



CHAMBER'S COPIES

505 Sansome Street, Suite 1575
San Francisco, CA 94111
T: 415.247.6000 F: 415.247.6001

VIA ECF

June 8, 2023

Hon. Cathy Seibel
U.S. District Court, Southern District of New York
300 Quarropas Street
White Plains, NY 10601-4150

Re: *OV Loop, Inc. v. Mastercard Incorporated et al.*, No. 7:23-cv-01773-CS

Dear Judge Seibel:

This letter responds to Mastercard's request to file a 12(b)(6) motion (ECF 29) ("Ltr.").

I. **THE '171 PATENT IS BOTH CONCRETE AND INVENTIVE.**

At Alice Step 1, Mastercard mischaracterizes the invention as "authorizing a person[']s ... identity, which idea has existed for centuries...and can be provided by a mental process and pen-and-paper analogue." Ltr. at 3. This is not a fair claims description. It is, instead, exactly the kind of "reductionist simplicity" inimical to patent law. As Judge Forrest memorably put it:

[E]very invention could be described at a high level...: "A method to provide answers to questions" for a search engine; "a tool to assist a user to draft documents" for a document-processing program; "a tool to remove a cork from a container" for a battery-operated wine-bottle opener; "a beverage container that does not leak when tipped" for...a particularly nifty lid....This reductionist simplicity may obscure underlying complexity...it may jeopardize the innovative improvements upon longstanding accomplishments that patents are intended to incent....Many recent motions...**suffer from such reductionist simplicity—from characterizing as simply a mousetrap that which is in fact a better mousetrap.**

Verint Sys. Inc. v. Red Box Recorders Ltd., 226 F. Supp. 3d 190, 192 (S.D.N.Y. 2016).

Judge Forrest's analysis respects the Federal Circuit's "reiterat[ion of] the Supreme Court's caution against 'overgeneralizing claims' in the § 101 analysis," since "characterizing claims at a 'high level of abstraction' that is 'untethered from the language of the claims all but ensures that the exceptions to § 101 swallow the rule.'" *TecSec, Inc. v. Adobe Inc.*, 978 F.3d 1278, 1293 (Fed. Cir. 2020). The Federal Circuit has explained that in software cases courts ask whether a claim's focus "is on a solution to 'a problem specifically arising in the realm of computer networks'...and whether the claim is properly characterized as identifying a 'specific' improvement ... rather than only claiming a desirable result" *Id.* Properly characterized, the '171 claims describe a complex and uniquely computer-centric solution to a problem itself digitally based.

The improvements are achieved through several components, including: (1) a "mobile device" (e.g., smartphone) with a payment "application" that "does not have access to a permanent cryptographic key;" (2) a "remote system" (cloud-based backend) that generates "non-permanent cryptographic keys;" (3) storing such cloud generated non-permanent cryptographic keys on the phone to use with "point-of-sale" terminals (e.g., cash register), given the "interrogations" between the two; and (4) using stored non-permanent cryptographic keys to generate "response cryptograms" to POS "commands" for mobile payment transaction authorizations. *See* Claims 1 & 17. The solution's focus is concrete—for example, it uses cloud generated non-permanent cryptographic keys ("NPCK"), not permanent cryptographic keys ("PCK"), all to provision a new, secure digital payment method. *See id.*; *see also* '171, Abstract ("without access to a local persistently stored [PCK]"); '171, Field ("remotely hosted Secure Element"). The '171 claims are entirely computer centric; they are not abstract. To elaborate: mobile-based payment systems

present a security problem. Information on a mobile computing device is very vulnerable to theft. The old mode solved for this by storing PCKs in a device secure element (“SE”). This SE could be a physical, tamper-proof chip. A PCK is a cryptographic key (a key used to encrypt data) that is unchanging (or static) throughout the life of a payment card. So, for example, in the old mode, the device SE chip would be pre-loaded with a PCK, and that permanent key—protected by the specialized chip—would be used every transaction to generate a cryptogram (encrypted data used in authorization decisions). A drawback was that the solution provider needed to work with others (e.g., mobile network operators, phone manufacturers) to ensure devices had PCK loaded SEs. This solution was inflexible, as the ’171’s prosecution history explained. *See* Ex. 1 at 018-19 (“a more flexible system for mobile payment authorization is required”). A platform agnostic solution was needed.¹

