002, p. 891

REFERENCES

[1] *EMV – Integrated Circuit Card Specifications for Payment Systems, Book 1: Application Independent ICC to Terminal Interface Requirements*, Version 4.2 ed., EMVCo, LLC, June 2008.

[2] *EMV – Integrated Circuit Card Specifications for Payment Systems, Book 2: Security and Key Management*, Version 4.2 ed., EMVCo, LLC, June 2008.

[3] *EMV – Integrated Circuit Card Specifications for Payment Systems, Book 3: Application Specification*, Version 4.2 ed., EMVCo, LLC, June 2008.

[4] *EMV – Integrated Circuit Card Specifications for Payment Systems, Book 4: Cardholder, Attendant, and Acquirer Interface Requirements*, Version 4.2 ed., EMVCo, LLC, June 2008.

[5] EMVCo, "About EMV," November 2009. [Online]. Available: http://www.emvco.com/about_emv.aspx

[6] APACS, "2008 fraud figures announced by APACS," March 2009. [Online]. Available: http://www.ukpayments.org.uk/media_centre/press_releases/-/page/685/

[7] Which?, "Fraud victims struggle to get money back," June 2009. [Online]. Available: http://www.which.co.uk/news/2009/06/fraud-victims-struggle-to-get-money-back-179150.jsp

[8] *Visa Integrated Circuit Card – Card Specification*, Version 1.4.0 ed., Visa International, October 2001.

[9] S. J. Murdoch, S. Drimer, R. Anderson, and M. Bond, "EMV PIN verification "wedge" vulnerability," February 2010. [Online]. Available: http://www.cl.cam.ac.uk/research/security/banking/nopin/

[10] Maxim Integrated Products, Inc., *MAX1740, MAX1741 SIM/smart-card level translators in μMAX*, January 2001, http://datasheets.maxim-ic.com/en/ds/MAX1740-MAX1741.pdf. [Online]. Available: http://datasheets.maxim-ic.com/en/ds/MAX1740-MAX1741.pdf

[11] Xilinx Inc., "Spartan-3E starter kit," November 2009. [Online]. Available: http://www.xilinx.com/products/devkits/HW-SPAR3E-SK-US-G.htm

[12] "BLADOX Turbo SIM," March 2010. [Online]. Available: http://www.bladox.com/

[13] *Standard 70, Book 2 – Card Acceptor to Acquirer Interface Standards: Messages, Data Elements and Code Values for Real-time Systems*, The UK Cards Association, October 2009.

[14] L. Gong and P. Syverson, "Fail-stop protocols: An approach to designing secure protocols," in *International Working Conference on Dependable Computing for Critical Applications*, September 1995, pp. 44–55.

[15] T. Dierks and C. Allen, "The TLS protocol," IETF, RFC 2246, January 1999.

[16] "Job v Halifax PLC, case number 7BQ00307, commentary by Alistair Kelman," in *Digital Evidence and Electronic Signature Law Review*, vol. 6. Pario Communications, November 2009, ISBN 0-9543245-9-5; see also http://www.alikelman.com/jobhbos.pdf.

[17] S. J. Murdoch, "Reliability of chip & PIN evidence in banking disputes," in *Digital Evidence and Electronic Signature Law Review*, vol. 6. Pario Communications, November 2009, pp. 98–115, ISBN 0-9543245-9-5.

[18] E. V. Herreweghen and U. Wille, "Risks and potentials of using EMV for Internet payments," *USENIX Workshop on Smartcard Technology*, May 1999.

[19] R. Anderson, M. Bond, and S. J. Murdoch, "Chip and spin," March 2005. [Online]. Available: http://www.chipandspin.co.uk/spin.pdf

[20] S. Drimer and S. J. Murdoch, "Keep your enemies close: Distance bounding against smartcard relay attacks," in *USENIX Security Symposium*, August 2007. [Online]. Available: http://www.usenix.org/events/sec07/tech/drimer/drimer.pdf

[21] S. Drimer, S. J. Murdoch, and R. Anderson, "Thinking inside the box: system-level failures of tamper proofing," in *IEEE Symposium on Security and Privacy (Oakland)*, May 2008, pp. 281–295. [Online]. Available: http://www.cl.cam.ac.uk/~sd410/papers/ped_attacks.pdf

[22] R. Anderson, "Chip and PIN is broken," Light Blue Touchpaper, February 2010. [Online]. Available: http://www.lightbluetouchpaper.org/2010/02/11/chip-and-pin-is-broken/

Mastercard, Ex1002, p. 892

APPENDIX

A. *Transaction Log of MITM Attack*

The following log was collected during one of our man-in-the-middle experiments, where we used one of our own cards to purchases goods in a online Chip and PIN transaction, while using the incorrect PIN. Data items which could be used to identify the merchant who assisted us with the experiments has been redacted (xx), and unnecessary detail has been removed for brevity (...). Principals are Terminal (T), Card (C), and man-in-the-middle (M).

T → C	00 a4 04 00 0e 31 50 41 59 2e 53 59 53 2e 44 44 - 46 30 31
C → T	6f 1a 84 0e 31 50 41 59 2e 53 59 53 2e 44 44 46 - 30 31 a5 08 88 01 02 5f 2d 02 65 6e 90 00
T → C	00 b2 01 14 00
C → T	70 40 61 1e 4f 07 a0 00 00 00 29 10 10 50 10 4c - 49 4e 4b 20 20 20 20 20 20 20 20 20 20 20 87 - 01 01 61 1e 4f 07 a0 00 00 00 03 10 10 50 10 56 - 49 53 41 20 44 45 42 49 54 20 20 20 20 20 20 87 - 01 02 90 00
T → C	00 a4 04 00 07 a0 00 00 00 03 10 10
C → T	6f 25 84 07 a0 00 00 00 03 10 10 a5 1a 50 10 56 - 49 53 41 20 44 45 42 49 54 20 20 20 20 20 20 87 - 01 02 5f 2d 02 65 6e 90 00
T → C	80 a8 00 00 02 83 00
C → T	80 0a 5c 00 08 01 01 00 10 01 04 01 90 00
T → C	00 b2 01 0c 00
C → T	70 3e 57...5f 20...9f 1f...90 00
T → C	00 b2 01 14 00
C → T	70 49 5f 25...5f 24...9f 07...5a...5f - 34...9f 0d...9f 0e...9f 0f...8e 10 00 00 - 00 00 00 00 00 00 41 03 1e 03 02 03 1f 03 90 00
T → C	00 b2 02 14 00
C → T	70 81 93 93...90 00
T → C	00 b2 03 14 00
C → T	70 81 c0 8f...9f 32...92...90 00
T → C	00 b2 04 14 00
C → T	70 48 8c 15 9f 02 06 9f 03 06 9f 1a 02 95 05 5f - 2a 02 9a 03 9c 01 9f 37 04 8d 17 8a 02 9f 02 06 - 9f 03 06 9f 1a 02 95 05 5f 2a 02 9a 03 9c 01 9f - 37 04 9f 08...5f 30...5f 28...9f 42...9f - 44...90 00

Select file "1PAY.SYS.DDF01"

Opened "1PAY.SYS.DDF01" (language EN)

Read Record
Available applications: "LINK" and "VISA DEBIT"

Select file "VISA DEBIT"
Opened "VISA DEBIT" (language EN)

Get Processing Options
Transaction started, 5 records available

Read Record
Record (Track 2 Equivalent Data, Cardholder Name, Track 1 Discretionary Data)

Read Record
Signed record (Application Effective Date, Application Expiration Date, Application Usage Control, Application Primary Account Number, Application Primary Account Number Sequence Number, Issuer Action Code – Default, Issuer Action Code – Denial, Issuer Action Code – Online, Cardholder Verification Method List)

Read Record
Record (Signed Static Application Data)

Read Record
Record (Certification Authority Public Key Index, Issuer Public Key Certificate, Issuer Public Key Exponent, Issuer Public Key Remainder)

Read Record
Record (Card Risk Management Data Object List 1 (CDOL1), Card Risk Management Data Object List 2 (CDOL2), Application Version Number, Service Code, Issuer Country Code, Application Currency Code, Application Currency Exponent)

Mastercard, Ex1002, p. 893

T → C	80 ca 9f 17 00
C → T	9f 17 01 03 90 00
T → M	**00 20 00 80 08 24 00 00 ff ff ff ff ff**
M → T	**90 00**
T → C	80 ae 80 00 1d xx xx xx xx xx xx 00 00 00 00 00 – 00 08 26 00 80 00 80 00 08 26 xx 11 09 00 xx xx – xx xx
C → T	80 12 80 xx xx xx xx xx xx xx xx xx xx 06 01 0a – 03 a0 00 10 90 00
T → C	00 82 00 00 0a xx xx xx xx xx xx xx xx 30 30
C → T	90 00
T → C	80 ae 40 00 1f 30 30 xx xx xx xx xx xx 00 00 00 – 00 00 00 08 26 00 80 00 80 00 08 26 xx 11 09 00 – xx xx xx xx
C → T	80 12 40 xx xx xx xx xx xx xx xx xx xx 06 01 0a – 03 60 00 10 90 00

Get Data (PIN try counter)
Remaining PIN tries = 3

Verify PIN "0000"
PIN correct

Generate AC (ARQC)

ARQC

External Authenticate
External authenticate successful

Generate AC (TC)

TC

Mastercard, Ex1002, p. 894

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/599,647	YEAGER, C. Douglas
	Examiner	Art Unit
	GARRISON PRINSLOW	3695

CPC - Searched*		
Symbol	**Date**	**Examiner**
H04L2209/56 OR H04L9/3234 OR H04L2209/80 OR H04L9/321 OR H04L9/3271 OR G06Q20/30 OR G06Q20/382 OR G06Q20/385 OR G06Q20/02 OR G06Q20/20 OR G06Q20/32 OR G06Q20/322 OR G06Q20/3223 OR G06Q20/40 OR G06Q20/40975 -- all, limited by text	02/09/2018	/GP/

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**
705	71, 67 -- all, limited by text	02/09/2018	/GP/

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
Inventor Search	9/27/2015	AP
East Search (please see attached)	9/29/2015	AP
East Search (please see attached)	6/10/2016	AP
East Search (please see attached)	5/29/2017	AP
Consulted with SPE Ryan Donlon, QEM Panel	02/09/2018	/GP/
Updated EAST Search Conducted, includes Inventor, Assignee, US, FOR DBs -- see attached search history	02/09/2018	/GP/
Updated search performed in Google Patents (Pats, NPL) -- find prior art of US 20130054474 A1	02/09/2018	/GP/

/G.P./ Examiner, Art Unit 3695	

Mastercard, Ex1002, p. 895

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/599,647	YEAGER, C. Douglas
	Examiner	Art Unit
	GARRISON PRINSLOW	3695

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/G.P./ Examiner, Art Unit 3695	

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	("13/599647").APP.	US-PGPUB; USPAT	OR	ON	2018/02/08 14:58
S2	55491	(((cryptogram$8) OR (cryptograph$8)) NEAR4 (key$8))	US-PGPUB; USPAT	OR	ON	2018/02/08 15:00
S3	584	S2 WITH ((temporar$8) OR (nonpermanent$8) OR ((non) ADJ (permanent$8)))	US-PGPUB; USPAT	OR	ON	2018/02/08 15:01
S4	30	S3 WITH (credential$8)	US-PGPUB; USPAT	OR	ON	2018/02/08 15:02
S5	192	S3 AND (credential$8)	US-PGPUB; USPAT	OR	ON	2018/02/08 15:02
S6	77	S5 AND (transact$8)	US-PGPUB; USPAT	OR	ON	2018/02/08 15:02
S7	60	S6 AND (authoriz$8)	US-PGPUB; USPAT	OR	ON	2018/02/08 15:03
S8	57	S7 AND (protocol$8)	US-PGPUB; USPAT	OR	ON	2018/02/08 15:03
S9	15	S8 AND (interrogat$8)	US-PGPUB; USPAT	OR	ON	2018/02/08 15:04
S10	53	S8 AND ((interrogat$8) OR (respons$8))	US-PGPUB; USPAT	OR	ON	2018/02/08 15:05
S11	57	S8 AND ((interrogat$8) OR (request$8) OR (respons$8))	US-PGPUB; USPAT	OR	ON	2018/02/08 15:06
S12	3	S7 NOT S8	US-PGPUB; USPAT	OR	ON	2018/02/08 15:06
S13	1324	S2 WITH ((temporar$8) OR (nonpermanent$8) OR ((non) ADJ (permanent$8)) OR ((one) ADJ2 ((time) OR (use))))	US-PGPUB; USPAT	OR	ON	2018/02/08 15:10
S14	58	S13 WITH (credential$8)	US-PGPUB; USPAT	OR	ON	2018/02/08 15:10
S15	2	S14 WITH (protocol$8)	US-PGPUB; USPAT	OR	ON	2018/02/08 15:11
S16	43	S14 AND (protocol$8)	US-PGPUB; USPAT	OR	ON	2018/02/08 15:11
S17	43	S14 AND (protocol$8)	US-PGPUB; USPAT	OR	ON	2018/02/08 15:13
S18	58	S13 WITH (credential$8)	US-PGPUB; USPAT	OR	ON	2018/02/08 15:14
S19	55491	(((cryptogram$8) OR (cryptograph$8)) NEAR4 (key$8))	US-PGPUB; USPAT	OR	ON	2018/02/08 18:50
S20	1324	S19 WITH ((temporar$8) OR (nonpermanent$8) OR ((non) ADJ (permanent$8)) OR ((one) ADJ2 ((time) OR (use))))	US-PGPUB; USPAT	OR	ON	2018/02/08 18:50

S21	58	S20 WITH (credential$8)	US-PGPUB; USPAT	OR	ON	2018/02/08 18:50
S23	58	S20 WITH (credential$8)	US-PGPUB; USPAT	OR	ON	2018/02/08 18:50
S24	25	S23 AND ((H04L2209/56 OR H04L9/3234 OR H04L2209/80 OR H04L9/321 OR H04L9/3271 OR G06Q20/30 OR G06Q20/382 OR G06Q20/385 OR G06Q20/02 OR G06Q20/20 OR G06Q20/32 OR G06Q20/322 OR G06Q20/3223 OR G06Q20/40 OR G06Q20/40975).CPC. OR (705/71 OR 705/67).CCLS. OR (H04L9/32 OR G06Q20/40 OR G06Q20/38 OR G06Q20/30).IPCR.)	US-PGPUB; USPAT	OR	ON	2018/02/08 19:01
S25	25	S23 AND ((H04L2209/56 OR H04L9/3234 OR H04L2209/80 OR H04L9/321 OR H04L9/3271 OR G06Q20/30 OR G06Q20/382 OR G06Q20/385 OR G06Q20/02 OR G06Q20/20 OR G06Q20/32 OR G06Q20/322 OR G06Q20/3223 OR G06Q20/40 OR G06Q20/40975).CPC. OR (705/71 OR 705/67).CCLS. OR (H04L9/32 OR G06Q20/40 OR G06Q20/38 OR G06Q20/30).IPCR.)	US-PGPUB; USPAT	OR	ON	2018/02/08 19:01
S26	17	S25 AND (protocol$8)	US-PGPUB; USPAT	OR	ON	2018/02/08 19:03
S27	8	S25 NOT S26	US-PGPUB; USPAT	OR	ON	2018/02/08 19:12
S28	55491	(((cryptogram$8) OR (cryptograph$8)) NEAR4 (key$8))	US-PGPUB; USPAT	OR	ON	2018/02/09 13:27
S29	1324	S28 WITH ((temporar$8) OR (nonpermanent$8) OR ((non) ADJ (permanent$8)) OR ((one) ADJ2 ((time) OR (use))))	US-PGPUB; USPAT	OR	ON	2018/02/09 13:27
S30	58	S29 WITH (credential$8)	US-PGPUB; USPAT	OR	ON	2018/02/09 13:27
S31	25	S30 AND ((H04L2209/56 OR H04L9/3234 OR H04L2209/80 OR H04L9/321 OR H04L9/3271 OR G06Q20/30 OR G06Q20/382 OR G06Q20/385 OR G06Q20/02 OR G06Q20/20 OR G06Q20/32 OR G06Q20/322 OR G06Q20/3223 OR G06Q20/40 OR G06Q20/40975).CPC. OR (705/71 OR 705/67).CCLS. OR (H04L9/32 OR G06Q20/40 OR G06Q20/38 OR G06Q20/30).IPCR.)	US-PGPUB; USPAT	OR	ON	2018/02/09 13:28
S32	33	S30 NOT S31	US-PGPUB; USPAT	OR	ON	2018/02/09 13:28
S33	16	((Douglas) NEAR2 (Yeager)).INV.	US-PGPUB; USPAT	OR	ON	2018/02/09 13:33
S34	0	(Simplytapp).AS.	US-PGPUB; USPAT	OR	ON	2018/02/09 13:33
S35	0	(Simplytapp).INV.	US-PGPUB; USPAT	OR	ON	2018/02/09 13:33
S36	16	S33 OR S34 OR S35	US-PGPUB; USPAT	OR	ON	2018/02/09 13:33

Mastercard, Ex1002, p. 898

S37	27	("20060143326" | "20060255158" | "20070208949" | "20070262138" | "20080128513" | "20090039156" | "20090187687" | "6439464" | "6763399" | "6883715" | "6991173" | "7011247" | "7150397" | "7213766" | "7249266").PN. OR ("8151345").URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2018/02/09 13:40
S38	58	S29 WITH (credential$8)	US-PGPUB; USPAT; USOCR	OR	ON	2018/02/09 13:42
S39	0	S29 WITH (credential$8)	FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/02/09 13:42
S40	4	(((cryptogram$8) OR (cryptograph$8)) NEAR4 (key$8)) WITH ((temporar$8) OR (nonpermanent$8) OR ((non) ADJ (permanent$8)) OR ((one) ADJ2 ((time) OR (use)))) WITH (credential$8)	FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/02/09 13:43
S41	185	(((cryptogram$8) OR (cryptograph$8)) NEAR4 (key$8)) WITH ((temporar$8) OR (nonpermanent$8) OR ((non) ADJ (permanent$8)) OR ((one) ADJ2 ((time) OR (use))))	FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/02/09 13:45
S43	16	S41 AND (protocol$8)	FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/02/09 13:45

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S45	58	(((cryptogram$8) OR (cryptograph$8)) NEAR4 (key$8)) WITH ((temporar$8) OR (nonpermanent$8) OR ((non) ADJ (permanent$8)) OR ((one) ADJ2 ((time) OR (use)))) WITH (credential$8)	US-PGPUB; USPAT	OR	ON	2018/02/09 13:49

2/9/2018 2:05:43 PM
C:\Users\gprinslow\Documents\EAST\Workspaces\13599647.wsp

Mastercard, Ex1002, p. 899

Substitute Form PTO/SB/08b

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/599,647
				Filing Date	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	~~Puttalah, Asha~~ Prinslow, Garrison
Sheet	1	of	1	Atty Docket Number	STAPP1100-5

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C4	International Preliminary Report on Patentability for Int'l Application No. PCT/US2012/053129, mailed 12/10/2013, 11 pgs.	

Examiner Signature	/GARRISON PRINSLOW/	Date Considered 02/08/2018	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /G.P./

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

44654 7590 03/01/2018

Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705

EXAMINER
PRINSLOW, GARRISON T

ART UNIT	PAPER NUMBER
3695	

DATE MAILED: 03/01/2018

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/599,647	08/30/2012	C. Douglas YEAGER	STAPP1100-5	1919

TITLE OF INVENTION: SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500	$0	$0	$500	06/01/2018

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PTOL-85 (Rev. 02/11)

Mastercard, Ex1002, p. 901

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

44654 7590 03/01/2018
Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/599,647	08/30/2012	C. Douglas YEAGER	STAPP1100-5	1919

TITLE OF INVENTION: SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500	$0	$0	$500	06/01/2018

EXAMINER	ART UNIT	CLASS-SUBCLASS
PRINSLOW, GARRISON T	3695	705-071000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Mastercard, Ex1002, p. 902

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/599,647	08/30/2012	C. Douglas YEAGER	STAPP1100-5	1919

44654 7590 03/01/2018

Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705

EXAMINER	
PRINSLOW, GARRISON T	
ART UNIT	**PAPER NUMBER**
3695	

DATE MAILED: 03/01/2018

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Mastercard, Ex1002, p. 903

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 13/599,647	Applicant(s) YEAGER, C. Douglas	
	Examiner GARRISON PRINSLOW	Art Unit 3695	AIA Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to 10/05/2017 .
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____ .

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are See Continuation Sheet . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file areply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☑ Notice of References Cited (PTO-892)
2. ☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date See Continuation Sheet
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____ .
5. ☐ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☑ Other BIB Data Sheet .

/G.P./ Examiner, Art Unit 3695	/KITO R ROBINSON/ Primary Examiner, Art Unit 3695

Continuation of 3. The allowed claim(s) is/are: 30-42,44-57 and 59-64

Continuation of Attachment(s) 2. Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date: 12/14/2016, 10/05/2017, 10/26/2017, 01/31/2018

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1) The present application is being examined under the pre-AIA first to invent provisions.

Introduction and Status of Claims

2) This communication is in response to Applicant's communications filed 10/05/2017, 10/26/2017, and 01/31/2018, which were filed in response to the prior Office Action (Non-Final Rejection dated 06/05/2017, hereinafter 'prior Office Action') and Applicant-Initiated Interview Summary (dated 09/25/2017, hereinafter 'prior Interview Summary').

