

File No. 10009.PV

Date: Aug. 30, 2011

New PROVISIONAL APPLICATION

Applicant(s): C. Douglas YEAGER

Title: REMOTE HOSTED SECURE ELEMENT REPOSITORY

Enclosures:

- (1.) Check #1104 in the amount of \$110
- (2.) Provisional Application for Patent Cover Sheet (PTO/SB/16) (2 pp.)(in duplicate)
- (3.) Specification (18 pp.)
- (4.) Drawings (9 pp.)
- (5.) Express Mail #

COMMISSIONER FOR PATENTS

Please acknowledge receipt of the above-identified documents by applying the USPTO receipt stamp hereto and mailing this slip in the enclosed envelope.

PATENT APPLICATION SERIAL NO. _____

**U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET**

09/01/2011 JADD01 00000028 61575846
01 FC:2005 110.00 OP

PTO-1556
(5/87)

16085 U.S. PTO
083011

PTO/SB/16 (12-08)

Approved for use through 06/30/2010. OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

PROVISIONAL APPLICATION FOR PATENT COVER SHEET – Page 1 of 2

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. _____

INVENTOR(S)		
Given Name (first and middle (if any))	Family Name or Surname	Residence (City and either State or Foreign Country)
CHARLES DOUGLAS	YEAGER	AUSTIN, TX

Additional inventors are being named on the _____ separately numbered sheets attached hereto.

TITLE OF THE INVENTION (500 characters max):

REMOTE HOSTED SECURE ELEMENT REPOSITORY

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☐ The address corresponding to Customer Number:

OR

☒ Firm or Individual Name DOUG YEAGER

Address 7502 WEST RIM DR.

City AUSTIN	State TX	Zip 78731
Country	Telephone 865-604-6546	Email

ENCLOSED APPLICATION PARTS (check all that apply)

☐ Application Data Sheet. See 37 CFR 1.76 ☒ Drawing(s) Number of Sheets <u>9</u> ☒ Specification (e.g. description of the invention) Number of Pages <u>18</u>	☐ CD(s), Number of CDs _____ ☐ Other (specify) _____
---	---

Fees Due: Filing Fee of \$220 (\$110 for small entity). If the specification and drawings exceed 100 sheets of paper, an application size fee is also due, which is \$270 (\$135 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

METHOD OF PAYMENT OF THE FILING FEE AND APPLICATION SIZE FEE FOR THIS PROVISIONAL APPLICATION FOR PATENT

☒ Applicant claims small entity status. See 37 CFR 1.27. ☒ A check or money order made payable to the Director of the United States Patent and Trademark Office is enclosed to cover the filing fee and application size fee (if applicable). ☐ Payment by credit card. Form PTO-2038 is attached. ☐ The Director is hereby authorized to charge the filing fee and application size fee (if applicable) or credit any overpayment to Deposit Account Number: _____	\$ 110 TOTAL FEE AMOUNT (\$)
--	--

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PROVISIONAL APPLICATION COVER SHEET
Page 2 of 2

PTO/SB/16 (12-08)

Approved for use through 06/30/2010. OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

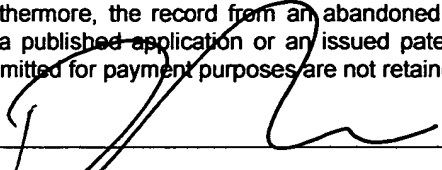
The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

SIGNATURE  Date 8/30/2011

TYPED or PRINTED NAME DOUG YEAGER REGISTRATION NO. _____
(if appropriate)

TELEPHONE 865-604-6546 Docket Number: 6009.PV

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

PROVISIONAL APPLICATION FOR PATENT COVER SHEET – Page 1 of 2

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. _____

INVENTOR(S)		
Given Name (first and middle (if any))	Family Name or Surname	Residence (City and either State or Foreign Country)
CHARLES DOUGLAS	YEAGER	AUSTIN, TX

Additional inventors are being named on the _____ separately numbered sheets attached hereto.

TITLE OF THE INVENTION (500 characters max):

 REMOTE HOSTED SECURE ELEMENT REPOSITORY

Direct all correspondence to: CORRESPONDENCE ADDRESS

☐ The address corresponding to Customer Number:

 OR
☒ Firm or Individual Name DOUG YEAGER
 Address 7502 WEST RIM DR.