The ’171 provided just such a solution by introducing an off-device SE on a secure backend. *See* Ex. 1 at 019-20 (“to address the problem....Remote Hosted Secure Element...generates the appropriate cryptogram....These solutions provide the advantage that the mobile device does not need to access the [PCK]”). But, as the prosecution history further explained, this leads to system delay and network latency. *See id.* at 020 (“solutions such as those...can introduce delays...that may have deleterious effects”). For instance, at purchase time, cellular connectivity is needed, as the phone needs to receive from the cloud a cryptogram to send onto the POS. The ’171 solved such conundrums by introducing cloud generated NPCKs. Since these keys change, for example, after a preset number of interrogations, storing them on the phone does not introduce the security risk that storing a PCK does. *See id.* at 021 (“the key used...changes, limiting the key’s usefulness if stolen....[T]he claimed invention helps address the issue of network delay...by retaining response cryptogram generation at the mobile device”).

These claims are not abstract in the least: they provide a specific mobile payment computer architecture that improves system scalability, while maintaining security and reduced latency. They are directed to improvements in computer and network functionality, just as the Patent Office found: “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.” *Id.* at 044.

As to Alice Step 2, the claimed inventions embody inventive concepts in at least the remote SE and NPCKs, as these features, as explained, “provide[] a specific solution that improves the computer system itself by providing security while making the system more efficient.” Ex. 1 at 042. Such claims are clearly patent eligible. *See CosmoKey Solutions GmbH & Co. KG v. Duo Security LLC*, 15 F.4th 1091, 1098 (Fed. Cir. 2021) (finding claims that “recite a specific improvement to authentication that increases security, prevents unauthorized access by a third party, is easily implemented, and can advantageously be carried out with mobile devices of low complexity” eligible under Step 2 on a 12(c) motion). More, and despite Mastercard’s contrary characterization, *see* Ltr. at 3, as explained, the deployment of these features in smartphone payment systems was not “generic.” Both features represented a revolutionary departure from the prior art’s device-based SEs with PCKs. This is not an overstatement. For example, the ’171

¹ Given Mastercard attached the entire, lengthy ’171 Patent to its letter as Exhibit A, OV Loop here attaches relevant portions of the ’171’s prosecution history, as Exhibit 1. Both are matters of public record that this Court may take judicial notice of in deciding any motion to dismiss. *See Uniloc USA, Inc. v. ADP, LLC*, 772 Fed. App’x 890, 898 n.3 (Fed. Cir. 2019).

Hon. Cathy Seibel

Page 3

inventor's company was "awarded Best Contactless Payments Solution of the Year at the 2015 Future Digital Awards." <https://www.nfcw.com/2015/08/25/337201/simplytapp-picks-up-contactless-payments-award/>. A solution recognized as "redefin[ing] and reinvigorat[ing]" a market by providing a "technological backbone," *see id.*, is not some mere application of "well-understood, routine, conventional activities previously known in the industry." *CosmoKey*, 15 F.4th at 1097.

Mastercard should not be permitted an obligatory 12(b)(6) *Alice* motion that rests on self-serving over generalizations divorced from reality.

II. THE COMPLAINT PROVIDES FAIR AND AMPLE NOTICE.

Mastercard says it is left "to guess what this case is about." Ltr. at 2. Hardly. The Complaint tells Mastercard that systems implementing its Host Card Emulation ("HCE") specifications are accused, cites an example Mastercard HCE specification by name—"MCBP"—and cites Mastercard public documents discussing Mastercard HCE specifications. *See* ECF 1, ¶¶ 59-62, 66. The Complaint also tells Mastercard exactly what Mastercard technology is implicated: its HCE "MDES" backend technology, *see, id.* ¶¶ 63, 66, 78, a fact Mastercard ignores in its letter. And, even Mastercard admits that the Complaint identifies by name an accused application-remote system combination example, the MDES-Garmin combination. Fair notice does not require a complaint to list, name-by-name, every infringing product. Indeed, the Local Patent Rules affirm that no such pleading requirement exists, as they call for product identification post-CMC. *See* Rule 6 ("after the [CMC]...serve...Infringement Contentions[], which identifies...each product...of which the party claiming infringement is aware...").