3) Applicant's Amendments to the Claims dated 10/05/2017 (hereinafter, 'Amendments to the Claims') have been entered. Accordingly, claims 30, 31, 37-39, 42, 44, 45, 52, and 57 are currently amended. Claims 1-29, 43, and 58 are cancelled. New claims 59-64 have been entered. Claims 30-42, 44-57, and 59-64 are pending in this application (claims 30 and 44 being independent).

4) With regard to the prior Office Action, in view of the Amendments to the Claims, the previous Claim Rejections under 35 U.S.C. 112 (regarding claims 42, 43, 57, and 58), and Claim Rejections under 35 U.S.C. 103 (regarding claims 30-42 and 44-57) of the prior Office Action are hereby withdrawn.

5) It is further noted that the reasons for withdrawing previous Claim Rejections under 35 U.S.C. 101 were indicated in the prior Office Action (at page 3, paragraph 8).

Information Disclosure Statements

6) The information disclosure statements (IDSs) submitted on 12/14/2016, 10/05/2017, 10/26/2017, and 01/31/2018 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements have been considered by the Examiner.

Response to Amendment

7) Applicant's Arguments/Remarks filed 10/05/2017 (hereinafter, 'Applicant's Arguments') have been fully considered, with respect to the Amendments to the Claims and the prior Office Action. The Examiner's responses are indicated herein-below.

Allowable Subject Matter

8) Claims 30-42, 44-57, and 59-64 are allowed.

9) The following is the Examiner's statement of reasons for the indication of allowable subject matter.

10) It is noted that the reasons for withdrawing previous Claim Rejections under 35 U.S.C. 101 were indicated in the prior Office Action (at page 3, paragraph 8). Regarding analysis under 35 U.S.C. 101, the Examiner further notes that even if the instant claims could be argued to be "directed to" an abstract idea, such as "participation in a payment card transaction authorization process" (per the preamble of independent claim 30), under *Step 2A*, at least the following limitations of the instant claims are deemed by the Examiner to encompass "*Significantly More*" under *Step 2B* by being, for example, directed to an improvement to digital credential cryptographic key technology and/or by adding specific limitations other than what is well-understood, routine and conventional in the field and/or by adding unconventional steps that confine the claim to a particular useful application and/or by adding other meaningful limitations beyond generally linking the use of the judicial exception to a particular technological environment (illustrated by limitations of independent claim 30, however, independent claim 44 incorporates substantially similar limitations, *mutatis mutandis*):

- at a mobile device, executing an application in an operating system of the mobile device, the application interrogable by an electronic reader, over a first communications channel, for digital credential data corresponding to an account having a corresponding digital credential and configured to request, from a remote computer system hosting the corresponding digital credential, over a wireless network that is separate from the first communications channel, data associated with the account and generate cryptograms request during interrogations over the first communications channel using the data associated with the account received from the remote computer system, wherein the application does not access a permanent cryptographic key issued for the digital credential during the interrogations; [...]
- receiving by the application, from the remote computer system, over the wireless network, the first set of data associated with the account, the first set of data associated with the account usable by the application to formulate a first application protocol data unit response, the first set of data comprising a first non-permanent cryptographic key associated with the account; [...]

- receiving by the application, from the remote computer system, over the wireless network, the second set of data associated with the account, the second set of data comprising a second non-permanent cryptographic key associated with the account;

11) Thus, for at least the reasons above, the pending instant claims are deemed to be directed to patent-eligible subject matter under 35 U.S.C. 101. *See, e.g., 2014 Interim Guidance* and *July 2015 Update*.

12) It is noted that, per above, in view of the Amendments to the Claims, the previous rejections of the claims under 35 U.S.C. 103 in the prior Office Action have been withdrawn. The Examiner further notes that after an updated search was conducted, the closest prior art of record (Royyuru et al., US-2010/0185545-A1), does not reasonably teach or suggest, alone or in combination, at least the following limitations of the pending instant claims (illustrated by limitations of independent claim 30, however, independent claim 44 incorporates substantially similar limitations, *mutatis mutandis*):

- at a mobile device, executing an application in an operating system of the mobile device, the application interrogable by an electronic reader, over a first communications channel, for digital credential data corresponding to an account having a corresponding digital credential and configured to request, from a remote computer system hosting the corresponding digital credential, over a wireless network that is separate from the first communications channel, data associated with the account and generate cryptograms request during interrogations over the first communications channel using the data associated with the account received from the remote computer system, wherein the application does not access a permanent cryptographic key issued for the digital credential during the interrogations; [...]
- receiving by the application, from the remote computer system, over the wireless network, the first set of data associated with the account, the first set of data associated with the account usable by the application to formulate a first application protocol data unit response, the first set of data comprising a first non-permanent cryptographic key associated with the account; [...]
- receiving by the application, from the remote computer system, over the wireless network, the second set of data associated with the account, the second set of data comprising a second non-permanent cryptographic key associated with the account;

13) Thus, for at least the reasons above, the pending instant claims are deemed to be allowable over the closest prior art.

14) Any comments considered necessary by Applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

15) The prior art made of record but not relied upon herein but pertinent to Applicant's disclosure is listed in the enclosed PTO-892.

16) Any inquiry concerning this communication or earlier communications from the examiner should be directed to GARRISON PRINSLOW whose telephone number is (571) 270-1812. The examiner can normally be reached on Monday-Friday 9:30am-6pm ET.

17) Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

18) If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ryan D Donlon can be reached on (571) 270-3602. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

19) Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/G.P./
Examiner, Art Unit 3695

/KITO R ROBINSON/
Primary Examiner, Art Unit 3695

9 February 2018

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/599,647	YEAGER, C. Douglas
	Examiner	Art Unit
	GARRISON PRINSLOW	3695

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	09/29/2015	06/10/2016	05/29/2017	02/09/2018					
	1	✓	-	-	-					
	2	✓	-	-	-					
	3	✓	-	-	-					
	4	✓	-	-	-					
	5	✓	-	-	-					
	6	✓	-	-	-					
	7	✓	-	-	-					
	8	✓	-	-	-					
	9	✓	-	-	-					
	10	✓	-	-	-					
	11	✓	-	-	-					
	12	✓	-	-	-					
	13	✓	-	-	-					
	14	✓	-	-	-					
	15	✓	-	-	-					
	16	✓	-	-	-					
	17	✓	-	-	-					
	18	✓	-	-	-					
	19	✓	-	-	-					
	20	✓	-	-	-					
	21	✓	-	-	-					
	22	✓	-	-	-					
	23	✓	-	-	-					
	24	✓	-	-	-					
	25	✓	-	-	-					
	26	✓	-	-	-					
	27	✓	-	-	-					
	28	✓	-	-	-					
	29		-	-	-					
1	30		✓	✓	=					
2	31		✓	✓	=					
3	32		✓	✓	=					
4	33		✓	✓	=					
5	34		✓	✓	=					
6	35		✓	✓	=					
7	36		✓	✓	=					
8	37		✓	✓	=					
9	38		✓	✓	=					
10	39		✓	✓	=					
11	40		✓	✓	=					
12	41		✓	✓	=					
13	42		✓	✓	=					

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/599,647	YEAGER, C. Douglas
	Examiner	Art Unit
	GARRISON PRINSLOW	3695

CLAIM		DATE								
Final	Original	09/29/2015	06/10/2016	05/29/2017	02/09/2018					
	43		✓	✓	-					
17	44		✓	✓	=					
18	45		✓	✓	=					
19	46		✓	✓	=					
20	47		✓	✓	=					
21	48		✓	✓	=					
22	49		✓	✓	=					
23	50		✓	✓	=					
24	51		✓	✓	=					
25	52		✓	✓	=					
26	53		✓	✓	=					
27	54		✓	✓	=					
28	55		✓	✓	=					
29	56		✓	✓	=					
30	57		✓	✓	=					
	58		✓	✓	-					
14	59				=					
31	60				=					
15	61				=					
32	62				=					
16	63				=					
33	64				=					

INFORMATION DISCLOSURE STATEMENT				Application Number	13/599,647
				Filing or 371 (c) Date:	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	~~Puttaiah, Asha~~ Prinslow, ~~Garrison~~
Sheet	1	of	1	Attorney Docket Number	STAPP1100-5

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C21	Office Action issued for Chinese Patent Application No. 201280053080.6, mailed October 18, 2017, 19 pages.	

Examiner Signature	/GARRISON PRINSLOW/	Date Considered 02/08/2018	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /G.P./

Notice of References Cited	Application/Control No. 13/599,647	Applicant(s)/Patent Under Reexamination YEAGER, C. Douglas	
	Examiner GARRISON PRINSLOW	Art Unit 3695	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-8306228-B2	11-2012	Le Saint; Eric	H04L63/0421	380/259
*	B	US-9767262-B1	09-2017	Canavor; Darren E.	G06F21/6218	1/1
*	C	US-20130262317-A1	10-2013	COLLINGE; Mehdi	G06Q20/3823	705/71
*	D	US-20140189359-A1	07-2014	MARIEN; DIRK	H04L9/3228	713/172
*	E	US-9124433-B2	09-2015	Marien; Dirk	H04L9/3234	1/1
*	F	US-8806600-B2	08-2014	Taratine; Boris	G06F21/34	713/185
*	G	US-20120317628-A1	12-2012	Yeager; C. Douglas	G06Q20/204	726/5
*	H	US-8151345-B1	04-2012	Yeager; C. Douglas	G06Q20/367	235/375
*	I	US-20120173432-A1	07-2012	Yeager; C. Douglas	G06Q20/367	705/65
*	J	US-8548924-B2	10-2013	Yeager; C. Douglas	G06Q20/367	235/375
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Murdoch et al., "Chip and PIN is Broken", 2010, IEEE Symposium on Security and Privacy, 1081-6011/10, pg. 1-14 (Year: 2010)
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 1919

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/599,647	08/30/2012	705	3695	STAPP1100-5

APPLICANTS

INVENTORS

C. Douglas YEAGER, Austin, TX;

**** CONTINUING DATA ***************************

This appln claims benefit of 61/685,863 03/26/2012
and claims benefit of 61/573,476 09/06/2011
and claims benefit of 61/575,846 08/30/2011

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☐ No Verified and Acknowledged /GARRISON PRINSLOW/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		TX	24	~~29~~ 33	~~3~~ 2

ADDRESS

Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705
UNITED STATES

TITLE

SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE

FILING FEE RECEIVED		
960	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/599,647	YEAGER, C. Douglas
	Examiner	**Art Unit**
	GARRISON PRINSLOW	3695

CPC						
Symbol					**Type**	**Version**
G06Q	/	20	/	40975	F	2013-01-01
G06Q	/	20	/	3223	I	2013-01-01
G06Q	/	20	/	02	I	2013-01-01
G06Q	/	20	/	20	I	2013-01-01
G06Q	/	20	/	32	I	2013-01-01
G06Q	/	20	/	382	I	2013-01-01
G06Q	/	20	/	385	I	2013-01-01
G06Q	/	20	/	40	I	2013-01-01
H04L	/	9	/	321	I	2013-01-01
H04L	/	9	/	3234	I	2013-01-01
H04L	/	9	/	3271	I	2013-01-01
H04L	/	2209	/	56	A	2013-01-01
H04L	/	2209	/	80	A	2013-01-01

CPC Combination Sets								
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

/GARRISON PRINSLOW/ Examiner, Art Unit 3695	09 February 2018	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	33	
/KITO R ROBINSON/ Primary Examiner, Art Unit 3695	13 February 2018	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	28

U.S. Patent and Trademark Office — Part of Paper No.: 20180204

Mastercard, Ex1002, p. 916

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/599,647	YEAGER, C. Douglas
	Examiner	Art Unit
	GARRISON PRINSLOW	3695

INTERNATIONAL CLASSIFICATION					
CLAIMED					
G06Q	/	20	/	40	

NON-CLAIMED					
	/		/		

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS

CROSS REFERENCES(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					

/GARRISON PRINSLOW/ Examiner, Art Unit 3695	09 February 2018	Total Claims Allowed:	
(Assistant Examiner)	(Date)	33	
/KITO R ROBINSON/ Primary Examiner, Art Unit 3695	13 February 2018	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	28

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/599,647	YEAGER, C. Douglas
	Examiner	**Art Unit**
	GARRISON PRINSLOW	3695

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		10		19		28	8	37	19	46	28	55	33	64
	2		11		20		29	9	38	20	47	29	56		
	3		12		21	1	30	10	39	21	48	30	57		
	4		13		22	2	31	11	40	22	49		58		
	5		14		23	3	32	12	41	23	50	14	59		
	6		15		24	4	33	13	42	24	51	31	60		
	7		16		25	5	34		43	25	52	15	61		
	8		17		26	6	35	17	44	26	53	32	62		
	9		18		27	7	36	18	45	27	54	16	63		

/GARRISON PRINSLOW/ Examiner, Art Unit 3695	09 February 2018	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	33	
/KITO R ROBINSON/ Primary Examiner, Art Unit 3695	13 February 2018	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	28

U.S. Patent and Trademark Office — Part of Paper No.: 20180204

Mastercard, Ex1002, p. 918

INFORMATION DISCLOSURE STATEMENT				Application Number	13/599,647
				Filing or 371 (c) Date:	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	Garrison T. Prinslow
Sheet	1	of	1	Attorney Docket Number	STAPP1100-5

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C22	Notice of Allowance issued for Canadian Patent Application No. 2,846,462, mailed February 1, 2018, 1 page.	

Examiner Signature		Date Considered	

Innovation, Sciences et Développement économique Canada
Office de la propriété intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

ROBIC
opic.brevets@robic.com

Date : 2018/02/01

Classification :
G06Q 20/40

AVIS D'ACCEPTATION/NOTICE OF ALLOWANCE

N° de demande/Application No. : 2,846,462 **Date de dépôt/Filing date :** 2012/08/30

Votre référence/ Your Reference : 011446-0050

Titre de l'invention/ Title of Invention : SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM

Propriétaire(s)/Owner(s) : SIMPLYTAPP, INC.

Revendications/Claims : 033

Examiné tel que modifié/ Examined as amended : 2017/11/01

Taxe pour pages en sus/ Excess Pages Fee : $102.00

La demande de brevet susmentionnée a été jugée acceptable.

Il faut acquitter la taxe finale de TROIS CENTS DOLLARS (300$), ou CENT CINQUANTE DOLLARS (150$) si le requérant a le droit de revendiquer le statut de petite entité et a soumis une déclaration de petite entité, dans les six mois suivant la date du présent avis. Faute de quoi la demande sera réputée abandonnée conformément à l'alinéa 73(1)f) de la Loi sur les brevets.

Une taxe additionnelle de six dollars (6$) par page excédant 100 pages du mémoire descriptif et dessins devra aussi être payée.

Le brevet sera délivré au nom du dernier propriétaire inscrit à nos dossiers à qui a fourni une documentation acceptable, au plus tard la date du paiement de la taxe finale, conformément à l'article 41 des Règles sur les brevets.

La réponse au présent avis doit comprendre l'identification complète de la demande et la date de l'avis.

La publication des brevets canadiens délivrés dans la Gazette du Bureau des brevets peut comprendre aussi une note concernant la mise en vente d'un brevet ou de sa licence. Si vous désirez profiter de ce service gratuit, veuillez l'indiquer au moment de payer la taxe finale.

L'OPIC valorise la rétroaction de ses clients et vous invite à remplir un sondage continu, court et anonyme, sur les produits et services relatifs aux brevets. Vous pouvez accéder au sondage au lien suivant : http://ic.sondages-surveys.ca/s/SCB-OPS/langfr-ca/

The above application for patent has been found allowable.

The final fee of THREE HUNDRED DOLLARS ($300), or ONE HUNDRED AND FIFTY DOLLARS ($150) where the applicant is entitled to claim small entity status and has submitted a small entity declaration, must be paid within six months following the date of this notice. Otherwise, the application will be deemed to be abandoned pursuant to paragraph 73(1)(f) of the Patent Act.

An additional fee of six dollars ($6.00) per page over 100 pages of specification and drawings must also be paid.

The patent shall issue to the last registered owner who has submitted acceptable documentation on or before the date that the final fee is paid (as pursuant to Section 41 of the Patent Rules).

A reply to this notice must include full identification of the application including the date of the notice.

The publication of issued Canadian patents in the Patent Office Record can also include an indication that the patent is available for licence or sale. If you wish to take advantage of this free service, please indicate this when paying the final fee.

CIPO values your feedback and invites you to complete a short and anonymous ongoing survey on patent examination products and services. You can access the survey at the following link : http://ic.sondages-surveys.ca/s/SCB-OPS/langeng

Commissaire aux brevets/Commissioner of Patents

Electronic Patent Application Fee Transmittal

Application Number:	13599647
Filing Date:	30-Aug-2012
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Filer:	John L. Adair/Stephanie Lee
Attorney Docket Number:	STAPP1100-5

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION INFORMATION DISCLOSURE STMT	2806	1	120	120
		Total in USD ($)		**120**

Electronic Acknowledgement Receipt	
EFS ID:	32490521
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Customer Number:	44654
Filer:	John L. Adair/Stephanie Lee
Filer Authorized By:	John L. Adair
Attorney Docket Number:	STAPP1100-5
Receipt Date:	30-APR-2018
Filing Date:	30-AUG-2012
Time Stamp:	17:27:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$120
RAM confirmation Number	050118INTEFSW00025453503183
Deposit Account	503183
Authorized User	Stephanie Lee
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		STAPP1100-5_IDS_04-30-18.pdf	277757 433e2d12c92ad49160baf574cf4cd4a3f3879b	yes	4

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	3
	Information Disclosure Statement (IDS) Form (SB08)	4	4

Warnings:					
Information:					
2	Non Patent Literature	STAPP1100_Ref_C22.pdf	1695952 70445b31b4cccc25197969485d53a9dd4b2c5b6c	no	1
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30646 7e2e6cc0bc827bcab51b4405334d5b3279f2c413e	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2004355		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. **STAPP1100-5**

First Named Inventor **C. Douglas Yeager**	
Application Number **13/599,647**	Date Filed **August 30, 2012**
Title **SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE**	
Group Art Unit **3695**	Examiner **Garrison T. Prinslow**
Confirmation Number **1919**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATION OF TRANSMISSION UNDER 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on April 30, 2018.

Stephanie Lee

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. A copy of foreign patent documents as well as the information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

☐ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☐ This Information Disclosure Statement is being submitted before the mailing of a first Office action on the merits; or

☐ This Information Disclosure Statement is being submitted before the mailing of a first Office action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(b) and before the mailing date of any of a Final Action under 37 C.F.R. § 1.113, a Notice of Allowance under 37 C.F.R. § 1.311, or an Action that otherwise closes prosecution in the application, and is accompanied by one of:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); or
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $120 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

☒ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(c) and on or before payment of the issue fee and is accompanied by:

- ☒ The statement specified in 37 C.F.R. § 1.97(e); and
- ☒ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $120 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

Pursuant to 37 C.F.R. § 1.97(e), Applicant hereby states:

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. § 1.56(c) more than three months prior to the filing of the information disclosure statement.

Pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application.

Applicant does not believe any fees are due and owing at this time. If Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

SPRINKLE IP LAW GROUP
Attorneys for Applicant

John L. Adair
Reg. No. 48,828

Dated: April 30, 2018

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 371-9088

PRINTER RUSH
(PTO ASSISTANCE)

Application: 13599647	Examiner: Prinslow	GAU: 3695
From: Denise Fisher	Location: RTFM	Creation Date: 05/01/2018

Week Date: 2/26/2018

DOC CODE	DOC DATE	MISCELLANEOUS
[ ] 1449		[ ] Continuing Data
[X] IDS	04/30/2018	[ ] Foreign Priority
[ ] CLM		[ ] Document Legibility
[ ] IIFW/FWCLM		[ ] Fees
[ ] SRFW		[ ] Petition (TC)
[ ] DRW		[ ] Other
[ ] OATH		
[ ] 312		
[ ] SPEC		

[RUSH] Message:

Please respond to the 04/30/18, IDS.

Thank You

DF

[XRUSH] Response:

Initials: _____

Examiner: PUBS contact - James Leija, (703) 756-1197
NOTE: This form will be included as part of the official USPTO record with the response document coded as XRUSH.
REV: AUG 16

Mastercard, Ex1002, p. 929

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
Comments on Statement of Reasons for Allowance	Atty. Docket No. **STAPP1100-5**

First Named Inventor **C. Douglas Yeager**	
Application No. **13/599,647**	Filing or 371 (c) Date **August 30, 2012**
Title **SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE**	
Group Art Unit **3695**	Examiner **Garrison T. Prinslow**
Confirmation No. **1919**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Certificate of Transmission Under 37 C.F.R. § 1.8

I hereby certify that this correspondence is being deposited electronically with the U.S. Patent and Trademark Office using the United States Patent and Trademark Office's EFS-Web system on May 2, 2016.

Shenise Ramdeen

Applicant appreciates the Examiner's allowance of Claims 30-42, 44-57 and 59-64 of United States Patent Application No. 13/599,647. Applicant submits the record as a whole makes evident the reasons for allowance and that there are additional reasons for patentability not enumerated by the Examiner. While Applicant agrees with the Examiner's reasons for patentability to the extent such reasons are consistent with the record as a whole, Applicant does not acquiesce or agree to any characterization of the claims that place unwarranted limitations or interpretations upon the claims, especially to the extent such limitations or interpretations are inconsistent with the claim language, specification or prior prosecution history in this case.