City <u>AUSTIN</u>	State <u>TX</u>	Zip <u>78731</u>
Country _____	Telephone <u>865-604-6546</u>	Email _____

ENCLOSED APPLICATION PARTS (check all that apply)

☐ Application Data Sheet. See 37 CFR 1.76 ☒ Drawing(s) Number of Sheets <u>9</u> ☒ Specification (e.g. description of the invention) Number of Pages <u>18</u>	☐ CD(s), Number of CDs _____ ☐ Other (specify) _____
---	---

Fees Due: Filing Fee of \$220 (\$110 for small entity). If the specification and drawings exceed 100 sheets of paper, an application size fee is also due, which is \$270 (\$135 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

METHOD OF PAYMENT OF THE FILING FEE AND APPLICATION SIZE FEE FOR THIS PROVISIONAL APPLICATION FOR PATENT

☒ Applicant claims small entity status. See 37 CFR 1.27.
☒ A check or money order made payable to the Director of the United States Patent and Trademark Office is enclosed to cover the filing fee and application size fee (if applicable).
☐ Payment by credit card. Form PTO-2038 is attached.
☐ The Director is hereby authorized to charge the filing fee and application size fee (if applicable) or credit any overpayment to Deposit Account Number: _____

\$ 110

TOTAL FEE AMOUNT (\$)

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PROVISIONAL APPLICATION COVER SHEET
Page 2 of 2

PTO/SB/16 (12-08)

Approved for use through 06/30/2010. OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

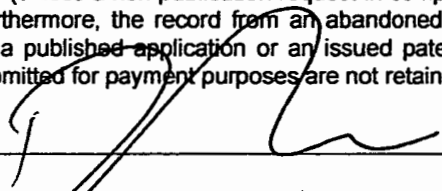
The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

SIGNATURE  Date 8/30/2011

TYPED or PRINTED NAME DOUG YEAGER REGISTRATION NO. _____
(if appropriate)

TELEPHONE 865-604-6546 Docket Number: 6009.PV

PROVISIONAL PATENT APPLICATION

OF

DOUG YEAGER

FOR

REMOTE HOSTED SECURE ELEMENT REPOSITORY

Name C. Douglas Yeager
Address 7502 West Rim Dr., Austin, TX 78731
Citizen of USA

1.865.604.6546 (Tel)

doug@elementalknowledge.com

Attorney Docket: 10009.PV

EXPRESS MAIL NO.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

on _____
Date

FIELD

[0001] This invention relates to the field of payment and authorization methods using a mobile computing application in combination with a remotely hosted Secure Element. This invention is also related to methods by which such devices may be used to make payments, authorizations or exchange information with other devices.

[0002] BACKGROUND

[0003] In some payment technologies such as smartcard payment, a microchip referred to as a “Secure Element” (SE) is embedded into the payment card, payment FOB, or other mobile devices that can be used for making payments. For the purpose of simplifying language in this document, the device that houses the SE will be referred to as the “card” or “card device”. It is important to note that the “card” or “card device” may not physically resemble the shape or size of a typical payment card and may come in various form factors such as embedded into a mobile phone or embedded into a removable storage or removable device. Also, it is important to note that the SE may be an emulated software based SE and not strictly hardware based. Any microprocessor controller has the ability to emulate and pretend to be an SE.

[0004] In order to extract information from the SE, an interrogator, which also may be referred to in this document as a “reader”, is required to communicate with the SE. The interrogator typically follows standards set forth by ISO and application providers to do so.

[0005] A significant advantage of extracting and delivering the data within a SE is the ability to know beyond all doubt that the data string being delivered indeed came from a particular SE or card. This knowledge creates a more secure transaction with lower risk to the merchant, card issuing bank, and card associations. Prior to the present invention, most methods for extracting information from a banking card are traditional methods of swiping the magnetic stripe on a card through a magnetic stripe reader, or extracting the information with a separate contact or contactless reader connected to a POS (POS). These more secure methods of extracting the information on the card allow a merchant to receive a discounted transaction fee for the particular transaction. An example of a less secure transaction would be reading or entering account numbers, expiration dates, and card verification codes off of a card during a phone call or internet shopping experience.

[0006] It is important to note that acquiring transactional data from a SE such as Track1/Track2 data is significantly different than simply using a duplicate of

transactional data such as a copy of Track1/Track2 data located on a card magnetic stripe. A magnetic stripe on a card is considered a static data set and never changes Track1/Track2 data between transactions or “swipes”. For this reason, the data on the stripe could simply be copied or duplicated for use by other form factors. Also, simply copying the card digits printed on the front and back of the card presents this same security risk.

[0007] Acquiring transactional Track1/Track2 data from a SE is considered singular and has a life span of a single transaction or a single “swipe” and then the data is no longer valid. Moreover the Track1/Track2 data acquired during an SE interrogation cannot be created by any other entity except the SE which has been programmed with secret shared keys owned by the bank or application which was loaded to that SE.

[0008] In contrast, the data on a magnetic stripe can be copied and programmed to a mobile device and used to make transactions continuously from the copy with no technical limitation. In the same way, card numbers that are simply copied from the face or front or back of the card and programmed to a mobile device and can also be continuously used to make transactions without a technical limitation.

[0009] Knowing this difference, the subject of the present invention is directed specifically to SE transactions because the security of these types of transactions makes the architecture defined in this patent much more plausible and secure to current industry banking and processing standards.

[0010] Cards containing a SE are typically presented to an RFID (Radio Frequency Identification) reader device as the interrogator that extracts the information from the card and delivers the data to the POS (Point Of Sale) and then on to the card processor for authorization. Mobile phones that contain NFC (Near Field Communication) functionality with embedded SEs have the ability to pretend or emulate a card that would contain an SE. In this case the mobile phone can be presented to the RFID reader just as a card would and the information can be extracted from the SE that is on the mobile phone and delivered to POS and then on to the card processor for authorization.