Mastercard next claims that no "comparison...of [its] allegedly infringing acts with any of the patent claims" is provided and that card network specifications are "voluminous." Ltr. at 2. Mastercard so insists that a complaint must contain full **infringement charts** and that these charts must cite, by page and verse, confidential Mastercard information, all pre-discovery. *See* ECF 1 at 21 n.2 (the specifications are non-public). But a plaintiff "need not 'prove its case at the pleading stage,'" and claim-element-by-claim-element pleading is not required. *See Nalco Company v. Chem-Mod, LLC*, 883 F.3d 1337, 1350 (Fed. Cir. 2018).

Mastercard then argues that OV Loop's Garmin example fails. But, Mastercard ignores not only the actual Garmin allegations, *see* ECF 1, ¶¶ 80-81, but the plain claim language. The claims are agnostic as to where the cloud-generated NPCKs are stored on the device. *See* Claim 1 ("locally storing the first [NPCK] at the mobile device"). The NPCKs can be stored in a device SE, so long as they come from a remote SE. What cannot be relied on is a device SE with PCKs. Nothing in the articles Mastercard points to say that its MDES-Garmin implementation uses device SE PCKs. More, while Mastercard happily cites material in a Complaint cited document that it, mistakenly, believes favors it, it ignores material that says that HCE can be implemented using device SE storage. *See* <https://www.securetechalliance.org/wp-content/uploads/HCE-101-WP-FINAL-081114-clean.pdf> at 10 ("credentials used by this HCE...could be stored in other secure locations such as...an SE") & 22 ("HCE does not dictate where to store"), cited at ECF 1, ¶ 62.

Finally, Mastercard's conduct contradicts its letter. Mastercard concluded from the Complaint's supposed "conclusory allegations" that its MDES-Samsung combination was fairly put at issue. The day after Mastercard filed its request for leave, OV Loop received a letter from Samsung telling it that Mastercard sought indemnity from Samsung for Samsung Pay based on this case. Mastercard knows it is on the hook for its MDES-Samsung Pay instrumentality.

Mastercard's feigned ignorance should not be rewarded with wasteful motion practice.

HOSIE | RICE LLP
ATTORNEYS AT LAW

Hon. Cathy Seibel

Page 4

Very truly yours,

/s/ Spencer Hosie
Spencer Hosie

EXHIBIT 1



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	Simplytapp0002US1	1919

122870	7590	10/06/2015	EXAMINER	
Hanchuk Kheit LLP			PUTTAIAH, ASHA	
258 Saint Nicholas Avenue, No. 8A				
New York, NY 10027-5353				

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

Application/Control Number: 13/599,647
Art Unit: 3695

Page 4

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

Application/Control Number: 13/599,647

Page 5

Art Unit: 3695

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*

Application/Control Number: 13/599,647
Art Unit: 3695

Page 6

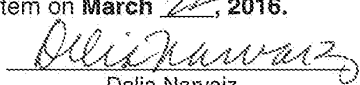
requesting the digital credential data wherein the at least one POS command communication conforms to a card specification; and
sending through the communication channel at least one device response communication from the mobile device to the point-of-sale terminal comprising the expected cryptogram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

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

Dear Sir:

<u>Certificate of Transmission Under 37 C.F.R. § 1.8</u> 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

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.

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

18

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;

ExcerptPage006

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

19

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 response 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

ExcerptPage007

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

20

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

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

21

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

ExcerptPage009

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

22

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.

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

23

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

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

24

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.