The Director of the U.S. Patent and Trademark Office is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

Sprinkle IP Law Group

John L. Adair
Reg. No. 48,828

Dated: May 2, 2016

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. 512-637-9220
Fax. 512-371-9088

Electronic Acknowledgement Receipt

EFS ID:	32543182
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Customer Number:	44654
Filer:	John L. Adair/Shenise Ramdeen
Filer Authorized By:	John L. Adair
Attorney Docket Number:	STAPP1100-5
Receipt Date:	07-MAY-2018
Filing Date:	30-AUG-2012
Time Stamp:	08:51:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Post Allowance Communication - Incoming	STAPP1100-5_CommentsonStatement05-07-18.pdf	74272 dba6e0800005990fcc4f32a60091cee2cfe4f876f	no	1

Warnings:

Information:	
Total Files Size (in bytes):	74272

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
REQUEST FOR CORRECTED FILING RECEIPT	Atty. Docket No. **STAPP1100-5**

First Named Inventor **C. Douglas Yeager**	
Application Number **13/599,647**	Filing or 371(c) Date **August 30, 2012**
Title **SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE**	
Group Art Unit **3695**	Confirmation No. **1919**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

CERTIFICATE OF TRANSMISSION UNDER 37 C.F.R. § 1.8

I hereby certify that this correspondence is being deposited electronically with the U.S. Patent and Trademark Office using the United States Patent and Trademark Office's EFS-Web system on May 31, 2018.

Shenise Ramdeen

Shenise Ramdeen

1. Attached is an annotated copy of the official filing receipt received from the PTO in the above application for which issuance of a corrected filing receipt is respectfully requested. An Updated Application Data Sheet is being filed concurrently herewith in support of this Request.

2. There is an error with respect to the following data, which is:

[X]	Incorrectly entered	and/or
[ ]	Omitted	

		Error in		***Correct data***
A.	[X]	Correspondence Address	A.	**Sprinkle IP Law Group, 1301 W. 25th Street, Suite 408, Austin, Texas 78748**
B.	[X]	Attorney Docket No.	B.	**STAPP1100-5**
C.	[X]	Title	C.	**Systems and Methods for Secure Application-Based Participation in an Interrogation by Mobile Device**
D.	[ ]	Applicant	D.	
E.	[X]	Customer No.	E.	**44654**

May 31, 2018
Date

John L. Adair
Reg. No.: 48,828

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE RECD	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/599,647	08/30/2012	2617	800	~~67979.112~~ STAPP3100-5	29	3

CONFIRMATION NO. 1919

~~408~~ 44654
~~LUEDEKA NEELY GROUP, P.C.~~ Sprinkle IP Law Group
~~P O BOX 1871~~ 1301 W. 25th Street, Suite 408
~~KNOXVILLE, TN 37901~~ Austin, TX 78705

FILING RECEIPT



Date Mailed: 09/18/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

C. Douglas YEAGER, Austin, TX;

Applicant(s)

C. Douglas YEAGER, Austin, TX;

Power of Attorney: The patent practitioners associated with Customer Number ~~000408~~ 44654

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/685,863 03/26/2012
and claims benefit of 61/573,476 09/06/2011
and claims benefit of 61/575,846 08/30/2011

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

Projected Publication Date: 02/28/2013

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****

Mastercard, Ex1002, p. 934

Title

~~SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM~~ SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE

Preliminary Class

455

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where

Mastercard, Ex1002, p. 935

the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PTO/SB/14 (11-08)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	67979.U2 STAPP1100-5
	Application Number	13/599,647
Title of Invention	~~SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM~~ Systems and Methods for Secure Application-Based Participation in an Interrogation by Mobile Device	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1 [Remove]

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Douglas	C.	Yeager	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Austin	State/Province	TX	Country of Residence i	US

Citizenship under 37 CFR 1.41(b) i: US

Mailing Address of Applicant:

Address 1	7502 West Rim Dr.		
Address 2			
City	Austin	State/Province	TX
Postal Code	78731	Country i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button. [Add]

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence information of this application.**

Customer Number	~~00400~~ 44654		
Email Address	~~JPalmer@NCYPatent.com~~ docketing@sprinklelaw.com	[Add Email]	[Remove Email]

Application Information:

Systems and Methods for Secure Application-Based Participation in an Interrogation by Mobile Device

Title of the Invention	~~SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM~~		
Attorney Docket Number	~~67979.U2~~ STAPP1100-5	Small Entity Status Claimed	X
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)		Suggested Figure for Publication (if any)	

PTO/SB/14 (11-08)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	~~67970-U2~~ STAPP1100-5
	Application Number	13/599,647
Title of Invention	SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION WITH AN UNEXPECTED CRYPTOGRAM	

Systems and Methods for Secure Application-Based Participation in an Interrogation by Mobile Device

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	~~88408~~ 44554		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61685863	2012-03-26
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61573476	2011-09-06
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61575846	2011-08-30

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button. Add

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

Application Number	Country	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			◉ Yes ○ No

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	STAPP1100-S
	Application Number	13/599,647
Title of Invention	Systems and Methods for Secure Application-Based Participation in an Interrogation by Mobile Device	

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[1] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country[1]	Filing Date (YYYY-MM-DD)	Access Code[1] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the Add button.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	STAPP1100-S
	Application Number	13/599,647
Title of Invention	Systems and Methods for Secure Application-Based Participation in an Interrogation by Mobile Device	

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◯ Assignee	◯ Legal Representative under 35 U.S.C. 117	◯ Joint Inventor
◯ Person to whom the inventor is obligated to assign.	◯ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :	
If the Applicant is an Organization check here. ☐	
Organization Name	

Mailing Address Information For Applicant:

Address 1			
Address 2			
City		**State/Province**	
Country[i]		Postal Code	
Phone Number		Fax Number	

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	STAPP1100-S
	Application Number	13/599,647
Title of Invention	Systems and Methods for Secure Application-Based Participation in an Interrogation by Mobile Device	

Email Address	

Additional Applicant Data may be generated within this form by selecting the Add button.

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Signature				Date (YYYY-MM-DD)	2015-05-30
First Name	John L.	Last Name	Adair	Registration Number	48,828

Additional Signature may be generated within this form by selecting the Add button.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	STAPP3100-5
	Application Number	13/599,647
Title of Invention	Systems and Methods for Secure Application-Based Participation in an Interrogation by Mobile Device	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Electronic Acknowledgement Receipt

EFS ID:	32774500
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Customer Number:	44654
Filer:	John L. Adair/Shenise Ramdeen
Filer Authorized By:	John L. Adair
Attorney Docket Number:	STAPP1100-5
Receipt Date:	31-MAY-2018
Filing Date:	30-AUG-2012
Time Stamp:	17:42:53
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		STAPP1100-5_RequestforCorrFR05-31-18.pdf	746780 f456135c8c44a6cce2089ab0e861826e45cd557ee	yes	10

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Request for Corrected Filing Receipt	1	4
	Application Data Sheet	5	10
Warnings:			
Information:			
	Total Files Size (in bytes):	746780	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
AMENDMENT UNDER 37 CFR 1.312	Atty. Docket No. (Opt.) **STAPP1100-5**

First Named Inventor: **C. Douglas Yeager**	
Application Number **13/599,647**	Filed **August 30, 2012**
For **SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE**	
Group Art Unit **3695**	Confirmation Number **1919**

Mail Stop: Issue Fee

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313

Dear Sir:

Certificate of Transmission Under 37 C.F.R. § 1.8

I hereby certify that this correspondence is being deposited electronically with the U.S. Patent and Trademark Office using the United States Patent and Trademark Office's EFS-Web system on **June 1, 2018.**

Janice Pampell
Janice Pampell

A Notice of Allowance and Fee(s) Due was issued by the Examiner on March 1, 2018. Applicant therefore respectfully requests that the Examiner enter the following amendment under 37 CFR 1.312. While Applicant understands that entry of an Amendment after the notice of allowance is a matter of discretion and not of right, Applicant respectfully requests that the Examiner consider and enter the following changes to the specification.

Amendments to the Claims begin on page 2.

Amendments to the Specification begin on page 10.

Remarks begin on page 32.

IN THE CLAIMS

Please amend the application as follows:

1-29 (Cancelled)

30. (Currently Amended) A method for secure application-based participation in a payment card transaction authorization process by a mobile device, the method comprising:

at a mobile device, executing an application in an operating system of the mobile device, the application interrogable by an electronic reader, over a first communications channel, for digital credential data corresponding to an account having a corresponding digital credential and configured to request, from a remote computer system hosting the corresponding digital credential, over a wireless network that is separate from the first communications channel, data associated with the account and generate cryptograms requested during interrogations over the first communications channel using the data associated with the account received from the remote computer system, wherein the application does not access a permanent cryptographic key issued for the digital credential during the interrogations;

requesting by the application, from the remote computer system, over the wireless network, a first set of data associated with the account;

receiving by the application, from the remote computer system, over the wireless network, the first set of data associated with the account, the first set of data associated with the account usable by the application to formulate ~~a first~~ an application protocol data unit response, the first set of data comprising a first non-permanent cryptographic key associated with the account;

locally storing the first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;

participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device comprising:

receiving at least one POS command communication sent by the POS terminal over the first communications channel, wherein the at least one POS command communication comprises a request for digital credential data to authorize a transaction against the account, the request for digital credential data including a cryptogram request;

generating a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram; and

responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to an electronic reader through the communication channel, the at least one device response communication comprising at least one response application data protocol unit containing the response cryptogram and an account identifier for the account;

subsequent to the interrogation, requesting by the application, from the remote computer system, over the wireless network, a second set of data associated with the account;

receiving by the application, from the remote computer system, over the wireless network, the second set of data associated with the account, the second set of data comprising a second non-permanent cryptographic key associated with the account; and

~~replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key as the local cryptographic key associated with the account prior to the application participating in a subsequent interrogation~~ storing the received second non-permanent cryptographic key as the local cryptographic key associated with the account to change the local cryptographic key associated with the account between at least two interrogations.

31. (Previously Presented) The method of Claim 30, wherein the mobile device is an NFC emulating device, wherein the first communications channel is an NFC communications channel and the first set of data associated with the account and the second set of data associated with the account are received via a data connection over the internet.

32. (Previously Presented) The method of Claim 30, wherein the response cryptogram is a hash.

33. (Previously Presented) The method of Claim 30, wherein the interrogation conforms to a card specification, the set of inputs is specified by the card specification and the at least one device response is formulated according to the card specification.

34. (Previously Presented) The method of Claim 33, wherein the request for digital credential data comprises a request for a first cryptogram according to the card specification and the at least one device response communication comprises a second cryptogram, wherein the second cryptogram is the response cryptogram.

35. (Previously Presented) The method of Claim 30, wherein generating the response cryptogram comprises encrypting the set of inputs using the local cryptographic key according to a digital encryption standard (DES) calculation to generate an output, wherein the response cryptogram includes a portion, but not all, of the output.

36. (Previously Presented) The method of Claim 30, wherein the mobile device does not have connectivity to the wireless network during the interrogation.

37. (Currently Amended) The method of Claim 30, further comprising, at the remote computer system:

prior to the interrogation, generating the first non-permanent cryptographic key at the remote computer system, associating the first non-permanent cryptographic key with the account, and sending the first non-permanent cryptographic key and the account identifier to the mobile device over the wireless network; and

after the interrogation, generating the second non-permanent cryptographic key at the remote computer system, associating the second non-permanent cryptographic key with the account and sending the second non-permanent cryptographic key and the account identifier to the mobile device over the wireless network.

38. (Previously Presented) The method of Claim 37, wherein the digital credential comprises a secure element representation maintained at the remote computer system.

39. (Previously Presented) The method of Claim 30, further comprising, at the remote computer system, performing an authorization process comprising:

receiving an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the response cryptogram and the account identifier;

determining a current non-permanent cryptographic key associated with the account using the account identifier;

calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account;

verifying a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram; and

sending an authorization response to the POS terminal, wherein the data contained in the authorization response is determined, at least in part, by the verifying the correctness of the response cryptogram.

40. (Previously Presented) The method of Claim 39, wherein:

the set of inputs comprises unpredictable data;

the authorization data comprises the unpredictable data; and

the calculated cryptogram is calculated using the unpredictable data.

41. (Previously Presented) The method of Claim 40, wherein the POS command communications comprise the unpredictable data.

42. (Previously Presented) The method of Claim 41, wherein the authorization data further comprises values from the transaction.

43. (Cancelled)

44. (Currently Amended) A system for secure application-based participation by a mobile device in point-of-sale interrogations, the system comprising:

a mobile device comprising:

a controller configured to route communications received over a communication channel from an electronic reader;

a wireless interface to connect to a wireless network that is separate from the communications channel;

a processor;

a computer readable storage medium accessible by the processor storing an application executable in an operating system of the mobile device, the application,

when executed, interrogable over the communications channel for digital credential data to authorize transactions against an account having a corresponding digital credential hosted at a remote computer system, wherein the application does not have access to a permanent cryptographic key issued for the digital credential and the application is executable to:

request from the remote computer system, over the wireless network, a first set of data associated with the account;

receive by the application, from the remote computer system, over the wireless network, the first set of data associated with the account, the first set of data associated with the account usable by the application to formulate ~~a first~~ an application protocol data unit response, the first set of data comprising a first non-permanent cryptographic key associated with the account;

store the first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;

during an interrogation:

receive at least one point-of-sale (POS) command communication sent by a POS terminal to the mobile device over the communications channel, wherein the at least one POS command communication comprises a request for digital credential data, the request for digital credential data including a cryptogram request;

access the ~~locally stored~~ local cryptographic key associated with the account;

generate a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram; and

respond to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response to the electronic reader through the communication channel, the at least one device response communication comprising at least one response application data protocol unit containing the response cryptogram and an account identifier for the account;

subsequent to the interrogation, request from the remote computer system, over the wireless network, a second set of data associated with the account;

receive by the application, from the remote computer system, over the wireless network, the second set of data associated with the account, the second set of data associated with the account comprising a second non-permanent cryptographic key associated with the account; and

store the received second non-permanent cryptographic key as the local ~~locally stored~~ cryptographic key associated with the account to change the ~~locally stored~~ local cryptographic key associated with the account between at least two interrogations.

45. (Previously Presented) The system of Claim 44, wherein the mobile device is an NFC emulating device, the first communication channel is an NFC channel, and the application is further executable to request and receive the first set of data associated with the account and the second set of data associated with the account via a data connection over the internet to the remote computer system.

46. (Previously Presented) The system of Claim 44, wherein the response cryptogram is a hash.

47. (Previously Presented) The system of Claim 44, wherein the interrogations conform to a card specification, the set of inputs is specified by the card specification and the at least one device response is formulated according to the card specification.

48. (Previously Presented) The system of Claim 47, wherein the request for digital credential data requests digital credential data comprising a first cryptogram and the at least one device response communication comprises a second cryptogram, wherein the second cryptogram is the response cryptogram.

49. (Previously Presented) The system of Claim 44, wherein generating the response cryptogram comprises encrypting the set of inputs using the local cryptographic key according to a digital encryption standard (DES) calculation to generate an output, wherein the response cryptogram includes a portion, but not all, of the output.

50. (Previously Presented) The system of Claim 44, wherein the mobile device does not have connectivity to the wireless network during the interrogation.

51. (Previously Presented) The system of Claim 44, wherein the mobile device is programmed to request a new non-permanent cryptographic key after the interrogation.

52. (Previously Presented) The system of Claim 44, further comprising the remote computer system, the remote computer system configured to generate non-permanent cryptographic keys associated with the account and send each of the non-permanent cryptographic keys and the account identifier to the mobile device over the wireless network.

53. (Previously Presented) The system of Claim 52, wherein the remote computer system is configured to maintain a secure element representation for the account, wherein the digital credential comprises the secure element representation.

54. (Previously Presented) The system of Claim 44, further comprising, a remote computer system programmed to:

receive an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the response cryptogram and the account identifier;

determine a current non-permanent cryptographic key associated with the account using the account identifier;

calculate a calculated cryptogram using the current non-permanent cryptographic key associated with the account;

verify a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram; and

send an authorization response to the POS terminal, wherein the data contained in the authorization response is determined, at least in part, by the verifying the correctness of the response cryptogram.

55. (Previously Presented) The system of Claim 54, wherein:

the set of inputs comprises unpredictable data;

the authorization data comprises the unpredictable data; and

the calculated cryptogram is calculated using the unpredictable data.

56. (Previously Presented) The system of Claim 55, wherein the POS command communications comprise the unpredictable data.

57. (Previously Presented) The system of Claim 55, wherein the authorization data further comprises values from the transaction.

58. (Cancelled)

59. (Previously Presented) The method of Claim 30, wherein the first non-permanent cryptographic key and second non-permanent cryptographic key are shared by a remote payment authorization process.

60. (Previously Presented) The system of Claim 44, wherein the first non-permanent cryptographic key and second non-permanent cryptographic key are shared by a remote payment authorization process.

61. (Previously Presented) The method of Claim 30, wherein the application is configured to generate the response cryptogram according to a card specification.

62. (Previously Presented) The system of Claim 44, wherein the application is executable to generate the responsive cryptogram according to a card specification.

63. (Previously Presented) The method of Claim 30, wherein the first and second non-permanent cryptographic key are associated with an issuer master key.

64. (Previously Presented) The system of Claim 44, wherein the first and second non-permanent cryptographic key are associated with an issuer master key.

IN THE SPECIFICATION

Please amend the Application as follows (references to paragraph/page numbers of the Application as filed):

Please replace paragraph [0011] with the following replacement paragraph:

[0011] Fig. 2 illustrates an embodiment of a command and response APDU flow between a reader and an SE with specific details about the MASTERCARD ~~PayPass~~ PAYPASS application that may be installed on the SE;

Please replace paragraph [0025] with the following replacement paragraph:

[0025] Fig. 16 illustrates an embodiment of an example of caching being used during a MASTERCARD ~~PayPass~~ PAYPASS transaction between a RFID POS and a remote SE;

Please replace paragraph [0026] with the following replacement paragraph:

[0026] Fig. 17 illustrates an embodiment of an example of 100% transaction caching being used during a VISA ~~PayWave~~ PAYWAVE transaction;

Please replace paragraph [0048] with the following replacement paragraph:

[0048] The APDU data typically are transmitted over the air on 13.56 MHz radio waves between the reader and the SE. There is no hardware requirement limitation on this process; the APDU commands are just data moving from one entity to another. Various embodiments disclosed herein use the standard APDU commands to interact with the SE regardless of whether the SE is the mobile device's own embedded SE, or is a remote SE embedded into a different mobile device or a card. Communications 1, 2, 3 and 4 show the sequential commands of a typical command and response between and SE and a reader. Usually multiple steps are involved with accessing a SE, which involves multiple APDU commands and responses. Fig. 1 shows the general interrogation steps to access digital credential data specifically for a MASTERCARD ~~PayPass~~ PAYPASS Mag Stripe application running on an SE, according to "Mag Stripe.pdf"

(Ver. 3.3) presently available at http://www.PayPass.com/approved-products.html. The term "digital credential data" as used herein refers to at least a portion of all data, including any data that are required to calculate the data, that are necessary to authorize approval of a transaction at a POS terminal.

Please replace paragraph [0049] with the following replacement paragraph:

[0049] Fig. 2 describes the detailed commands and responses expected when a reader interrogates a MASTERCARD ~~PayPass~~ PAYPASS Mag Stripe Ver. 3.3 application running on a SE. This sequence is provided in the MASTERCARD ~~PayPass~~ PAYPASS card specification. Shown in Fig. 2 are communications 5, 6, 7, 8 and 9 with details including abbreviations and acronyms explained subsequently herein.

Please replace paragraph [0050] with the following replacement paragraph:

[0050] Fig. 3 describes example transactions at the ISO/IEC 7816-4 Application Protocol Data Unit (APDU) protocol level between a reader and a card. The transaction processing depicted in Fig. 3 is representative of the MASTERCARD ~~PayPass~~ PAYPASS Mag Stripe application card specification v. 3.3. The notation ">CARD" denotes commands to the card and the notation "CARD>" denotes responses from the card. Communication 9 defines some of the initial parameters used in the transaction which include an unpredictable number issued by the reader, a transaction counter maintained on the SE. Communication 10 describes the command that the reader issues to the SE to find out what applications exist on the SE. This example shows that the MASTERCARD ~~PayPass~~ PAYPASS application responds as an active one. Next, communication 11 shows how the reader commands the SE to properly select the ~~PayPass~~ PAYPASS application for further processing. Communication 12 shows how the reader receives the type of processing options that the ~~PayPass~~ PAYPASS application supports. Communication 13 shows how the reader commands and then receives the ~~PayPass~~ PAYPASS application specific credential information about its card holder including card account number, holder name, expiration date, and more. Communication 14 shows how the reader receives the dynamic aspects of the transaction that will be inserted into the Track 1 and Track 2 data. This command uses a shared key on the SE, the unpredictable number from the reader, and the transaction counter on the SE to determine a new number sequence for each

transaction called a cryptogram. After the SE calculates the cryptogram, it sends it back to the reader in the response APDU. These data are obtained through the MASTERCARD ~~PayPass~~ PAYPASS card specification that was referenced earlier in this document. All details including abbreviations and acronyms are explained in detail through that card specification document

Please replace paragraph [0051] with the following replacement paragraph:

[0051] Fig. 4 describes how the reader 21 in Fig. 5 formats the response data received from the SE into accepted Track1 and Track2 data strings that are used in existing processing systems. Communication 15 shows a Track2 data string built from the card interrogation in Fig. 3. The CVC3 (Track2) UN and ATC numbers will all vary with each transaction or interrogation of the SE. Communication 16 shows a Track1 data string built from the card interrogation in figure 3. CVC3 (Track1), ATC, and UN numbers will all vary with each transaction or interrogation of the SE. These data are obtained through the MASTERCARD ~~PayPass~~ PAYPASS card specification that was referenced earlier herein. All details including abbreviations and acronyms are explained in detail through the cited MASTERCARD card specification document.

Please replace paragraph [0059] with the following replacement paragraph:

[0059] In the case where the SEs in an array of SEs are database secure element representations, a SE card reader is not needed to interrogate the SE representations. [[.]]In such systems the data may be acquired by using an electronic processor to translate the ISO 7816-4 protocol queries (commands) from the remote device into standard database queries and then translating the database responses into ISO 7816-4 responses for transmittal to the remote device. An array of SEs may include combinations of one or more types of secure element representations. That is, an array may include hardware representations and/or virtual hardware representations and/or database secure element representations.

Please replace paragraph [0063] with the following replacement paragraph:

[0063] Fig. 8 illustrates an embodiment of a repository 400 that employs a plurality of contact readers 404 operating under ISO 7816. A separate dedicated reader is provided for each of a plurality of secure element hardware representations 408. In the embodiment of Fig. 8 the secure

element hardware representations 408 are bank-issued cards containing a secure element chip that is accessible by a Universal Serial Bus (USB) connector, and the contact readers 404 are USB readers. A first portion 420 of a CPU 424 in a computer 428 is a multitasking data server to conduct a plurality of command/response time-wise overlapping sessions with the plurality of secure element hardware representations 408 through the plurality of contact readers 404. The USB standards typically limit the number of USB ports on a computer to 127 ports. A different bus architecture may be used to overcome that limitation, or a single USB reader may be configured to address multiple cards through electronic or even mechanical switching mechanisms. In the latter case the switching mechanism acts as a portion of a multitasking data server. In some embodiments (such as, for example, embodiments that employ contact readers as illustrated in the Fig. 8) a plurality of secure element representations may be disposed proximate to a secure element reader. As used herein the terms "proximate to" and "local" refers to a spatial condition where two devices are close to each other, but may not be adjacent to each other. For example, two devices that are in the same building (but not the same room) are considered to be proximate to each other. The term "proximate to" encompasses devices that are "adjacent to" each other.

Please replace paragraph [0069] with the following replacement paragraph:

[0069] It is important to note that at the ISO/IEC 7816-4 (APDU) level, an entire interrogation similar to those described in Fig. 1, and Fig. 2 may be carried out from a RFID POS reader 21 through an NFC enabled mobile device 626, through a data connection over the internet 35 to a remote system 631 that contains the actual SE 634. An example of reader commands is illustrated in element 638 as a ~~PayPass~~ PAYPASS reader. The ~~PayPass~~ PAYPASS reader 638 shows an exemplary sequence of ISO/IEC 7816-4 APDU commands and responses that may be pushed through the reader 21 and end up at the remote SE 634. Element 637 shows an example of APDU commands that are received by the remote SE 634 and the appropriate response that is issued as defined by the 7816-4 application for MASTERCARD ~~PayPass~~ PAYPASS. Elements 638 and 637 show how Figure 2 may be broken up so that the ~~PayPass~~ PAYPASS card may be hosted on a remote SE 634 on a remote system 631 and show that the ~~PayPass~~ PAYPASS reader may be an RFID POS 621.

Please replace paragraph [0083] with the following replacement paragraph:

[0083] With some data networks that pass TCP/UDP/IP information there are network delays and latencies that contribute to delays for round trip information exchange with a destination. With many embodiments disclosed herein, data are intended to go round-trip from a mobile device to a remote SE. Many payment applications that communicate with an SE may require a plurality of commands and responses to the SE for each transaction carried out by an interrogation from the POS RFID reader. Each or some of these command and responses to the SE may be subject to network delays and latency. Prolonged delays during a transaction with the RFID POS may cause an unsatisfactory user experience. Here is an example of a delay that was recorded during evaluation of an embodiment described herein:

a. Card transaction with a MASTERCARD ~~PayPass~~ PAYPASS plastic card and a RFID POS reader was measured to take ~200ms
b. Card transaction with a remote SE programmed with the MASTERCARD ~~PayPass~~ PAYPASS application over a 3G network managed by VERIZON ~~Verizon~~ through a mobile handset was measured to take ~600ms

Please replace paragraph [0086] with the following replacement paragraph:

[0086] Fig. 16 illustrates an example of caching being used during a MASTERCARD ~~PayPass~~ PAYPASS transaction between a RFID POS and a remote SE. The vertical line 778 represents the RFID POS entity. The vertical line 779 represents the mobile device. The vertical line 781 represents the remote system authentication server, and the vertical line 782 represents the remote hosted SE. The vertical line 780 represents the caching system in the mobile device.

Please replace paragraph [0087] with the following replacement paragraph:

[0087] The MASTERCARD ~~PayPass~~ PAYPASS card specification indicates that the response to the Select PPSE APDU 83 will always be the same:

a. APDU to the card for Select PPSE APDU:
   00 A4 04 00 0E 32 50 41 59 2E 53 59 53 2E 44 44 46
   30 31 00
b. APDU response from the card for Select PPSE APDU is ALWAYS:
   6F 23 84 0E 32 50 41 59 2E 53 59 53 2E 44 44 46 30

31 A5 11 BF 0C 0E 61 0C 4F 07 A0 00 00 00 04 10 10
87 01 01 90 00

Please replace paragraph [0088] with the following replacement paragraph:

[0088] The MASTERCARD ~~PayPass~~ PAYPASS card specification indicates that the response to the Select ~~PayPass~~ PAYPASS AID APDU 84 always be the same:

a. APDU to the card for Select ~~PayPass~~ PAYPASS AID APDU:
   00 A4 04 00 07 A0 00 00 00 04 10 10 00
b. APDU response from the card for Select AID APDU is ALWAYS:
   6F 17 84 07 A0 00 00 00 04 10 10 A5 0C 50 0A 4D 61
   73 74 65 72 43 61 72 64 90 00

This prescribed response to this APDU may also be cached and the caching system 780 may respond to this APDU without making a command all the way to the remote SE over the data network.

Please replace paragraph [0089] with the following replacement paragraph:

[0089] Furthermore, the MASTERCARD ~~PayPass~~ PAYPASS card specification indicates that the response to the GPO (Get Processing Options) APDU 785 always be the same:

a. APDU to the card for GPO APDU:
   80 A8 00 00 02 83 00 00
b. APDU response from the card for GPO APDU is ALWAYS:
   77 0A 82 02 00 00 94 04 08 01 01 00 90 00

Please replace paragraph [0090] with the following replacement paragraph:

[0090] The MASTERCARD ~~PayPass~~ PAYPASS card specification indicates that the response to the Read Record APDU 786 is to always be the same for a particular card that has been personalized, but will be different from personalized card to a different personalized card:

a. APDU to the card for Read Record APDU:

   00 B2 01 0C 00

b. APDU response from the card for Read Record APDU is ALWAYS for a specific card:

70	7F	9F	6C	02	00	01	56	3E	42	35	34	31	33	31	32	33
34	35	36	37	38	34	38	30	30	5E	53	55	50	50	4C	49	45
44	2F	4E	4F	54	5E	30	39	30	36	31	30	31	33	33	30	30
30	33	33	33	30	30	30	32	32	32	32	32	30	30	30	31	31
31	31	30	9F	64	01	03	9F	62	06	00	00	00	38	00	00	9F
63	06	00	00	00	00	E0	E0	9F	65	02	00	0E	9F	66	02	0E
70	9F	6B	13	54	13	12	34	56	78	48	00	D0	90	61	01	90
00	99	00	00	00	0F	9F	67	01	03	90	00					

This means that the response to this APDU may be cached and the caching system 780 may respond to this APDU without making a command all the way to the remote SE over the data network, UNLESS the card on the SE has changed to a different card, in which case the caching system should send this command to the remote SE for processing.

Please replace paragraph [0091] with the following replacement paragraph:

[0091] The MASTERCARD ~~PayPass~~ PAYPASS card specification indicates that the request and the response to the Compute Cryptographic Checksum APDU 787 will always be different for each transaction. This means that this APDU will always need to be processed by the actual remote SE through the data network. Communication 793 indicates the estimated or example of network processing time for this single APDU command and response 787. The over-all example in Fig. 16 illustrates how there is potentially only a single command and response that need to happen in real time over the data network 793 as a result of implementing a caching system.

Please replace paragraph [0093] with the following replacement paragraph:

[0093] Fig. 17 illustrates a slightly different caching concept using a VISA ~~payWave~~ PAYWAVE transaction as an example. In this figure, the entire transactional sequence with all APDU

commands and responses is cached at a separate time 802 prior to the actual transaction. In this example illustrated in Fig. 17, the RFID POS 794 does not initiate the initial request to the remote authentication server 797. Instead, it is initiated by the mobile device application at some prior time from the actual RFID POS transaction. When the mobile device 795 makes a request to the remote system authentication server 797, the remote system authentication server 797 either retrieves caching information from a database, or from making a request to a HSM (Hardware Security Module) or other storage system or, if needed, makes commands with a remote SE 799 as indicated by the dotted box in the figure with a read record request 800 to the remote SE 799. The remote SE 799 may be a hardware representation of a secure element or a software representation of a secure element. This example is particularly pertinent in the event that the response to the read record request 800 is dynamically changing data with each individual transaction with the SE. When all known responses to the remote SE transactional command(s) are gathered, the entire set of caching information may be passed back to the mobile device 795 as shown in communication 801. In communication 801 the SE responses to Select PPSE, Select ~~PayPass~~ PAYPASS, GPO, and Read Record APDU is passed back to the mobile device all at once.

Please replace paragraph [0096] with the following replacement paragraph:

[0096] The configuration of Fig. 18 closely represents an embodiment which employs secure element software representations where the secure element software representations are in the remote system authorization server 836. Much of the transaction scenario in Fig. 18 is identical to Fig. 23 including the time delay 838 (802 in Fig. 23) prior to the actual transaction 840 (803 in Fig. 23) and the delivery of the transactional data from the server 836 (801 in Fig. 23). This type of data substitution is possible with existing contactless APDU commands as defined in the VISA ~~payWave~~ PAYWAVE card specification. That card specification allows for a transaction with an RFID POS to be made using these commands:

a. Select AID: communication 11 Fig. 3
b. GPO: communication 12 Fig. 3
c. Read Record: communication 13 Fig. 3

Please replace paragraph [0097] with the following replacement paragraph:

[0097] The read record command for VISA ~~payWave~~ PAYWAVE indicates there may be 3 data elements with the tags:

a. Tag 57: Track 2 Equivalent Data
b. Tag 5F20: Cardholder Name
c. Tag 9F1F: Track 1 Discretionary Data

Please replace paragraph [00100] with the following replacement paragraph:

[00100] Extrapolating this concept displayed in Fig. 18 further, it is possible to substitute any Track 2 data into tag 57 of the read record APDU response. Some substitution examples are:

a. MASTERCARD data: 54 13 12 34 56 78 48 00 D0 90 61 01 90 94 99 89 92 50 3F
b. VISA data: 44 13 12 34 56 78 48 00 D0 90 61 01 90 94 99 89 92 50 3F
c. AMEX data: 34 13 12 34 56 78 48 00 D0 90 61 01 90 94 99 89 92 50 3F
d. Any propriety data format (MCDONALDS ARCH CARD~~Arch Card~~): 64 13 12 34 56 78 48 00 D0 90 61 01 90 94 99 89 92 50 3F

Please replace paragraph [00103] with the following replacement paragraph:

[00103] The right side of Fig. 19 shows a repository 157 where the function of the SE are handled as multiple software representations 154 (SE Emulation Instances) in a single computer or a bank of several computers. In this configuration, there is no separate hardware that is the SE. In the embodiment of Fig. 19[[.]], the functions of the SEs are provided as software representations depicted as SE Emulation Instances 154 that are established entirely in software and contained inside a Network Server 153. The communication format of APDU 7816-4 structure 155 may also be provided by the software of the Network Server 153. A general purpose computer or server typically has all the necessary components (such as ROM, RAM, Persistent Memory, and a processor) that are necessary to provide the SE software representations. The software architecture within the Network Server 153 may be arranged as such to divide and address many different SE software representations 154 within a single computer. In the same manner the hardware based SEs 147 are exposed to the Internet over TCP/UDP/IP, the software representations of the SEs 154 are also be exposed to the Internet.

Please replace paragraph [00106] with the following replacement paragraph:

[00106] Fig. 21 illustrates an arrangement of an application system 201 (a variant of remote system auth server) that contains a Hardware Security Module (HSM) 200. The application system also includes a system of one or more computers that all may have access to the transaction table 205 and the credential table 206 within the application system. The application system contains data that should be kept in a secure manner and as a result may have both network accessibility and physical accessibility limitations built in to it. The application system can be further detailed as a "software representation" of a plurality of secure element representations as the application system has access to all the information used to create APDU responses for any particular SE representation in its repository data. An added feature of the application system that extend its capabilities beyond a "software representation" of a plurality of secure element representations is that because it has access to the HSM that stores keys used to create the data in each SE representation, it can be configured for authorizing or verifying the output data (digital credential data) for any of the SEs contained in its repository data as well. An HSM is a device commonly used in the banking and processing industry. The HSM is responsible for securely containing encryption keys 203 (cryptographic keys) that are used to authorize card payments, or create digital credential data for new cards. Encryption algorithms 204 that use these keys are also contained on the HSM. An example of an HSM used in the industry at the time of this filing is currently distributed by SafeNet Inc. and is named the ~~Luna~~ LUNA EFT Mark II Edition. An example, from the MASTERCARD ~~PayPass~~ PAYPASS MSD v3.3 card specification document, of an encryption key that may be stored on the HSM is called an Issuer Master Key (IMK). The HSM can then, for example, use the embedded algorithms 204 to create a "diversified key for card verification code creation" (KDcvc3) from the IMK that is used for each individual card that is issued based on a certain algorithm that is also stored in the HSM. The HSM is designed to protect individual encryption keys, and to use embedded encryption algorithms to calculate encryption output based on an encryption input request from an application system. The encryption algorithm must be located within the HSM because the algorithm must have direct access to the protected encryption keys 203. The application system will provide additional input data to be used in the encryption algorithms to the HSM. The application system will also expect output data from the encryption algorithms from the HSM. The input data to the HSM may be stored in the transaction table 205 and the credential table 206. An HSM is commonly a separate device within the application system that

is connected to other devices within the application system through a communication channel. The communication channel may be a network connection such as an RJ45 cable or in some cases is a hardware bus connection such as a PCI connector within a computer casing. An example of using this arrangement may be that the application system contains:

a. Encrypted data (cryptogram)
b. Unpredictable number (UN)
c. Application Transaction Counter (ATC)
d. Transaction data such as a dollar amount
e. A key identifier (but the not key itself)

in its transaction table and credential table. The application system would like to verify encrypted data (a) was created from a particular encryption key (e), unpredictable number (b), ATC (c), and transaction data (d). The application system knows which key was used to create the cryptogram (a), but opts, for security reasons, not to have access to the key itself. The application system then uses the cryptogram (a), unpredictable number (b), ATC (c), transaction data (d), and a key identifier (e) as input for the HSM and sends the input to the HSM. The HSM then uses the input data from the application system and locates the proper encryption algorithm and encryption key to use. The HSM then creates the output response from the algorithm using the encryption key and sends the output to the application system. The output in this example would be a simple "verified" or "not verified" message.

Please replace paragraph [00108] with the following replacement paragraph:

[00108] Examples of SE responses are shown in Fig. 3 next to the 'CARD>:' prompt indicating data from the SE to the point-of-sale. The application system may know the specific responses based on a number of factors. In figure 3, the responses are for a ~~PayPass~~ PAYPASS 3.3 MSD transaction, because the application system knows the particular card id or PAN is associated to this ~~PayPass~~ PAYPASS 3.3 MSD transaction, and the ~~PayPass~~ PAYPASS card specification for 3.3 MSD dictates specifically elements 10, 11, and 12 exactly as shown in figure 3, so the response APDU data as shown in 10, 11, and 12 can be sent verbatim over a communication channel to the mobile device cache when requested by the mobile device.

Please replace paragraph [00109] with the following replacement paragraph:

[00109] Figure 3, element 13 after the 'CARD>:' prompt shows the format of the read record command response, but the data inside the response may change from one card id or PAN to another because it is credential data that is stored in the read record command response. Fortunately the application system has access to all the credential data that comprises the response to the read record command such as displayed, in part in figure 2, element 7:

a. Track 1 and Track 2 data comprised of PAN, Exp Date, card code, issuer discretionary data
b. Substitution bitmaps for Track 1 and Track 2 (PUNATC, PCVC3)
c. Number of ATC digits used in bitmaps (NATC)
d. Application Version Number

From this data, the application system can create the proper APDU response to the read record command that is formatted just like figure 3, element 13 and send it specifically for the card credential the mobile device has requested to the mobile device for caching over a communication channel. For a MASTERCARD ~~PayPass~~ PAYPASS MSD v. 3.3 credential, table 2 shows a technical breakdown of how the data in the read record response is formulated from data in the application system in proper APDU response BER-TLV format.

Please replace paragraph [00110] with the following replacement paragraph:

[00110] As used herein the term "cryptogram" refers to encrypted data that may or may not be able to be un-encrypted. Encrypted data that cannot be un-encrypted is many times called a "hash." A cryptogram is typically calculated from a series of input data that comprises some data and a cryptographic key, where the cryptographic key is used to encrypt some data. As used herein the term "cryptographic key" refers to a key used, at least in part, to calculate a cryptogram. A cryptogram is calculated based on an algorithm or calculation formula. As use herein the term "calculation formula" refers to an algorithm or formula that is specified by a card specification as the method to calculate a cryptogram. A calculation formula typically may be known by any entity. The output result of the calculation formula that uses the input data and a cryptographic key is a cryptogram. Examples of cryptograms at the time of this filing are defined by the following card specifications in table 4.

Table 4

Card specification	Cryptogram Designator or Name
MASTERCARD ~~PayPass~~ PAYPASS MSD	CVC3
VISA Contactless MSD	dCVV
DISCOVER ZIP MSD	dCVV
EMV, VISA QVSDC, VISA VSDC, MASTERCARD MCHIP	AC, TC, AAC, ARQC

A "cryptogram" as used herein may be classified as "dynamic" meaning that it is always changing from one interrogation (transaction) to the next over the life a digital credential (SE representation). As used herein the term "life of", as in, the life of a digital credential, the life of a card, the life of a SE, the life of a SE representation, refers to the life beginning when it is used its first interrogation and ending when it is used in its last interrogation. One indication of this dynamic aspect of a cryptogram is to perform two sequential independent interrogations between a mobile device and a point-of-sale terminal where the same digital credential is used on the mobile device, and the point-of-sale terminal receives two sets of digital credential data with each including a single cryptogram, one with each interrogation. If the cryptogram received by the point-of-sale terminal is different from one interrogation to the next, it is dynamic.

Please replace paragraph [00111] with the following replacement paragraph:

[00111] The details of an interrogation between a point-of-sale and a digital credential, card, SE representation, and mobile device are defined in "card specifications" and implemented in point-of-sale terminals. Examples of these card specifications at the time of this filing are MASTERCARD ~~PayPass~~ PAYPASS --Mag Stripe v3.3, Contactless EMV, DISCOVER NETWORK ~~Network~~ RF Contactless Specification--Supplement Guide For Functional Support, AMEX ALIS v1.7, and VISA Contactless Payment Specification v2.0.2. As used herein the term "card specification" refers to a specification or reference within the specification to other specifications and so on that a point-of-sale terminal must adhere to in order to interrogate a card, SE, mobile device as expected by that card specification. A point-of-sale terminal, as the interrogator, controls the interrogation. The card specification that defines the details of an interrogation may also define the details of a cryptogram request, calculation, and delivery from

the card, SE, or mobile device to the point-of-sale as part of the interrogation sequence. Card specifications may include references to other specifications and those other specifications to even more specification wherein the card specification may be defined by the card specification in conjunction with other supporting documents sited within a card specification. Card specifications typically consist of an application layer that defines an interrogation sequence and calculations that are to be performed by both the card, SE, mobile device and also the interrogator or point-of-sale. Both a mobile device and a point-of-sale are expected to be operating under the direction of a card specification during an interrogation.

Please replace paragraph [00116] with the following replacement paragraph:

[00116] As used herein the terms "transient," "transiently stored," "non-persistent," and "non-persistently stored" refers to data that are stored in a storage container where [[the]] they are erased or otherwise rendered not accessible after a power failure to the storage container. An example of a transient storage container is RAM (Random Access Memory).