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

25

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."

ExcerptPage013

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

30

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.

ExcerptPage014

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

31

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

ExcerptPage015

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

32

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

ExcerptPage016

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

33

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).

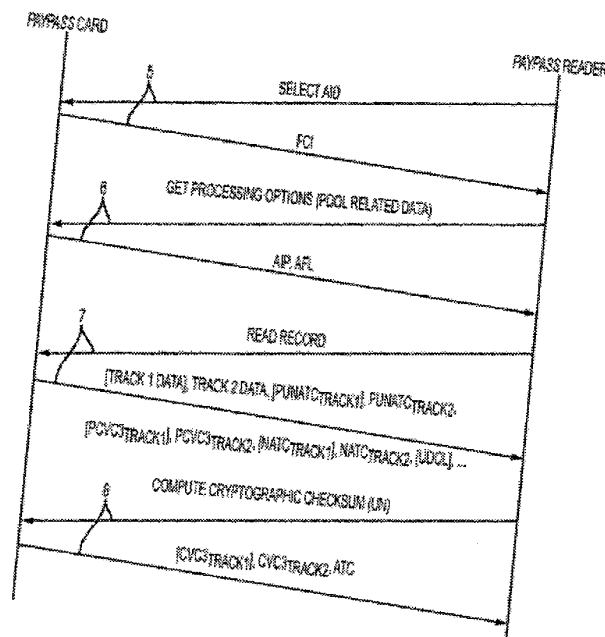


FIG. 2

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 CRYPTOGRAPHIC 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

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

34

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

ExcerptPage018

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

35

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 CRYPTOGRAPHIC 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

ExcerptPage019

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

36

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 CRYPTOGRAPHIC 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 CRYPTOGRAPHIC 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 by 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;

ExcerptPage020

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

37

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

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

38

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

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

39

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.

ExcerptPage023



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	06/14/2016	EXAMINER	
Sprinkle IP Law Group			PUTTAIAH, ASHA	
1301 W. 25th Street				
Suite 408				
Austin, TX 78705				

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.

Application/Control Number: 13/599,647
Art Unit: 3695

Page 4

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.

Application/Control Number: 13/599,647
Art Unit: 3695

Page 7

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

Application/Control Number: 13/599,647
Art Unit: 3695

Page 8

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

ExcerptPage027

Application/Control Number: 13/599,647
Art Unit: 3695

Page 9

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.*

ExcerptPage028

Application/Control Number: 13/599,647
Art Unit: 3695

Page 10

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

Application/Control Number: 13/599,647
Art Unit: 3695

Page 11

- 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.

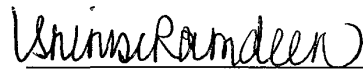
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
REPLY TO OFFICE ACTION DATED 06/14/2016	Atty. Docket No. STAPP1100-5
First Named Inventor C. Douglas Yeager	
Application Number 13/599,647	Date Filed August 30, 2012
Title SYSTEMS AND METHODS FOR SECURE APPLICATION-BASED PARTICIPATION IN AN INTERROGATION 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.

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

2

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

ExcerptPage032

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

3

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 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

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

4

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

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

5

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

ExcerptPage035

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

6

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.

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

7

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.

ExcerptPage037

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

8

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.

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.”)

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

11

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.

ExcerptPage040

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

12

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 recognize 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

Attorney Docket No.
STAPP1100-5

Application No. 13/599,647
Customer ID: 44654

13

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’.” Manduley 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.*

ExcerptPage042



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	06/05/2017	EXAMINER	
Sprinkle IP Law Group			PUTTAIAH, ASHA	
1301 W. 25th Street				
Suite 408				
Austin, TX 78705				

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.

Application/Control Number: 13/599,647
Art Unit: 3695

Page 3

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

ExcerptPage044



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.

Application/Control Number: 13/599,647
Art Unit: 3695

Page 3

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; [...]

ExcerptPage046

Application/Control Number: 13/599,647
Art Unit: 3695

Page 4

- 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;

ExcerptPage047