Please replace paragraph [00122] with the following replacement paragraph:

[00122] The response for the compute cryptographic checksum command (figure 3, element 14), is created by a method employed in figures 22, 23, 24, 25, 26, 27, 28, 29 and 30 called "Cryptogram Substitution" using a predetermined cryptogram or unpredictable cryptogram and in some embodiments sent for each transaction to the mobile device cache over a communication channel when requested by the mobile device. In other embodiments cryptogram substitution is used with unexpected cryptograms created on the mobile device and sent to a remote application system. For a MASTERCARD ~~PayPass~~ PAYPASS MSD v. 3.3 credential, table 3 shows a technical breakdown of how the data in the read compute cryptographic checksum response is formulated from data in the application system in proper APDU response BER-TLV format.

Table 3

77 0F		
T	L	V
9F 61	02	B8 92 T2_CVC3
9F 60	02	FB C7 T1_CVC3
9F 36	02	00 5E ATC
90 00		

The ATC is the automated transaction counter that increments with every point-of-sale interrogation, and can be stored in the transaction table or credential table and updated with each interrogation by a mobile device. The CVC3 is cryptogram that is expected to be calculated with this algorithm from the MASTERCARD ~~PayPass~~ PAYPASS MSD v3.3 card specification:

First KDcvc3 is created:

$Z_L := DES3(IMK_{CVC3})[Y]$

$Z_R := DES3(IMK_{CVC3})[Y \oplus$ ('FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF')]

and define:

$KD_{CVC3} := (Z_L || Z_R)$.

KDcvc3 calculation may be performed inside the HSM because the HSM contains IMK. The application system will pass Y, which is defined as the PAN and PAN sequence number concatenated as an input to the HSM in conjunction with the IMK id to use. The HSM will respond back with the KDcvc3 as output. The KDcvc3 in this example would be considered a permanent cryptographic key because it will not change over the life of the digital credential, as none of the inputs to the calculation of KDcvc3 change over the life of the credential.

Next T2_IVCVC3 is created:

O:=PayPass-MagStripe(3.3) Annex B alg(KDcvc3)[Track 2 Data]

The least two significant bytes of the output data are defined to be T2_IVCVC3.

Finally, the CVC3 cryptogram for track 2 is calculated:

$O:=DES3(KD_{CVC3})$

$O:=DES3(KD_{CVC3})[T2\_IVcvc3||UN||ATC]$

The least two significant bytes of the output data are defined to be CVC3.

CVC3 calculation may be performed inside the HSM because the HSM contains the IMK which is used to create KDcvc3, which is used to create IVCVC and CVC3. So the application system will pass UN and ATC as inputs in conjunction with the IMK id to use. The HSM will respond back with the CVC3 cryptogram as output. The CVC3 is a dynamic cryptogram as the input to the calculation of the cryptogram change with each interrogation. This is known because with each interrogation the digital credential is expected to increment the ATC (Automated Transaction Counter) and also have different UN value.

Please replace paragraph [00131] with the following replacement paragraph:

[00131] Fig. 16 illustrates a caching system for each transaction or interrogation between a point-of-sale 778 and a mobile device 779 for a MASTERCARD ~~PayPass~~ PAYPASS transaction. The advantage of caching secure element responses is to lessen the effect of network latency and speed up an interrogation. In the example contained Fig. 16, network latency is reduced from a potential 800ms to a potential 200ms because of the caching technique applied. This is a significant effect in the application of NFC or RFID because the as the total interrogation timeframe shrinks, the likelihood of a successful interrogation sequence goes up because it is less likely the communication channel between the point-of-sale and the mobile device will be interrupted from the mobile device moving out of the field generated by the point-of-sale. Notice that not all interrogation command and responses 787 and 793 in Fig. 16 are handled from the mobile device cache 780. The non-cached command and response, lead to the 200ms network latency of the entire transaction in figure 16.'

Please replace paragraph [00133] with the following replacement paragraph:

[00133] Depending on the interrogation sequence selected by the point-of-sale, it may not

always be possible to implement a system set forth in Fig. 17. Many point-of-sale interrogation sequences carried out at the time of this filing are based on card specifications such as:

a. MASTERCARD, ~~PayPass~~ PAYPASS, MChip
b. AMERICAN EXPRESS, EXPRESS PAY ~~Express Pay~~
c. DISCOVER ZIP [[Zip]]
d. VISA QVSDC, VSDC
e. Contactless EMV

Employ a method of creating an expected cryptogram by the mobile device that is calculated, at least in part, from unpredictable data generated on the point-of-sale and delivered to the mobile device during the interrogation sequence. Because creating an expected cryptogram requires a calculation to be performed that includes a permanent cryptographic key, the secure element or system with access to this key must be used to carry out the expected cryptogram calculation. Because the secure element representation is stored in a remote repository and contains the permanent cryptographic key, this expected cryptogram calculation would incur network latency to perform the calculation during the interrogation, as shown in figure 16, element 793.

Please please replace paragraph [00138] with the following replacement paragraph:

[00138] Fig. 22 illustrates how one embodiment of an application system could create cryptograms using random, predetermined, or "made up" input data. A transaction table 210 is defined in which each row represents a transaction between a mobile device and a point-of-sale. The state of the data in this table currently shows transaction data that have been delivered to a mobile device cache, but have not been verified through a point-of-sale. In order to comply with the request of a point-of-sale to a mobile device during an interrogation, the mobile device must deliver cryptogram in the proper data format that the point-of-sale expects. The data that is contained in the actual cryptogram that is delivered to the point-of-sale from the mobile device may not be accurately calculated with the input data from the point-of-sale, but it does not matter at this point as the point-of-sale alone does not verify the cryptogram, it simply receives the cryptogram and relays it for verification to the application system, which has access to the input data used to create the original pre-determined cryptogram. This is why the predetermined cryptogram 218 can [[may]] be calculated based on randomly selected terminal input data UN 213, and Transaction Data 215. The other inputs to create the predetermined cryptogram are based on credential data of each secure element such as the Application

Transaction Counter 214, the Issuer Master Key id 212, and the account Personal Account Number 211. After gathering all predetermined cryptogram input data, the application system sends the input to the HSM and receives the predetermined cryptogram as an output response. The application system may optionally store the predetermined cryptogram 218 into the table 210, for use during verification later.

Please replace paragraph [00142] with the following replacement paragraph:

[00142] These methods of substituting a predetermined cryptogram and of substituting an unpredictable cryptogram are vital to the concept of 100% transaction caching with the existing point-of-sale infrastructure. The existing point-of-sale infrastructure is pre-set for each interrogation sequence and expects data to be formatted according to each interrogation sequence that is programmed in the point-of-sale. Changing the interrogation sequence(s) is out of the control of the mobile device, and so this method of creating a predetermined cryptogram or unpredictable cryptogram as defined using data, at least in part, from Fig. 22 may be required for 100% transaction caching which creates no network latency during the interrogation between the point-of-sale and the mobile device. Because the predetermined cryptogram is created without input from the point-of-sale, the calculation time to create a predetermined cryptogram may also <u>be</u> removed from the overall interrogation time. In the case of an unpredictable cryptogram, this calculation time persists and cannot be removed from the overall interrogation time.

Please replace paragraph [00143] with the following replacement paragraph:

[00143] Fig. 29 illustrates a representation of a table of digital credentials 350 (digital credential data) that may be stored inside the application system. This table, in conjunction with the transaction table, and in some embodiments the HSM allows the application system to perform as a repository of a plurality of secure element software representations. The credential data used to create data inside an SE and also allow it to formulate its proper APDU responses is contained in this table for a plurality of credentials (SEs). For a MASTERCARD ~~PayPass~~ <u>PAYPASS</u> MSD v3.3 credential, the example shown in this table, the columns of data list personal account number (PAN) 351, expiration date 352, name of card holder 353, card code 354, track 1 data 355, track 2 data 356, track 1 cvc3 bitmap 357, track 2 cvc3 bitmap 358, track 1

UN and ATC bitmaps 359, track 2 UN and ATC bitmaps 360, track 1 number of ATC digits 361, track 2 number of ATC digits 362, CVM list 363, AC 364, application version number 365, and the master key identifier 366.

Please replace paragraph [00145] with the following replacement paragraph:

[00145] For an example, the MASTERCARD ~~PayPass~~ PAYPASS interrogation from the point of sale incorporates an APDU command request called "compute cryptographic checksum" 14 as seen in Fig. 3. The command APDU follows a particular format and may look like this:

80 2A 8E 80 04 00 00 08 99 00

The digits 00 00 08 99 in the APDU command above from the point-of-sale indicate the unpredictable number to be used as an expected cryptogram calculation input. This unpredictable number is a random sequence of numbers that changes with each interrogation the point-of-sale initiates. The format of this APDU command request is discussed in more detail inside the MASTERCARD ~~PayPass~~ PAYPASS MSD v3.3 card specification. The immediate APDU response from the mobile device is expected to follow a particular format and may look like this:

77 0F 9F 61 02 B8 92 9F 60 02 FB C7 9F 36 02 00 5E 90 00

The digits B8 92 represent the cryptogram. It is identified by the preceding BER-TLV formatted tag 9F 61 (track 2 CVC3), and length value of 02. It was expected to have been calculated from the unpredictable number issued by the preceding point-of-sale APDU command request in combination with other inputs such as the ATC. A correct expected cryptogram must be calculated using the permanent cryptographic key that is securely stored inside the SE. Because figure 23 implements 100% transaction caching, it is not impossible for the expected cryptogram to be calculated after receiving the unpredictable number from the point-of-sale, because in that event, the mobile device would need to access the network to contact the remote repository as in figure 16, elements 787 and 793 in order to perform the expected cryptogram calculation. The method of substituting a predetermining a cryptogram, or an unpredictable cryptogram in place of the expected cryptogram, in this case, needs to be applied in order to create this response. With

this method applied, the "compute cryptographic checksum" response from the mobile device can be successfully delivered interrogation with the point-of-sale without contacting the remote SE representation during the interrogation. In this case, the cached response may look like this instead:

77 0F 9F 61 02 A4 56 9F 60 02 FB C7 9F 36 02 00 5E 90 00

Where, in one embodiment, the digits A4 56 is the predetermined cryptogram, and NOT calculated using, at least in part, the expected unpredictable number from point-of-sale. Where, in another embodiment, the digits A4 56 is the unpredictable cryptogram, and NOT calculated, at least in part, using the expected permanent cryptographic key rather using a temporary cryptographic. This is an example of "Cryptogram Substitution" technique. The point-of-sale does not have the means or keys to check the received cryptogram for correctness, so it will accept the cryptogram answer because it is of the proper format. The point-of-sale will rely on the authorization request later to verify the correctness of the cryptogram.

Please replace paragraph [00169] with the following replacement paragraph:

[00169] As used herein "sending data" from one entity to another such as a mobile device to a remote application system or ~~vise~~ vice versa should be taken to mean sending the data from one location to another wherein the receiving entity may receive the data as a duplicate from the sending entity or receive the data in parts in addition to receiving information about the data that would enable the receiving entity to reconstruct the original data that was sent from the sending entity.

Please replace paragraph [00181] with the following replacement paragraph:

[00181] In a further embodiment, the verification process could be verification of an unpredictable cryptogram using a temporary cryptographic key assigned to the transaction in the transaction table to calculate and verify the unpredictable ~~crytptogram~~ cryptogram.

Please replace paragraph [00207] with the following replacement paragraph:

[00207] In some embodiments disclosed herein, a specific payment standard issued from MASTERCARD International. This standard is based on reference documentation published by ~~PayPass~~ PAYPASS --Mag Stripe (V3.3).pdf and other derivations. In this card specification, ~~PayPass~~ PAYPASS contactless payment card reader and card interrogation is documented. This document discusses specifically how an RFID reader interrogator would interact with a card containing a SE to extract and build Track1/Track2 equivalent data that is compatible for existing processing infrastructure, but contains the more secure and dynamic aspects of SE driven credential data.

Please replace paragraph [00224] with the following replacement paragraph:

[00224] Some embodiments disclosed herein combine both the tasks performed by the NFC mobile device and the remote system to allow for a complete and un-interrupted interrogation between a RFID POS reader or remote terminal and an NFC mobile device. The interrogation may be performed as set forth by payment card standards such as MASTERCARD ~~PayPass~~ PAYPASS, VISA Contactless, AMEX ~~Express Pay~~ EXPRESS PAY, DISCOVER ZIP [[Zip]], and contactless EMV.

Please replace paragraph [00226] with the following replacement paragraph:

[00226] Some advantages of various embodiments include:

a. In the event a mobile device that is used to conduct an NFC payment transaction with an RFID terminal is lost or stolen, the remote system may be notified and communication with the SE may be blocked until the stolen or lost device is recovered or replaced. In the event the device is replaced, new card credentials do not have to be issued again, but a communication channel with the SE may be opened back up and continued upon proper authorization. Prior to this invention, all new SE credentials or cards would have to be re-issued as the hardware that contained the SE itself would have been lost or stolen also.
b. The SE that is associated with a remote mobile device may be switched to another mobile device fast and easily and is not hardware form factor ~~dependant~~ dependent. The same SE may be used with multiple mobile devices, laptop or desktop computers that have the ability to connect to this

remote system that contains the SE over a data connection and authenticate properly.

c. Compared to changing hardware interfaces, and array of different hardware interfaces, and supported hardware interfaces on a mobile device, a data connection is ubiquitous and standard. SE's currently have various hardware form factors such as:

    i. Embedded microchip (soldered to a circuit board)
    ii. SD, mini-SD, micro-SD interface
    iii. USB interface
    iv. SIM card interface

    Many mobile devices support different sets of the above hardware form factors and many support none of them at all, however, most all mobile devices support a data connection. This ubiquity aids to the portability of SE applications from device to device.

d. Because some embodiments contain an array of SEs or SE representations, and because the remote system is designed to host and connect SE applications to multiple remote devices, it is possible for multiple remote devices from separate remote device owners to share a single SE from the array of SEs in the remote system. This sort of sharing of space on the SE enables consolidation and ultimately savings by more efficient utilization of memory on an array of SEs.

e. Because some embodiments do not rely on a hardware specific interface for the SE, but a data connection only. It is a more ubiquitous interface and may be used with more devices without being modified or changed from a hardware perspective.

f. Because some embodiments use an array or plurality of SEs, the ability to purchase SE chips in quantity for use in this array brings a possibility of a lower over-all cost per SE chip.

REMARKS

Applicant appreciates the time taken by the Examiner to review the present amendment.

Interview Summary

On May 30, 2018, Primary Examiner Robinson and the undersigned participated in a telephonic interview to discuss amending claims 30 and 44 to change "a first application data protocol unit response" to "an application protocol data unit response" and amending the last portion of claim 30 to be consistent with the last portion of allowed claim 44. Primary Examiner Robinson agreed the amendments to claims 30 and 44 appeared to be proper subject matter for an amendment under 37 C.F.R. § 1.312.

Claims

Claims 30 and 44 are amended to change "a first application data protocol unit response" to "an application protocol data unit response." Claim 44 is amended to change "the locally stored cryptographic key associated with the account" to recite "the local cryptographic key associated with the account" consistent with the prior recitation of "a local cryptographic key associated with the account." Claim 37 is amended for grammar.

The last portion of Claim 30 is amended for consistency with the last portion of allowed claim 44. Applicant respectfully submits that, according to the Reasons of Allowability provided by the Examiner, the Examiner would have found amended claim 30 to be similarly allowable. *See* Notice of Allowability at 3-4.

Specification

In reviewing the above-identified application for issuance, the Specification is amended to correct typographical errors and further identify trademarks or tradenames.

Conclusion

Applicant respectfully submits that the amendments do not add new matter. Applicant therefore respectfully requests entry of the amendment.

The Commissioner is hereby authorized to charge any deficiencies or credit any overpayment to Deposit Account No. 50-3183.

Respectfully submitted,

Sprinkle IP Law Group

John L. Adair
Reg. No. 48,828

Dated: June 1, 2018

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. 512-637-9220
Fax. 512-371-9088

Electronic Patent Application Fee Transmittal

Application Number:	13599647
Filing Date:	30-Aug-2012
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Filer:	John L. Adair/Janice Pampell
Attorney Docket Number:	STAPP1100-5

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	2501	1	500	500

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**500**

Electronic Acknowledgement Receipt	
EFS ID:	32784136
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Customer Number:	44654
Filer:	John L. Adair/Janice Pampell
Filer Authorized By:	John L. Adair
Attorney Docket Number:	STAPP1100-5
Receipt Date:	01-JUN-2018
Filing Date:	30-AUG-2012
Time Stamp:	15:39:07
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$500
RAM confirmation Number	060418INTEFSW00002185503183
Deposit Account	503183
Authorized User	Janice Pampell
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	STAPP1100-5_Transmittal_of_Payment_of_Issue_Fee.pdf	555757 0cc5c951bca50df055b003132ce6b3849 0999e	no	1
Warnings:					
Information:					
2	Issue Fee Payment (PTO 85B)	STAPP1100 5_PTOL 85.pdf	1017029 3fac13dc03d2cf80a72045b07077211af54f8 764	no	1
Warnings:					
Information:					
3	Amendment after Notice of Allowance (Rule 312)	STAPP1100-5 Amendment Under_312.pdf	2254387 4ee7ce3d4d56a5565901ca80d1a74c94aaf8 52c8	no	33
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30507 df5a1ad0a6d071627b07e9d249c589c6a1ab 902b	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	3857680		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

TRANSMITTAL OF PAYMENT OF ISSUE FEE (Small Entity) 37 C.F.R. 1.311	Docket No. STAPP1100-5

First Named Inventor: **C. Douglas YEAGER**

Application No.	Filing Date	Examiner	Group Art Unit	Confirmation No.
13/599,647	08/30/2012	Prinflow, Garrison T.	3695	1919

Title:

Secure Application-Based Participation in an Interrogation by Mobile Device

Mail Stop: Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Transmitted herewith are the following items in reference to the above-identified application:

- ☒ Issue Fee Transmittal Form PTOL-85
- ☒ Issue Fee: $500
- ☒ Amendment Under 1.312
- ☒ The Director is hereby authorized to charge Deposit Account No. 50-3183 of Sprinkle IP Law Group.
- ☒ The Director is hereby authorized to charge any deficiencies or credit any overpayments to Deposit Account No. 50-3183 of Sprinkle IP Law Group.

John L. Adair
Reg. No. 48,828

Customer No. 109422
Sprinkle IP Law Group
1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 371-9088

Certificate of Transmission Under 37 C.F.R. § 1.8

I hereby certify that this correspondence and items referenced herein are being deposited electronically with the U.S. Patent and Trademark Office using the United States Patent and Trademark Office's EFS-Web system on Oct 18

Janice Pampell

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax **(571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

44654 7590 03/01/2018
Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

n/a. Filed EFS.	(Depositor's name)
	(Signature)
	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/599,647	08/30/2012	C. Douglas YEAGER	STAPP1100-5	1919

TITLE OF INVENTION: SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500	$0	$0	$500	06/01/2018

EXAMINER	ART UNIT	CLASS-SUBCLASS
PRINSLOW, GARRISON T	3695	705-071000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47, Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 Sprinkle IP Law Group
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)
PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: SimplyTapp, Inc.
(B) RESIDENCE: (CITY and STATE OR COUNTRY): Austin, TX

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
- ☒ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number: 503183 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ☐ Applicant certifying micro entity status. See 37 CFR 1.29
- ☐ Applicant asserting small entity status. See 37 CFR 1.27
- ☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature: /John L. Adair/ Date: May 31, 2018
Typed or printed name: John L. Adair Registration No.: 48,828

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Mastercard, Ex1002, p. 984

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/599,647	08/30/2012	3695	960	STAPP1100-5	29	3

CONFIRMATION NO. 1919

CORRECTED FILING RECEIPT

44654
Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705

Date Mailed: 06/04/2018

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

C. Douglas YEAGER, Austin, TX;

Applicant(s)

C. Douglas YEAGER, Austin, TX;

Power of Attorney: The patent practitioners associated with Customer Number 44654

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/685,863 03/26/2012
and claims benefit of 61/573,476 09/06/2011
and claims benefit of 61/575,846 08/30/2011

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: No

Permission to Access Search Results: No

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 06/04/2018

Mastercard, Ex1002, p. 985

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/599,647**

Projected Publication Date: Not Applicable

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****
Title

SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE

Preliminary Class

705

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

Mastercard, Ex1002, p. 986

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PRINTER RUSH
(PTO ASSISTANCE)

Application: 13599647	Examiner: PRINSLOW	GAU: 3695
From: Natarsha Horne	Location: RTFM	Creation Date: 06/04/2018

Week Date: 2/26/2018

DOC CODE	DOC DATE	MISCELLANEOUS
[ ] 1449		[ ] Continuing Data
[ ] IDS		[ ] Foreign Priority
[ ] CLM		[ ] Document Legibility
[ ] IIFW/FWCLM		[ ] Fees
[ ] SRFW		[ ] Petition (TC)
[ ] DRW		[ ] Other
[ ] OATH		
[X] 312	06/01/2018	
[ ] SPEC		

[RUSH] Message:

Please respond to the 6/1/2018, A.NA

Thank You
NYH

[XRUSH] Response:

Initials: _____

Examiner: PUBS contact - James Leija, (703) 756-1197
NOTE: This form will be included as part of the official USPTO record with the response document coded as XRUSH.
REV: AUG 16

Mastercard, Ex1002, p. 988

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/599,647	08/30/2012	C. Douglas YEAGER	STAPP1100-5	1919

44654 7590 06/05/2018

Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TEXAS 78705
UNITED STATES OF AMERICA

EXAMINER	
ROBINSON, KITO R	

ART UNIT	PAPER NUMBER
3695	

MAIL DATE	DELIVERY MODE
06/05/2018	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR/ PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
13/599,647	08/30/2012	YEAGER, C. Douglas	STAPP1100-5

	EXAMINER	
Sprinkle IP Law Group 1301 W. 25th Street Suite 408 Austin, TX 78705	KITO R ROBINSON	
	ART UNIT	PAPER
	3695	20180604

DATE MAILED: 04 June 2018

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

This communication is in reference to the 312 amendments submitted on June 01, 20118. The amendments have been reviewed in its entirety and does not affect patentability.

/KITO R ROBINSON/
Primary Examiner, Art Unit 3695

PTO-90C (Rev.04-03)

Response to Rule 312 Communication	Application No.	Applicant(s)	
	13/599,647	YEAGER, C. Douglas	
	Examiner	Art Unit	AIA Status
	KITO R ROBINSON	3695	No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

1. ☑ The amendment filed on 01 June 2018 under 37 CFR 1.312 has been considered, and has been:

a) ☑ entered.

b) ☐ entered as directed to matters of form not affecting the scope of the invention.

c) ☐ disapproved because the amendment was filed after the payment of the issue fee.
Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.

d) ☐ disapproved. See explanation below.

e) ☐ entered in part. See explanation below.

/KITO R ROBINSON/
Primary Examiner, Art Unit 3695

Mastercard, Ex1002, p. 991

OK TO ENTER: /K.R.R/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
AMENDMENT UNDER 37 CFR 1.312	Atty. Docket No. (Opt.) **STAPP1100-5**
First Named Inventor: **C. Douglas Yeager**	
Application Number **13/599,647**	Filed **August 30, 2012**
For **SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE**	
Group Art Unit **3695**	Confirmation Number **1919**

Mail Stop: Issue Fee

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313

Dear Sir:

Certificate of Transmission Under 37 C.F.R. § 1.8

I hereby certify that this correspondence is being deposited electronically with the U.S. Patent and Trademark Office using the United States Patent and Trademark Office's EFS-Web system on **June 1, 2018.**

Janice Pampell
Janice Pampell

A Notice of Allowance and Fee(s) Due was issued by the Examiner on March 1, 2018. Applicant therefore respectfully requests that the Examiner enter the following amendment under 37 CFR 1.312. While Applicant understands that entry of an Amendment after the notice of allowance is a matter of discretion and not of right, Applicant respectfully requests that the Examiner consider and enter the following changes to the specification.

Amendments to the Claims begin on page 2.

Amendments to the Specification begin on page 10.

Remarks begin on page 32.

IN THE CLAIMS

Please amend the application as follows:

1-29 (Cancelled)

30. (Currently Amended) A method for secure application-based participation in a payment card transaction authorization process by a mobile device, the method comprising:

at a mobile device, executing an application in an operating system of the mobile device, the application interrogable by an electronic reader, over a first communications channel, for digital credential data corresponding to an account having a corresponding digital credential and configured to request, from a remote computer system hosting the corresponding digital credential, over a wireless network that is separate from the first communications channel, data associated with the account and generate cryptograms requested during interrogations over the first communications channel using the data associated with the account received from the remote computer system, wherein the application does not access a permanent cryptographic key issued for the digital credential during the interrogations;

requesting by the application, from the remote computer system, over the wireless network, a first set of data associated with the account;

receiving by the application, from the remote computer system, over the wireless network, the first set of data associated with the account, the first set of data associated with the account usable by the application to formulate ~~a first~~ an application protocol data unit response, the first set of data comprising a first non-permanent cryptographic key associated with the account;

locally storing the first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;

participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device comprising:

receiving at least one POS command communication sent by the POS terminal over the first communications channel, wherein the at least one POS command communication comprises a request for digital credential data to authorize a transaction against the account, the request for digital credential data including a cryptogram request;

generating a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram; and

responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to an electronic reader through the communication channel, the at least one device response communication comprising at least one response application data protocol unit containing the response cryptogram and an account identifier for the account;

subsequent to the interrogation, requesting by the application, from the remote computer system, over the wireless network, a second set of data associated with the account;

receiving by the application, from the remote computer system, over the wireless network, the second set of data associated with the account, the second set of data comprising a second non-permanent cryptographic key associated with the account; and

~~replacing the first non-permanent cryptographic key with the second non-permanent cryptographic key as the local cryptographic key associated with the account prior to the application participating in a subsequent interrogation~~ storing the received second non-permanent cryptographic key as the local cryptographic key associated with the account to change the local cryptographic key associated with the account between at least two interrogations.

31. (Previously Presented) The method of Claim 30, wherein the mobile device is an NFC emulating device, wherein the first communications channel is an NFC communications channel and the first set of data associated with the account and the second set of data associated with the account are received via a data connection over the internet.

32. (Previously Presented) The method of Claim 30, wherein the response cryptogram is a hash.

33. (Previously Presented) The method of Claim 30, wherein the interrogation conforms to a card specification, the set of inputs is specified by the card specification and the at least one device response is formulated according to the card specification.

34. (Previously Presented) The method of Claim 33, wherein the request for digital credential data comprises a request for a first cryptogram according to the card specification and the at least one device response communication comprises a second cryptogram, wherein the second cryptogram is the response cryptogram.

35. (Previously Presented) The method of Claim 30, wherein generating the response cryptogram comprises encrypting the set of inputs using the local cryptographic key according to a digital encryption standard (DES) calculation to generate an output, wherein the response cryptogram includes a portion, but not all, of the output.

36. (Previously Presented) The method of Claim 30, wherein the mobile device does not have connectivity to the wireless network during the interrogation.

37. (Currently Amended) The method of Claim 30, further comprising, at the remote computer system:

prior to the interrogation, generating the first non-permanent cryptographic key at the remote computer system, associating the first non-permanent cryptographic key with the account, and sending the first non-permanent cryptographic key and the account identifier to the mobile device over the wireless network; and

after the interrogation, generating the second non-permanent cryptographic key at the remote computer system, associating the second non-permanent cryptographic key with the account and sending the second non-permanent cryptographic key and the account identifier to the mobile device over the wireless network.

38. (Previously Presented) The method of Claim 37, wherein the digital credential comprises a secure element representation maintained at the remote computer system.

39. (Previously Presented) The method of Claim 30, further comprising, at the remote computer system, performing an authorization process comprising:

receiving an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the response cryptogram and the account identifier;

determining a current non-permanent cryptographic key associated with the account using the account identifier;

calculating a calculated cryptogram using the current non-permanent cryptographic key associated with the account;

verifying a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram; and

sending an authorization response to the POS terminal, wherein the data contained in the authorization response is determined, at least in part, by the verifying the correctness of the response cryptogram.

40. (Previously Presented) The method of Claim 39, wherein:

the set of inputs comprises unpredictable data;

the authorization data comprises the unpredictable data; and

the calculated cryptogram is calculated using the unpredictable data.

41. (Previously Presented) The method of Claim 40, wherein the POS command communications comprise the unpredictable data.

42. (Previously Presented) The method of Claim 41, wherein the authorization data further comprises values from the transaction.

43. (Cancelled)

44. (Currently Amended) A system for secure application-based participation by a mobile device in point-of-sale interrogations, the system comprising:

a mobile device comprising:

a controller configured to route communications received over a communication channel from an electronic reader;

a wireless interface to connect to a wireless network that is separate from the communications channel;

a processor;

a computer readable storage medium accessible by the processor storing an application executable in an operating system of the mobile device, the application,

when executed, interrogable over the communications channel for digital credential data to authorize transactions against an account having a corresponding digital credential hosted at a remote computer system, wherein the application does not have access to a permanent cryptographic key issued for the digital credential and the application is executable to:

request from the remote computer system, over the wireless network, a first set of data associated with the account;

receive by the application, from the remote computer system, over the wireless network, the first set of data associated with the account, the first set of data associated with the account usable by the application to formulate ~~a first~~ an application protocol data unit response, the first set of data comprising a first non-permanent cryptographic key associated with the account;

store the first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;

during an interrogation:

receive at least one point-of-sale (POS) command communication sent by a POS terminal to the mobile device over the communications channel, wherein the at least one POS command communication comprises a request for digital credential data, the request for digital credential data including a cryptogram request;

access the ~~locally stored~~ local cryptographic key associated with the account;

generate a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram; and

respond to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response to the electronic reader through the communication channel, the at least one device response communication comprising at least one response application data protocol unit containing the response cryptogram and an account identifier for the account;

subsequent to the interrogation, request from the remote computer system, over the wireless network, a second set of data associated with the account;

receive by the application, from the remote computer system, over the wireless network, the second set of data associated with the account, the second set of data associated with the account comprising a second non-permanent cryptographic key associated with the account; and

store the received second non-permanent cryptographic key as the local ~~locally stored~~ cryptographic key associated with the account to change the ~~locally stored~~ local cryptographic key associated with the account between at least two interrogations.

45. (Previously Presented) The system of Claim 44, wherein the mobile device is an NFC emulating device, the first communication channel is an NFC channel, and the application is further executable to request and receive the first set of data associated with the account and the second set of data associated with the account via a data connection over the internet to the remote computer system.

46. (Previously Presented) The system of Claim 44, wherein the response cryptogram is a hash.

47. (Previously Presented) The system of Claim 44, wherein the interrogations conform to a card specification, the set of inputs is specified by the card specification and the at least one device response is formulated according to the card specification.

48. (Previously Presented) The system of Claim 47, wherein the request for digital credential data requests digital credential data comprising a first cryptogram and the at least one device response communication comprises a second cryptogram, wherein the second cryptogram is the response cryptogram.

49. (Previously Presented) The system of Claim 44, wherein generating the response cryptogram comprises encrypting the set of inputs using the local cryptographic key according to a digital encryption standard (DES) calculation to generate an output, wherein the response cryptogram includes a portion, but not all, of the output.

50. (Previously Presented) The system of Claim 44, wherein the mobile device does not have connectivity to the wireless network during the interrogation.

51. (Previously Presented) The system of Claim 44, wherein the mobile device is programmed to request a new non-permanent cryptographic key after the interrogation.

52. (Previously Presented) The system of Claim 44, further comprising the remote computer system, the remote computer system configured to generate non-permanent cryptographic keys associated with the account and send each of the non-permanent cryptographic keys and the account identifier to the mobile device over the wireless network.

53. (Previously Presented) The system of Claim 52, wherein the remote computer system is configured to maintain a secure element representation for the account, wherein the digital credential comprises the secure element representation.

54. (Previously Presented) The system of Claim 44, further comprising, a remote computer system programmed to:

receive an authorization request to authorize the transaction from the POS terminal, the authorization request comprising authorization data, wherein the authorization data comprises the response cryptogram and the account identifier;

determine a current non-permanent cryptographic key associated with the account using the account identifier;

calculate a calculated cryptogram using the current non-permanent cryptographic key associated with the account;

verify a correctness of the response cryptogram by comparing the calculated cryptogram with the response cryptogram; and

send an authorization response to the POS terminal, wherein the data contained in the authorization response is determined, at least in part, by the verifying the correctness of the response cryptogram.

55. (Previously Presented) The system of Claim 54, wherein:

the set of inputs comprises unpredictable data;

the authorization data comprises the unpredictable data; and

the calculated cryptogram is calculated using the unpredictable data.

56. (Previously Presented) The system of Claim 55, wherein the POS command communications comprise the unpredictable data.

57. (Previously Presented) The system of Claim 55, wherein the authorization data further comprises values from the transaction.

58. (Cancelled)

59. (Previously Presented) The method of Claim 30, wherein the first non-permanent cryptographic key and second non-permanent cryptographic key are shared by a remote payment authorization process.

60. (Previously Presented) The system of Claim 44, wherein the first non-permanent cryptographic key and second non-permanent cryptographic key are shared by a remote payment authorization process.

61. (Previously Presented) The method of Claim 30, wherein the application is configured to generate the response cryptogram according to a card specification.

62. (Previously Presented) The system of Claim 44, wherein the application is executable to generate the responsive cryptogram according to a card specification.

63. (Previously Presented) The method of Claim 30, wherein the first and second non-permanent cryptographic key are associated with an issuer master key.

64. (Previously Presented) The system of Claim 44, wherein the first and second non-permanent cryptographic key are associated with an issuer master key.

IN THE SPECIFICATION

Please amend the Application as follows (references to paragraph/page numbers of the Application as filed):

Please replace paragraph [0011] with the following replacement paragraph:

[0011] Fig. 2 illustrates an embodiment of a command and response APDU flow between a reader and an SE with specific details about the MASTERCARD ~~PayPass~~ PAYPASS application that may be installed on the SE;

Please replace paragraph [0025] with the following replacement paragraph:

[0025] Fig. 16 illustrates an embodiment of an example of caching being used during a MASTERCARD ~~PayPass~~ PAYPASS transaction between a RFID POS and a remote SE;

Please replace paragraph [0026] with the following replacement paragraph:

[0026] Fig. 17 illustrates an embodiment of an example of 100% transaction caching being used during a VISA ~~PayWave~~ PAYWAVE transaction;

Please replace paragraph [0048] with the following replacement paragraph:

[0048] The APDU data typically are transmitted over the air on 13.56 MHz radio waves between the reader and the SE. There is no hardware requirement limitation on this process; the APDU commands are just data moving from one entity to another. Various embodiments disclosed herein use the standard APDU commands to interact with the SE regardless of whether the SE is the mobile device's own embedded SE, or is a remote SE embedded into a different mobile device or a card. Communications 1, 2, 3 and 4 show the sequential commands of a typical command and response between and SE and a reader. Usually multiple steps are involved with accessing a SE, which involves multiple APDU commands and responses. Fig. 1 shows the general interrogation steps to access digital credential data specifically for a MASTERCARD ~~PayPass~~ PAYPASS Mag Stripe application running on an SE, according to "Mag Stripe.pdf"

(Ver. 3.3) presently available at http://www.PayPass.com/approved-products.html. The term "digital credential data" as used herein refers to at least a portion of all data, including any data that are required to calculate the data, that are necessary to authorize approval of a transaction at a POS terminal.

Please replace paragraph [0049] with the following replacement paragraph:

[0049] Fig. 2 describes the detailed commands and responses expected when a reader interrogates a MASTERCARD ~~PayPass~~ PAYPASS Mag Stripe Ver. 3.3 application running on a SE. This sequence is provided in the MASTERCARD ~~PayPass~~ PAYPASS card specification. Shown in Fig. 2 are communications 5, 6, 7, 8 and 9 with details including abbreviations and acronyms explained subsequently herein.

Please replace paragraph [0050] with the following replacement paragraph:

[0050] Fig. 3 describes example transactions at the ISO/IEC 7816-4 Application Protocol Data Unit (APDU) protocol level between a reader and a card. The transaction processing depicted in Fig. 3 is representative of the MASTERCARD ~~PayPass~~ PAYPASS Mag Stripe application card specification v. 3.3. The notation ">CARD" denotes commands to the card and the notation "CARD>" denotes responses from the card. Communication 9 defines some of the initial parameters used in the transaction which include an unpredictable number issued by the reader, a transaction counter maintained on the SE. Communication 10 describes the command that the reader issues to the SE to find out what applications exist on the SE. This example shows that the MASTERCARD ~~PayPass~~ PAYPASS application responds as an active one. Next, communication 11 shows how the reader commands the SE to properly select the ~~PayPass~~ PAYPASS application for further processing. Communication 12 shows how the reader receives the type of processing options that the ~~PayPass~~ PAYPASS application supports. Communication 13 shows how the reader commands and then receives the ~~PayPass~~ PAYPASS application specific credential information about its card holder including card account number, holder name, expiration date, and more. Communication 14 shows how the reader receives the dynamic aspects of the transaction that will be inserted into the Track 1 and Track 2 data. This command uses a shared key on the SE, the unpredictable number from the reader, and the transaction counter on the SE to determine a new number sequence for each

transaction called a cryptogram. After the SE calculates the cryptogram, it sends it back to the reader in the response APDU. These data are obtained through the MASTERCARD ~~PayPass~~ PAYPASS card specification that was referenced earlier in this document. All details including abbreviations and acronyms are explained in detail through that card specification document

Please replace paragraph [0051] with the following replacement paragraph:

[0051] Fig. 4 describes how the reader 21 in Fig. 5 formats the response data received from the SE into accepted Track1 and Track2 data strings that are used in existing processing systems. Communication 15 shows a Track2 data string built from the card interrogation in Fig. 3. The CVC3 (Track2) UN and ATC numbers will all vary with each transaction or interrogation of the SE. Communication 16 shows a Track1 data string built from the card interrogation in figure 3. CVC3 (Track1), ATC, and UN numbers will all vary with each transaction or interrogation of the SE. These data are obtained through the MASTERCARD ~~PayPass~~ PAYPASS card specification that was referenced earlier herein. All details including abbreviations and acronyms are explained in detail through the cited MASTERCARD card specification document.

Please replace paragraph [0059] with the following replacement paragraph:

[0059] In the case where the SEs in an array of SEs are database secure element representations, a SE card reader is not needed to interrogate the SE representations. [[.]]In such systems the data may be acquired by using an electronic processor to translate the ISO 7816-4 protocol queries (commands) from the remote device into standard database queries and then translating the database responses into ISO 7816-4 responses for transmittal to the remote device. An array of SEs may include combinations of one or more types of secure element representations. That is, an array may include hardware representations and/or virtual hardware representations and/or database secure element representations.

Please replace paragraph [0063] with the following replacement paragraph:

[0063] Fig. 8 illustrates an embodiment of a repository 400 that employs a plurality of contact readers 404 operating under ISO 7816. A separate dedicated reader is provided for each of a plurality of secure element hardware representations 408. In the embodiment of Fig. 8 the secure

element hardware representations 408 are bank-issued cards containing a secure element chip that is accessible by a Universal Serial Bus (USB) connector, and the contact readers 404 are USB readers. A first portion 420 of a CPU 424 in a computer 428 is a multitasking data server to conduct a plurality of command/response time-wise overlapping sessions with the plurality of secure element hardware representations 408 through the plurality of contact readers 404. The USB standards typically limit the number of USB ports on a computer to 127 ports. A different bus architecture may be used to overcome that limitation, or a single USB reader may be configured to address multiple cards through electronic or even mechanical switching mechanisms. In the latter case the switching mechanism acts as a portion of a multitasking data server. In some embodiments (such as, for example, embodiments that employ contact readers as illustrated in the Fig. 8) a plurality of secure element representations may be disposed proximate to a secure element reader. As used herein the terms "proximate to" and "local" refers to a spatial condition where two devices are close to each other, but may not be adjacent to each other. For example, two devices that are in the same building (but not the same room) are considered to be proximate to each other. The term "proximate to" encompasses devices that are "adjacent to" each other.

Please replace paragraph [0069] with the following replacement paragraph:

[0069] It is important to note that at the ISO/IEC 7816-4 (APDU) level, an entire interrogation similar to those described in Fig. 1, and Fig. 2 may be carried out from a RFID POS reader 21 through an NFC enabled mobile device 626, through a data connection over the internet 35 to a remote system 631 that contains the actual SE 634. An example of reader commands is illustrated in element 638 as a ~~PayPass~~ PAYPASS reader. The ~~PayPass~~ PAYPASS reader 638 shows an exemplary sequence of ISO/IEC 7816-4 APDU commands and responses that may be pushed through the reader 21 and end up at the remote SE 634. Element 637 shows an example of APDU commands that are received by the remote SE 634 and the appropriate response that is issued as defined by the 7816-4 application for MASTERCARD ~~PayPass~~ PAYPASS. Elements 638 and 637 show how Figure 2 may be broken up so that the ~~PayPass~~ PAYPASS card may be hosted on a remote SE 634 on a remote system 631 and show that the ~~PayPass~~ PAYPASS reader may be an RFID POS 621.

Please replace paragraph [0083] with the following replacement paragraph:

[0083] With some data networks that pass TCP/UDP/IP information there are network delays and latencies that contribute to delays for round trip information exchange with a destination. With many embodiments disclosed herein, data are intended to go round-trip from a mobile device to a remote SE. Many payment applications that communicate with an SE may require a plurality of commands and responses to the SE for each transaction carried out by an interrogation from the POS RFID reader. Each or some of these command and responses to the SE may be subject to network delays and latency. Prolonged delays during a transaction with the RFID POS may cause an unsatisfactory user experience. Here is an example of a delay that was recorded during evaluation of an embodiment described herein:

a. Card transaction with a MASTERCARD ~~PayPass~~ PAYPASS plastic card and a RFID POS reader was measured to take ~200ms
b. Card transaction with a remote SE programmed with the MASTERCARD ~~PayPass~~ PAYPASS application over a 3G network managed by VERIZON ~~Verizon~~ through a mobile handset was measured to take ~600ms

Please replace paragraph [0086] with the following replacement paragraph:

[0086] Fig. 16 illustrates an example of caching being used during a MASTERCARD ~~PayPass~~ PAYPASS transaction between a RFID POS and a remote SE. The vertical line 778 represents the RFID POS entity. The vertical line 779 represents the mobile device. The vertical line 781 represents the remote system authentication server, and the vertical line 782 represents the remote hosted SE. The vertical line 780 represents the caching system in the mobile device.

Please replace paragraph [0087] with the following replacement paragraph:

[0087] The MASTERCARD ~~PayPass~~ PAYPASS card specification indicates that the response to the Select PPSE APDU 83 will always be the same:

a. APDU to the card for Select PPSE APDU:
   00 A4 04 00 0E 32 50 41 59 2E 53 59 53 2E 44 44 46
   30 31 00
b. APDU response from the card for Select PPSE APDU is ALWAYS:
   6F 23 84 0E 32 50 41 59 2E 53 59 53 2E 44 44 46 30

31 A5 11 BF 0C 0E 61 0C 4F 07 A0 00 00 00 04 10 10
87 01 01 90 00

Please replace paragraph [0088] with the following replacement paragraph:

[0088] The MASTERCARD ~~PayPass~~ PAYPASS card specification indicates that the response to the Select ~~PayPass~~ PAYPASS AID APDU 84 always be the same:

a. APDU to the card for Select ~~PayPass~~ PAYPASS AID APDU:
   00 A4 04 00 07 A0 00 00 00 04 10 10 00
b. APDU response from the card for Select AID APDU is ALWAYS:
   6F 17 84 07 A0 00 00 00 04 10 10 A5 0C 50 0A 4D 61
   73 74 65 72 43 61 72 64 90 00

This prescribed response to this APDU may also be cached and the caching system 780 may respond to this APDU without making a command all the way to the remote SE over the data network.

Please replace paragraph [0089] with the following replacement paragraph:

[0089] Furthermore, the MASTERCARD ~~PayPass~~ PAYPASS card specification indicates that the response to the GPO (Get Processing Options) APDU 785 always be the same:

a. APDU to the card for GPO APDU:
   80 A8 00 00 02 83 00 00
b. APDU response from the card for GPO APDU is ALWAYS:
   77 0A 82 02 00 00 94 04 08 01 01 00 90 00

Please replace paragraph [0090] with the following replacement paragraph:

[0090] The MASTERCARD ~~PayPass~~ PAYPASS card specification indicates that the response to the Read Record APDU 786 is to always be the same for a particular card that has been personalized, but will be different from personalized card to a different personalized card:

a. APDU to the card for Read Record APDU:

   00 B2 01 0C 00

b. APDU response from the card for Read Record APDU is ALWAYS for a specific card:

70	7F	9F	6C	02	00	01	56	3E	42	35	34	31	33	31	32	33
34	35	36	37	38	34	38	30	30	5E	53	55	50	50	4C	49	45
44	2F	4E	4F	54	5E	30	39	30	36	31	30	31	33	33	30	30
30	33	33	33	30	30	30	32	32	32	32	32	30	30	30	31	31
31	31	30	9F	64	01	03	9F	62	06	00	00	00	38	00	00	9F
63	06	00	00	00	00	E0	E0	9F	65	02	00	0E	9F	66	02	0E
70	9F	6B	13	54	13	12	34	56	78	48	00	D0	90	61	01	90
00	99	00	00	00	0F	9F	67	01	03	90	00					

This means that the response to this APDU may be cached and the caching system 780 may respond to this APDU without making a command all the way to the remote SE over the data network, UNLESS the card on the SE has changed to a different card, in which case the caching system should send this command to the remote SE for processing.

Please replace paragraph [0091] with the following replacement paragraph:

[0091] The MASTERCARD ~~PayPass~~ PAYPASS card specification indicates that the request and the response to the Compute Cryptographic Checksum APDU 787 will always be different for each transaction. This means that this APDU will always need to be processed by the actual remote SE through the data network. Communication 793 indicates the estimated or example of network processing time for this single APDU command and response 787. The over-all example in Fig. 16 illustrates how there is potentially only a single command and response that need to happen in real time over the data network 793 as a result of implementing a caching system.

Please replace paragraph [0093] with the following replacement paragraph:

[0093] Fig. 17 illustrates a slightly different caching concept using a VISA ~~payWave~~ PAYWAVE transaction as an example. In this figure, the entire transactional sequence with all APDU

commands and responses is cached at a separate time 802 prior to the actual transaction. In this example illustrated in Fig. 17, the RFID POS 794 does not initiate the initial request to the remote authentication server 797. Instead, it is initiated by the mobile device application at some prior time from the actual RFID POS transaction. When the mobile device 795 makes a request to the remote system authentication server 797, the remote system authentication server 797 either retrieves caching information from a database, or from making a request to a HSM (Hardware Security Module) or other storage system or, if needed, makes commands with a remote SE 799 as indicated by the dotted box in the figure with a read record request 800 to the remote SE 799. The remote SE 799 may be a hardware representation of a secure element or a software representation of a secure element. This example is particularly pertinent in the event that the response to the read record request 800 is dynamically changing data with each individual transaction with the SE. When all known responses to the remote SE transactional command(s) are gathered, the entire set of caching information may be passed back to the mobile device 795 as shown in communication 801. In communication 801 the SE responses to Select PPSE, Select ~~PayPass~~ PAYPASS, GPO, and Read Record APDU is passed back to the mobile device all at once.

Please replace paragraph [0096] with the following replacement paragraph:

[0096] The configuration of Fig. 18 closely represents an embodiment which employs secure element software representations where the secure element software representations are in the remote system authorization server 836. Much of the transaction scenario in Fig. 18 is identical to Fig. 23 including the time delay 838 (802 in Fig. 23) prior to the actual transaction 840 (803 in Fig. 23) and the delivery of the transactional data from the server 836 (801 in Fig. 23). This type of data substitution is possible with existing contactless APDU commands as defined in the VISA ~~payWave~~ PAYWAVE card specification. That card specification allows for a transaction with an RFID POS to be made using these commands:

a. Select AID: communication 11 Fig. 3
b. GPO: communication 12 Fig. 3
c. Read Record: communication 13 Fig. 3

Please replace paragraph [0097] with the following replacement paragraph:

[0097] The read record command for VISA ~~payWave~~ PAYWAVE indicates there may be 3 data elements with the tags:

a. Tag 57: Track 2 Equivalent Data
b. Tag 5F20: Cardholder Name
c. Tag 9F1F: Track 1 Discretionary Data

Please replace paragraph [00100] with the following replacement paragraph:

[00100] Extrapolating this concept displayed in Fig. 18 further, it is possible to substitute any Track 2 data into tag 57 of the read record APDU response. Some substitution examples are:

a. MASTERCARD data: 54 13 12 34 56 78 48 00 D0 90 61 01 90 94 99 89 92 50 3F
b. VISA data: 44 13 12 34 56 78 48 00 D0 90 61 01 90 94 99 89 92 50 3F
c. AMEX data: 34 13 12 34 56 78 48 00 D0 90 61 01 90 94 99 89 92 50 3F
d. Any propriety data format (MCDONALDS ARCH CARD~~Arch Card~~): 64 13 12 34 56 78 48 00 D0 90 61 01 90 94 99 89 92 50 3F

Please replace paragraph [00103] with the following replacement paragraph:

[00103] The right side of Fig. 19 shows a repository 157 where the function of the SE are handled as multiple software representations 154 (SE Emulation Instances) in a single computer or a bank of several computers. In this configuration, there is no separate hardware that is the SE. In the embodiment of Fig. 19[[.]], the functions of the SEs are provided as software representations depicted as SE Emulation Instances 154 that are established entirely in software and contained inside a Network Server 153. The communication format of APDU 7816-4 structure 155 may also be provided by the software of the Network Server 153. A general purpose computer or server typically has all the necessary components (such as ROM, RAM, Persistent Memory, and a processor) that are necessary to provide the SE software representations. The software architecture within the Network Server 153 may be arranged as such to divide and address many different SE software representations 154 within a single computer. In the same manner the hardware based SEs 147 are exposed to the Internet over TCP/UDP/IP, the software representations of the SEs 154 are also be exposed to the Internet.

Please replace paragraph [00106] with the following replacement paragraph:

[00106] Fig. 21 illustrates an arrangement of an application system 201 (a variant of remote system auth server) that contains a Hardware Security Module (HSM) 200. The application system also includes a system of one or more computers that all may have access to the transaction table 205 and the credential table 206 within the application system. The application system contains data that should be kept in a secure manner and as a result may have both network accessibility and physical accessibility limitations built in to it. The application system can be further detailed as a "software representation" of a plurality of secure element representations as the application system has access to all the information used to create APDU responses for any particular SE representation in its repository data. An added feature of the application system that extend its capabilities beyond a "software representation" of a plurality of secure element representations is that because it has access to the HSM that stores keys used to create the data in each SE representation, it can be configured for authorizing or verifying the output data (digital credential data) for any of the SEs contained in its repository data as well. An HSM is a device commonly used in the banking and processing industry. The HSM is responsible for securely containing encryption keys 203 (cryptographic keys) that are used to authorize card payments, or create digital credential data for new cards. Encryption algorithms 204 that use these keys are also contained on the HSM. An example of an HSM used in the industry at the time of this filing is currently distributed by SafeNet Inc. and is named the ~~Luna~~ LUNA EFT Mark II Edition. An example, from the MASTERCARD ~~PayPass~~ PAYPASS MSD v3.3 card specification document, of an encryption key that may be stored on the HSM is called an Issuer Master Key (IMK). The HSM can then, for example, use the embedded algorithms 204 to create a "diversified key for card verification code creation" (KDcvc3) from the IMK that is used for each individual card that is issued based on a certain algorithm that is also stored in the HSM. The HSM is designed to protect individual encryption keys, and to use embedded encryption algorithms to calculate encryption output based on an encryption input request from an application system. The encryption algorithm must be located within the HSM because the algorithm must have direct access to the protected encryption keys 203. The application system will provide additional input data to be used in the encryption algorithms to the HSM. The application system will also expect output data from the encryption algorithms from the HSM. The input data to the HSM may be stored in the transaction table 205 and the credential table 206. An HSM is commonly a separate device within the application system that

is connected to other devices within the application system through a communication channel. The communication channel may be a network connection such as an RJ45 cable or in some cases is a hardware bus connection such as a PCI connector within a computer casing. An example of using this arrangement may be that the application system contains:

a. Encrypted data (cryptogram)
b. Unpredictable number (UN)
c. Application Transaction Counter (ATC)
d. Transaction data such as a dollar amount
e. A key identifier (but the not key itself)

in its transaction table and credential table. The application system would like to verify encrypted data (a) was created from a particular encryption key (e), unpredictable number (b), ATC (c), and transaction data (d). The application system knows which key was used to create the cryptogram (a), but opts, for security reasons, not to have access to the key itself. The application system then uses the cryptogram (a), unpredictable number (b), ATC (c), transaction data (d), and a key identifier (e) as input for the HSM and sends the input to the HSM. The HSM then uses the input data from the application system and locates the proper encryption algorithm and encryption key to use. The HSM then creates the output response from the algorithm using the encryption key and sends the output to the application system. The output in this example would be a simple "verified" or "not verified" message.

Please replace paragraph [00108] with the following replacement paragraph:

[00108] Examples of SE responses are shown in Fig. 3 next to the 'CARD>:' prompt indicating data from the SE to the point-of-sale. The application system may know the specific responses based on a number of factors. In figure 3, the responses are for a ~~PayPass~~ PAYPASS 3.3 MSD transaction, because the application system knows the particular card id or PAN is associated to this ~~PayPass~~ PAYPASS 3.3 MSD transaction, and the ~~PayPass~~ PAYPASS card specification for 3.3 MSD dictates specifically elements 10, 11, and 12 exactly as shown in figure 3, so the response APDU data as shown in 10, 11, and 12 can be sent verbatim over a communication channel to the mobile device cache when requested by the mobile device.

Please replace paragraph [00109] with the following replacement paragraph:

[00109] Figure 3, element 13 after the 'CARD>:' prompt shows the format of the read record command response, but the data inside the response may change from one card id or PAN to another because it is credential data that is stored in the read record command response. Fortunately the application system has access to all the credential data that comprises the response to the read record command such as displayed, in part in figure 2, element 7:

a. Track 1 and Track 2 data comprised of PAN, Exp Date, card code, issuer discretionary data
b. Substitution bitmaps for Track 1 and Track 2 (PUNATC, PCVC3)
c. Number of ATC digits used in bitmaps (NATC)
d. Application Version Number

From this data, the application system can create the proper APDU response to the read record command that is formatted just like figure 3, element 13 and send it specifically for the card credential the mobile device has requested to the mobile device for caching over a communication channel. For a MASTERCARD ~~PayPass~~ PAYPASS MSD v. 3.3 credential, table 2 shows a technical breakdown of how the data in the read record response is formulated from data in the application system in proper APDU response BER-TLV format.

Please replace paragraph [00110] with the following replacement paragraph:

[00110] As used herein the term "cryptogram" refers to encrypted data that may or may not be able to be un-encrypted. Encrypted data that cannot be un-encrypted is many times called a "hash." A cryptogram is typically calculated from a series of input data that comprises some data and a cryptographic key, where the cryptographic key is used to encrypt some data. As used herein the term "cryptographic key" refers to a key used, at least in part, to calculate a cryptogram. A cryptogram is calculated based on an algorithm or calculation formula. As use herein the term "calculation formula" refers to an algorithm or formula that is specified by a card specification as the method to calculate a cryptogram. A calculation formula typically may be known by any entity. The output result of the calculation formula that uses the input data and a cryptographic key is a cryptogram. Examples of cryptograms at the time of this filing are defined by the following card specifications in table 4.

Table 4

Card specification	Cryptogram Designator or Name
MASTERCARD ~~PayPass~~ PAYPASS MSD	CVC3
VISA Contactless MSD	dCVV
DISCOVER ZIP MSD	dCVV
EMV, VISA QVSDC, VISA VSDC, MASTERCARD MCHIP	AC, TC, AAC, ARQC

A "cryptogram" as used herein may be classified as "dynamic" meaning that it is always changing from one interrogation (transaction) to the next over the life a digital credential (SE representation). As used herein the term "life of", as in, the life of a digital credential, the life of a card, the life of a SE, the life of a SE representation, refers to the life beginning when it is used its first interrogation and ending when it is used in its last interrogation. One indication of this dynamic aspect of a cryptogram is to perform two sequential independent interrogations between a mobile device and a point-of-sale terminal where the same digital credential is used on the mobile device, and the point-of-sale terminal receives two sets of digital credential data with each including a single cryptogram, one with each interrogation. If the cryptogram received by the point-of-sale terminal is different from one interrogation to the next, it is dynamic.

Please replace paragraph [00111] with the following replacement paragraph:

[00111] The details of an interrogation between a point-of-sale and a digital credential, card, SE representation, and mobile device are defined in "card specifications" and implemented in point-of-sale terminals. Examples of these card specifications at the time of this filing are MASTERCARD ~~PayPass~~ PAYPASS --Mag Stripe v3.3, Contactless EMV, DISCOVER NETWORK ~~Network~~ RF Contactless Specification--Supplement Guide For Functional Support, AMEX ALIS v1.7, and VISA Contactless Payment Specification v2.0.2. As used herein the term "card specification" refers to a specification or reference within the specification to other specifications and so on that a point-of-sale terminal must adhere to in order to interrogate a card, SE, mobile device as expected by that card specification. A point-of-sale terminal, as the interrogator, controls the interrogation. The card specification that defines the details of an interrogation may also define the details of a cryptogram request, calculation, and delivery from

the card, SE, or mobile device to the point-of-sale as part of the interrogation sequence. Card specifications may include references to other specifications and those other specifications to even more specification wherein the card specification may be defined by the card specification in conjunction with other supporting documents sited within a card specification. Card specifications typically consist of an application layer that defines an interrogation sequence and calculations that are to be performed by both the card, SE, mobile device and also the interrogator or point-of-sale. Both a mobile device and a point-of-sale are expected to be operating under the direction of a card specification during an interrogation.

Please replace paragraph [00116] with the following replacement paragraph:

[00116] As used herein the terms "transient," "transiently stored," "non-persistent," and "non-persistently stored" refers to data that are stored in a storage container where [[the]] they are erased or otherwise rendered not accessible after a power failure to the storage container. An example of a transient storage container is RAM (Random Access Memory).

Please replace paragraph [00122] with the following replacement paragraph:

[00122] The response for the compute cryptographic checksum command (figure 3, element 14), is created by a method employed in figures 22, 23, 24, 25, 26, 27, 28, 29 and 30 called "Cryptogram Substitution" using a predetermined cryptogram or unpredictable cryptogram and in some embodiments sent for each transaction to the mobile device cache over a communication channel when requested by the mobile device. In other embodiments cryptogram substitution is used with unexpected cryptograms created on the mobile device and sent to a remote application system. For a MASTERCARD ~~PayPass~~ PAYPASS MSD v. 3.3 credential, table 3 shows a technical breakdown of how the data in the read compute cryptographic checksum response is formulated from data in the application system in proper APDU response BER-TLV format.

Table 3

77 0F		
T	L	V
9F 61	02	B8 92 T2_CVC3
9F 60	02	FB C7 T1_CVC3
9F 36	02	00 5E ATC
90 00		

The ATC is the automated transaction counter that increments with every point-of-sale interrogation, and can be stored in the transaction table or credential table and updated with each interrogation by a mobile device. The CVC3 is cryptogram that is expected to be calculated with this algorithm from the MASTERCARD ~~PayPass~~ PAYPASS MSD v3.3 card specification:

First KDcvc3 is created:

$Z_L := DES3(IMK_{CVC3})[Y]$

$Z_R := DES3(IMK_{CVC3})[Y \oplus$ ('FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF')]

and define:

$KD_{CVC3} := (Z_L || Z_R)$.

KDcvc3 calculation may be performed inside the HSM because the HSM contains IMK. The application system will pass Y, which is defined as the PAN and PAN sequence number concatenated as an input to the HSM in conjunction with the IMK id to use. The HSM will respond back with the KDcvc3 as output. The KDcvc3 in this example would be considered a permanent cryptographic key because it will not change over the life of the digital credential, as none of the inputs to the calculation of KDcvc3 change over the life of the credential.

Next T2_IVCVC3 is created:

O:=PayPass-MagStripe(3.3) Annex B alg(KDcvc3)[Track 2 Data]

The least two significant bytes of the output data are defined to be T2_IVCVC3.

Finally, the CVC3 cryptogram for track 2 is calculated:

$O:=DES3(KD_{CVC3})$

$O:=DES3(KD_{CVC3})[T2\_IVcvc3||UN||ATC]$

The least two significant bytes of the output data are defined to be CVC3.

CVC3 calculation may be performed inside the HSM because the HSM contains the IMK which is used to create KDcvc3, which is used to create IVCVC and CVC3. So the application system will pass UN and ATC as inputs in conjunction with the IMK id to use. The HSM will respond back with the CVC3 cryptogram as output. The CVC3 is a dynamic cryptogram as the input to the calculation of the cryptogram change with each interrogation. This is known because with each interrogation the digital credential is expected to increment the ATC (Automated Transaction Counter) and also have different UN value.

Please replace paragraph [00131] with the following replacement paragraph:

[00131] Fig. 16 illustrates a caching system for each transaction or interrogation between a point-of-sale 778 and a mobile device 779 for a MASTERCARD ~~PayPass~~ PAYPASS transaction. The advantage of caching secure element responses is to lessen the effect of network latency and speed up an interrogation. In the example contained Fig. 16, network latency is reduced from a potential 800ms to a potential 200ms because of the caching technique applied. This is a significant effect in the application of NFC or RFID because the as the total interrogation timeframe shrinks, the likelihood of a successful interrogation sequence goes up because it is less likely the communication channel between the point-of-sale and the mobile device will be interrupted from the mobile device moving out of the field generated by the point-of-sale. Notice that not all interrogation command and responses 787 and 793 in Fig. 16 are handled from the mobile device cache 780. The non-cached command and response, lead to the 200ms network latency of the entire transaction in figure 16.'

Please replace paragraph [00133] with the following replacement paragraph:

[00133] Depending on the interrogation sequence selected by the point-of-sale, it may not

always be possible to implement a system set forth in Fig. 17. Many point-of-sale interrogation sequences carried out at the time of this filing are based on card specifications such as:

a. MASTERCARD, ~~PayPass~~ PAYPASS, MChip
b. AMERICAN EXPRESS, EXPRESS PAY ~~Express Pay~~
c. DISCOVER ZIP [[Zip]]
d. VISA QVSDC, VSDC
e. Contactless EMV

Employ a method of creating an expected cryptogram by the mobile device that is calculated, at least in part, from unpredictable data generated on the point-of-sale and delivered to the mobile device during the interrogation sequence. Because creating an expected cryptogram requires a calculation to be performed that includes a permanent cryptographic key, the secure element or system with access to this key must be used to carry out the expected cryptogram calculation. Because the secure element representation is stored in a remote repository and contains the permanent cryptographic key, this expected cryptogram calculation would incur network latency to perform the calculation during the interrogation, as shown in figure 16, element 793.

Please please replace paragraph [00138] with the following replacement paragraph:

[00138] Fig. 22 illustrates how one embodiment of an application system could create cryptograms using random, predetermined, or "made up" input data. A transaction table 210 is defined in which each row represents a transaction between a mobile device and a point-of-sale. The state of the data in this table currently shows transaction data that have been delivered to a mobile device cache, but have not been verified through a point-of-sale. In order to comply with the request of a point-of-sale to a mobile device during an interrogation, the mobile device must deliver cryptogram in the proper data format that the point-of-sale expects. The data that is contained in the actual cryptogram that is delivered to the point-of-sale from the mobile device may not be accurately calculated with the input data from the point-of-sale, but it does not matter at this point as the point-of-sale alone does not verify the cryptogram, it simply receives the cryptogram and relays it for verification to the application system, which has access to the input data used to create the original pre-determined cryptogram. This is why the predetermined cryptogram 218 can [[may]] be calculated based on randomly selected terminal input data UN 213, and Transaction Data 215. The other inputs to create the predetermined cryptogram are based on credential data of each secure element such as the Application

Transaction Counter 214, the Issuer Master Key id 212, and the account Personal Account Number 211. After gathering all predetermined cryptogram input data, the application system sends the input to the HSM and receives the predetermined cryptogram as an output response. The application system may optionally store the predetermined cryptogram 218 into the table 210, for use during verification later.

Please replace paragraph [00142] with the following replacement paragraph:

[00142] These methods of substituting a predetermined cryptogram and of substituting an unpredictable cryptogram are vital to the concept of 100% transaction caching with the existing point-of-sale infrastructure. The existing point-of-sale infrastructure is pre-set for each interrogation sequence and expects data to be formatted according to each interrogation sequence that is programmed in the point-of-sale. Changing the interrogation sequence(s) is out of the control of the mobile device, and so this method of creating a predetermined cryptogram or unpredictable cryptogram as defined using data, at least in part, from Fig. 22 may be required for 100% transaction caching which creates no network latency during the interrogation between the point-of-sale and the mobile device. Because the predetermined cryptogram is created without input from the point-of-sale, the calculation time to create a predetermined cryptogram may also <u>be</u> removed from the overall interrogation time. In the case of an unpredictable cryptogram, this calculation time persists and cannot be removed from the overall interrogation time.

Please replace paragraph [00143] with the following replacement paragraph:

[00143] Fig. 29 illustrates a representation of a table of digital credentials 350 (digital credential data) that may be stored inside the application system. This table, in conjunction with the transaction table, and in some embodiments the HSM allows the application system to perform as a repository of a plurality of secure element software representations. The credential data used to create data inside an SE and also allow it to formulate its proper APDU responses is contained in this table for a plurality of credentials (SEs). For a MASTERCARD ~~PayPass~~ <u>PAYPASS</u> MSD v3.3 credential, the example shown in this table, the columns of data list personal account number (PAN) 351, expiration date 352, name of card holder 353, card code 354, track 1 data 355, track 2 data 356, track 1 cvc3 bitmap 357, track 2 cvc3 bitmap 358, track 1

UN and ATC bitmaps 359, track 2 UN and ATC bitmaps 360, track 1 number of ATC digits 361, track 2 number of ATC digits 362, CVM list 363, AC 364, application version number 365, and the master key identifier 366.

Please replace paragraph [00145] with the following replacement paragraph:

[00145] For an example, the MASTERCARD ~~PayPass~~ PAYPASS interrogation from the point of sale incorporates an APDU command request called "compute cryptographic checksum" 14 as seen in Fig. 3. The command APDU follows a particular format and may look like this:

80 2A 8E 80 04 00 00 08 99 00

The digits 00 00 08 99 in the APDU command above from the point-of-sale indicate the unpredictable number to be used as an expected cryptogram calculation input. This unpredictable number is a random sequence of numbers that changes with each interrogation the point-of-sale initiates. The format of this APDU command request is discussed in more detail inside the MASTERCARD ~~PayPass~~ PAYPASS MSD v3.3 card specification. The immediate APDU response from the mobile device is expected to follow a particular format and may look like this:

77 0F 9F 61 02 B8 92 9F 60 02 FB C7 9F 36 02 00 5E 90 00

The digits B8 92 represent the cryptogram. It is identified by the preceding BER-TLV formatted tag 9F 61 (track 2 CVC3), and length value of 02. It was expected to have been calculated from the unpredictable number issued by the preceding point-of-sale APDU command request in combination with other inputs such as the ATC. A correct expected cryptogram must be calculated using the permanent cryptographic key that is securely stored inside the SE. Because figure 23 implements 100% transaction caching, it is not impossible for the expected cryptogram to be calculated after receiving the unpredictable number from the point-of-sale, because in that event, the mobile device would need to access the network to contact the remote repository as in figure 16, elements 787 and 793 in order to perform the expected cryptogram calculation. The method of substituting a predetermining a cryptogram, or an unpredictable cryptogram in place of the expected cryptogram, in this case, needs to be applied in order to create this response. With

this method applied, the "compute cryptographic checksum" response from the mobile device can be successfully delivered interrogation with the point-of-sale without contacting the remote SE representation during the interrogation. In this case, the cached response may look like this instead:

77 0F 9F 61 02 A4 56 9F 60 02 FB C7 9F 36 02 00 5E 90 00

Where, in one embodiment, the digits A4 56 is the predetermined cryptogram, and NOT calculated using, at least in part, the expected unpredictable number from point-of-sale. Where, in another embodiment, the digits A4 56 is the unpredictable cryptogram, and NOT calculated, at least in part, using the expected permanent cryptographic key rather using a temporary cryptographic. This is an example of "Cryptogram Substitution" technique. The point-of-sale does not have the means or keys to check the received cryptogram for correctness, so it will accept the cryptogram answer because it is of the proper format. The point-of-sale will rely on the authorization request later to verify the correctness of the cryptogram.

Please replace paragraph [00169] with the following replacement paragraph:

[00169] As used herein "sending data" from one entity to another such as a mobile device to a remote application system or ~~vise~~ vice versa should be taken to mean sending the data from one location to another wherein the receiving entity may receive the data as a duplicate from the sending entity or receive the data in parts in addition to receiving information about the data that would enable the receiving entity to reconstruct the original data that was sent from the sending entity.

Please replace paragraph [00181] with the following replacement paragraph:

[00181] In a further embodiment, the verification process could be verification of an unpredictable cryptogram using a temporary cryptographic key assigned to the transaction in the transaction table to calculate and verify the unpredictable ~~crytptogram~~ cryptogram.

Please replace paragraph [00207] with the following replacement paragraph:

[00207] In some embodiments disclosed herein, a specific payment standard issued from MASTERCARD International. This standard is based on reference documentation published by ~~PayPass~~ PAYPASS --Mag Stripe (V3.3).pdf and other derivations. In this card specification, ~~PayPass~~ PAYPASS contactless payment card reader and card interrogation is documented. This document discusses specifically how an RFID reader interrogator would interact with a card containing a SE to extract and build Track1/Track2 equivalent data that is compatible for existing processing infrastructure, but contains the more secure and dynamic aspects of SE driven credential data.

Please replace paragraph [00224] with the following replacement paragraph:

[00224] Some embodiments disclosed herein combine both the tasks performed by the NFC mobile device and the remote system to allow for a complete and un-interrupted interrogation between a RFID POS reader or remote terminal and an NFC mobile device. The interrogation may be performed as set forth by payment card standards such as MASTERCARD ~~PayPass~~ PAYPASS, VISA Contactless, AMEX ~~Express Pay~~ EXPRESS PAY, DISCOVER ZIP [[Zip]], and contactless EMV.

Please replace paragraph [00226] with the following replacement paragraph:

[00226] Some advantages of various embodiments include:

a. In the event a mobile device that is used to conduct an NFC payment transaction with an RFID terminal is lost or stolen, the remote system may be notified and communication with the SE may be blocked until the stolen or lost device is recovered or replaced. In the event the device is replaced, new card credentials do not have to be issued again, but a communication channel with the SE may be opened back up and continued upon proper authorization. Prior to this invention, all new SE credentials or cards would have to be re-issued as the hardware that contained the SE itself would have been lost or stolen also.
b. The SE that is associated with a remote mobile device may be switched to another mobile device fast and easily and is not hardware form factor ~~dependant~~ dependent. The same SE may be used with multiple mobile devices, laptop or desktop computers that have the ability to connect to this

remote system that contains the SE over a data connection and authenticate properly.

c. Compared to changing hardware interfaces, and array of different hardware interfaces, and supported hardware interfaces on a mobile device, a data connection is ubiquitous and standard. SE's currently have various hardware form factors such as:

    i. Embedded microchip (soldered to a circuit board)
    ii. SD, mini-SD, micro-SD interface
    iii. USB interface
    iv. SIM card interface

    Many mobile devices support different sets of the above hardware form factors and many support none of them at all, however, most all mobile devices support a data connection. This ubiquity aids to the portability of SE applications from device to device.

d. Because some embodiments contain an array of SEs or SE representations, and because the remote system is designed to host and connect SE applications to multiple remote devices, it is possible for multiple remote devices from separate remote device owners to share a single SE from the array of SEs in the remote system. This sort of sharing of space on the SE enables consolidation and ultimately savings by more efficient utilization of memory on an array of SEs.

e. Because some embodiments do not rely on a hardware specific interface for the SE, but a data connection only. It is a more ubiquitous interface and may be used with more devices without being modified or changed from a hardware perspective.

f. Because some embodiments use an array or plurality of SEs, the ability to purchase SE chips in quantity for use in this array brings a possibility of a lower over-all cost per SE chip.

REMARKS

Applicant appreciates the time taken by the Examiner to review the present amendment.

Interview Summary

On May 30, 2018, Primary Examiner Robinson and the undersigned participated in a telephonic interview to discuss amending claims 30 and 44 to change "a first application data protocol unit response" to "an application protocol data unit response" and amending the last portion of claim 30 to be consistent with the last portion of allowed claim 44. Primary Examiner Robinson agreed the amendments to claims 30 and 44 appeared to be proper subject matter for an amendment under 37 C.F.R. § 1.312.

Claims

Claims 30 and 44 are amended to change "a first application data protocol unit response" to "an application protocol data unit response." Claim 44 is amended to change "the locally stored cryptographic key associated with the account" to recite "the local cryptographic key associated with the account" consistent with the prior recitation of "a local cryptographic key associated with the account." Claim 37 is amended for grammar.

The last portion of Claim 30 is amended for consistency with the last portion of allowed claim 44. Applicant respectfully submits that, according to the Reasons of Allowability provided by the Examiner, the Examiner would have found amended claim 30 to be similarly allowable. *See* Notice of Allowability at 3-4.

Specification

In reviewing the above-identified application for issuance, the Specification is amended to correct typographical errors and further identify trademarks or tradenames.

Conclusion

Applicant respectfully submits that the amendments do not add new matter. Applicant therefore respectfully requests entry of the amendment.

The Commissioner is hereby authorized to charge any deficiencies or credit any overpayment to Deposit Account No. 50-3183.

Respectfully submitted,

Sprinkle IP Law Group

John L. Adair
Reg. No. 48,828

Dated: June 1, 2018

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. 512-637-9220
Fax. 512-371-9088

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/599,647	08/30/2012	C. Douglas YEAGER	STAPP1100-5	1919

44654 7590 06/25/2018

Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TEXAS 78705
UNITED STATES OF AMERICA

EXAMINER	
ROBINSON, KITO R	

ART UNIT	PAPER NUMBER
3695	

MAIL DATE	DELIVERY MODE
06/25/2018	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR/ PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
13/599,647	08/30/2012	YEAGER, C. Douglas	STAPP1100-5

Sprinkle IP Law Group
1301 W. 25th Street Suite 408
Austin, TX 78705

EXAMINER	
KITO R ROBINSON	
ART UNIT	PAPER
3695	20180622

DATE MAILED: 22 June 2018

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

The IDS filed on 04/30/2018 has been reviewed and does not affect patentability.

/KITO R ROBINSON/
Primary Examiner, Art Unit 3695

PTO-90C (Rev.04-03)

INFORMATION DISCLOSURE STATEMENT				Application Number	13/599,647
				Filing or 371 (c) Date:	August 30, 2012
				First Named Inventor	C. Douglas Yeager
				Group Art Unit	3695
				Examiner Name	Garrison T. Prinslow
Sheet	1	of	1	Attorney Docket Number	STAPP1100-5

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
/K.R.R/	C22	Notice of Allowance issued for Canadian Patent Application No. 2,846,462, mailed February 1, 2018, 1 page.	

Examiner Signature	/KITO R ROBINSON/	Date Considered	06/22/2018	

PRINTER RUSH
(PTO ASSISTANCE)

Application: 13599647	Examiner: Prinslow	GAU: 3695
From: Denise Fisher	Location: RTFM	Creation Date: 05/01/2018

Week Date: 2/26/2018

DOC CODE	DOC DATE	MISCELLANEOUS
[ ] 1449		[ ] Continuing Data
[X] IDS	04/30/2018	[ ] Foreign Priority
[ ] CLM		[ ] Document Legibility
[ ] IIFW/FWCLM		[ ] Fees
[ ] SRFW		[ ] Petition (TC)
[ ] DRW		[ ] Other
[ ] OATH		
[ ] 312		
[ ] SPEC		

[RUSH] Message:

Please respond to the 04/30/18, IDS.

Thank You

DF

[XRUSH] Response:

The IDS filed on 04/30/2018 has been reviewed and does not affect patenability.

/K.R.R/
Initials: _____

Examiner: PUBS contact - James Leija, (703) 756-1197
NOTE: This form will be included as part of the official USPTO record with the response document coded as XRUSH.
REV: AUG 16

Mastercard, Ex1002, p. 1028

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/599,647	07/24/2018	10032171	STAPP1100-5	1919

44654 7590 07/04/2018

Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 845 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

C. Douglas YEAGER, Austin, TX;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

Application Number	13/599,647
Filing Date	August 30, 2012
First Named Inventor	C. Douglas Yeager
Title	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
Art Unit	
Examiner Name	
Attorney Docket Number	47810-0012002

SIGNATURE of Applicant or Patent Practitioner

Signature	/David L. Feigenbaum/	Date (Optional)	10/25/19
Name	David L. Feigenbaum	Registration Number	30,378
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of _____ forms are submitted.

23866474.doc

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on the Transmittal.)

☒ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter, which may be an application filed after the date of this power of attorney, or identified above:

26191

OR

☐ I hereby appoint Practitioner(s) named in the attached list as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter, which may be an application filed after the date of this power of attorney, or identified above.

Please recognize or change the correspondence address for the application identified in the attached transmittal letter to:

☐ The address associated with the above-mentioned Customer Number

OR

☒ The address associated with Customer Number: **26191**

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

OV Loop, Inc.

☐ Inventor or Joint Inventor (title not required below)

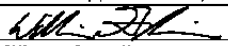
☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	
Name	William Graylin		
Title	CEO		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of _____ forms are submitted.

23949869.doc

Electronic Acknowledgement Receipt

EFS ID:	37562016
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Customer Number:	44654
Filer:	David L Feigenbaum/Marie Callina
Filer Authorized By:	David L Feigenbaum
Attorney Docket Number:	STAPP1100-5
Receipt Date:	25-OCT-2019
Filing Date:	30-AUG-2012
Time Stamp:	12:32:20
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	TransmittalPOA0012002.pdf	92236 [illegible]	no	2
Warnings:					

Information:	
Total Files Size (in bytes):	92236

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/599,647	08/30/2012	C. Douglas YEAGER	STAPP1100-5

CONFIRMATION NO. 1919

IMPROPER CPOA LETTER

44654
Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705

OC0000001122341 46

Date Mailed: 10/29/2019

NOTICE REGARDING POWER OF ATTORNEY

This is in response to the power of attorney filed 10/25/2019. The power of attorney in this application is not accepted for the reason(s) listed below:

- The power of attorney is from an assignee and the statement required by 37 CFR 3.73(c) has not been received.

/ldvan/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

26191
FISH & RICHARDSON P.C. (TC)
PO BOX 1022
MINNEAPOLIS, MN 55440-1022
UNITED STATES

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

Application Number	13/599,647
Filing Date	August 30, 2012
First Named Inventor	C. Douglas Yeager
Title	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
Art Unit	
Examiner Name	
Attorney Docket Number	47810-0012002

SIGNATURE of Applicant or Patent Practitioner

Signature	/David L. Feigenbaum/	Date (Optional)	10/25/19
Name	David L. Feigenbaum	Registration Number	30,378
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of _____ forms are submitted.

23866474.doc

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on the Transmittal.)

☒ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter, which may be an application filed after the date of this power of attorney, or identified above:

26191

OR

☐ I hereby appoint Practitioner(s) named in the attached list as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter, which may be an application filed after the date of this power of attorney, or identified above.

Please recognize or change the correspondence address for the application identified in the attached transmittal letter to:

☐ The address associated with the above-mentioned Customer Number

OR

☒ The address associated with Customer Number: **26191**

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

OV Loop, Inc.

☐ Inventor or Joint Inventor (title not required below)

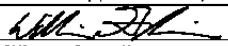
☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	
Name	William Graylin		
Title	CEO		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of _____ forms are submitted.

23949869.doc

Electronic Acknowledgement Receipt

EFS ID:	37725611
Application Number:	13599647
International Application Number:	
Confirmation Number:	1919
Title of Invention:	SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE
First Named Inventor/Applicant Name:	C. Douglas YEAGER
Customer Number:	44654
Filer:	David L Feigenbaum/Marie Callina
Filer Authorized By:	David L Feigenbaum
Attorney Docket Number:	STAPP1100-5
Receipt Date:	12-NOV-2019
Filing Date:	30-AUG-2012
Time Stamp:	14:26:53
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Assignee showing of ownership per 37 CFR 3.73	373Statement_47810_0012002.pdf	95562 8b4c9ea6e2f902708e037c8c95d7303934d03dc5	no	2

Warnings:

Information:					
2	Application Data Sheet	SuppADS47810_0012002.pdf	91333 53b24c4a1c7be1f03e634ce70bf3764daa3 6f578	no	2
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
3	Power of Attorney	TransmittalPOA0012002.pdf	92236 f3f5f6e18085d27ed6544e21b15e67ac01 3678e	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	279131		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: OV Loop, Inc.

Application No./Patent No.: 13/599,647 Filed/Issue Date: August 30, 2012

Titled: SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION BY MOBILE DEVICE

OV Loop, Inc., a assignee

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of the option 1, 2, 3 or 4 below):

1. ☒ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title and interest (check applicable box):

☐ The extent (by percentage) of its ownership interest is _____. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of the options A or B below):

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Douglas C. Yeager To: Simply Tapp, Inc.
The document was recorded in the United States Patent and Trademark Office at
Reel 031642, Frame 0304, or for which a copy thereof is attached.

2. From: Simply Tapp, Inc. To: Doug Yeager
The document was recorded in the United States Patent and Trademark Office at
Reel 046263, Frame 0266, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce. P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: Charles Douglas Yeager To: OV Loop Inc.

The document was recorded in the United States Patent and Trademark Office at

Reel 050756, Frame 0285, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☐ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy *(i.e.,* a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/David L. Feigenbaum/	/11/12/19/
Signature	Date
David L. Feigenbaum	30,378
Printed or Typed Name	Title or Registration Number

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	47810-0012002
	Application Number	13/599,647
Title of Invention	Systems and Methods for Secure Application-Based Participation in an Interrogation by Mobile Device	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

☒ Assignee	☐ Legal Representative under 35 U.S.C. 117	☐ Joint Inventor
☐ Person to whom the inventor is obligated to assign.	☐ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☒

Organization Name OV Loop, Inc.

Prefix	Given Name	Middle Name	Family Name	Suffix

Mailing Address Information:

Address 1	400 West Cummings Park		
Address 2	Suite 2050		
City	Woburn	State/Province	MA
Country	US	Postal Code	01801
Phone Number		Fax Number	
Email Address			

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/David L. Feigenbaum/			Date (MM/DD/YYYY)	11/12/2019
First Name	David	Last	Feigenbaum	Registration	30,378

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	47810-0012002
	Application Number	13/599,647
Title of Invention	Systems and Methods for Secure Application-Based Participation in an Interrogation by Mobile Device	

		Name		Number	

23957445.doc

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/599,647	08/30/2012	C. Douglas YEAGER	47810-0012002

CONFIRMATION NO. 1919

26191
FISH & RICHARDSON P.C. (TC)
PO BOX 1022
MINNEAPOLIS, MN 55440-1022

POA ACCEPTANCE LETTER

OC000000112673548

Date Mailed: 11/18/2019

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/12/2019.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/ngfissha/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/599,647	08/30/2012	C. Douglas YEAGER	STAPP1100-5

CONFIRMATION NO. 1919

POWER OF ATTORNEY NOTICE

44654
Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705

OC000000012673543

Date Mailed: 11/18/2019

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/12/2019.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/ngfissha/

To: PATDOCTC@fr.com,,
From: PAIR_eOfficeAction@uspto.gov
Cc: PAIR_eOfficeAction@uspto.gov
Subject: Private PAIR Correspondence Notification for Customer Number 26191

Nov 18, 2019 03:30:45 AM

Dear PAIR Customer:

FISH & RICHARDSON P.C. (TC)
PO BOX 1022
MINNEAPOLIS, MN 55440-1022
UNITED STATES

The following USPTO patent application(s) associated with your Customer Number, 26191 , have new outgoing correspondence. This correspondence is now available for viewing in Private PAIR.

The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

Disclaimer:
The list of documents shown below is provided as a courtesy and is not part of the official file wrapper. The content of the images shown in PAIR is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
13599647	N570	11/18/2019	47810-0012002
	N570	11/18/2019	47810-0012002

To view your correspondence online or update your email addresses, please visit us anytime at https://sportal.uspto.gov/secure/myportal/privatepair.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov with 'e-Office Action' on the subject line or call 1-866-217-9197 during the following hours:

Monday - Friday 6:00 a.m. to 12:00 a.m.

Thank you for prompt attention to this notice,

UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT APPLICATION INFORMATION RETRIEVAL SYSTEM