[0011] The present invention allows for a mobile phone or mobile device to engage and be interrogated by a POS device while the SE, that is the subject of the transaction, remains remotely hosted in a separate facility. The mobile device in the case of this invention acts as a pass-through to facilitate the interrogation of the remote SE by the POS RFID reader through a data link or data connection to the remotely hosted SE.

[0012] The present invention uses the base-band processor on the NFC mobile device to do one or all of the following tasks:

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

[0013] The present invention uses a remote server network and remote array of secure elements or representations of secure elements (remote system) to do one or all of the following tasks:

- a. Authenticate a particular remote mobile device or owner of a mobile device that wishes to send queries from an interrogator to a SE that is contained in this system.
- b. Properly address a single SE within an array of SEs to respond appropriately to the remote authenticated device.
- c. Properly route queries that were passed to this system to a particular SE or SE software representation within the system and properly route responses from the SE out of the system to the correct authenticated remote device.

[0014] The present invention combines both the tasks performed by the NFC mobile device and the remote system to allow for a complete and un-interrupted interrogation between a RFID POS reader and an NFC mobile device. The interrogation may be performed as set forth by payment card standards such as MasterCard PayPass, VISA Contactless, AMEX Express Pay, and Discover Zip.

[0015] The data link or data connection and communication between the mobile device and the remote system stated above could be carried out over standard TCP/IP services that is currently available on mobile devices.

[0016] Some advantages of the present invention include:

- a. In the event a mobile device that is used to conduct an NFC payment transaction with an RFID terminal is lost or stolen, the remote system can be notified and communication with the SE can be blocked until the stolen or lost device is recovered or replaced. In the event the device is replaced, new card credentials do not have to be issued again, but a communication channel with the SE can be opened back up and continued upon proper authorization. Prior to this invention, all new SE credentials or cards would have to be re-issued as the hardware that contained the SE itself would have been lost or stolen also.
- b. The SE that is associated with a remote mobile device can be switched to another mobile device fast and easily and is not hardware form factor dependant. The same SE may be used with multiple mobile devices, laptop or desktop computers that have the ability to connect to this remote system that contains the SE over a data connection and authenticate properly.
- c. Compared to changing hardware interfaces, and array of different hardware interfaces, and supported hardware interfaces on a mobile device, a data connection is ubiquitous and standard. SE's currently have various hardware form factors such as:

- 1) Embedded microchip (soldered to a circuit board)
- 2) SD, mini-SD, micro-SD interface
- 3) USB interface
- 4) SIM card interface

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

- d. Because the present invention contains an array of SEs or SE representations, and because the remote system is designed to host and connect SE applications to multiple remote devices, it is possible for multiple remote devices from separate remote device owners to share a single SE from the array of SEs in the remote system. This sort of sharing of space on the SE enables consolidation and ultimately savings by more efficient utilization of memory on an array of SEs.
- e. Because the present invention does not rely on a hardware specific interface for the SE, but a data connection only. It is a more ubiquitous interface and could be used with more devices without being modified or changed from a hardware perspective.
- f. Because the present invention uses an array or plurality of SEs, the ability to purchase SE chips in quantity for use in this array brings a possibility of a lower over-all cost per SE chip.

[0017] Some additional advantages of the present invention also include:

- a. Using “2 factor” authentication to protect connection to a remote SE from a mobile device. Upon authentication, a connection channel can be opened to a SE that relates to a particular mobile device. 2 factor

authentication comprises of “something you have or do” AND “something you know”.

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

[0018] In this document, the concept of “Remote Hosted Secure Element” (RHSE). This is referring to the concept of creating a remote repository for plurality SEs intended for a plurality of mobile devices or mobile device owners. The plurality of SEs or array of SEs is hosted in a secure environment and can be represented literally with actual SE hardware or as a virtual SE representation done entirely in software.

[0019] In the case an array of SEs are present in hardware, the complete system could be created with a large array of SE card readers that are each addressable. These SE card readers simply convert ISO 7816 card protocol into electrical signals that are eventually converted into TCP/IP data packets. These SE card readers each have an SE card plugged into them. Software and hardware that interacts with each card reader has the ability to query each SE at a particular address that corresponds to a particular remote mobile device. As a result data that is passed to a particular SE from a remote mobile device is translated and routed over a TCP/IP network to the correct hardware SE reader and hence to the SE. These concepts are not limited to one particular form factor or embodiment.

[0020] In the case an array of SEs are present in software as a representation of an SE, a SE card reader is not needed to interrogate the SE. A software representation would allow a completely contained system the gives the same remote mobile device functionality as the previous completely hardware based case.

[0021] The hardware case may be the preferred case as defined by the industry simply because of the more secure nature of controlling the removable SE that could be manufactured with secure data residing on the SE chip in a secure facility and then shipped to the remote system facility to be plugged in and activated and verified.

[0022] In this document, the concept of managing a remote system containing of a plurality of SE readers, each one being addressable and matched to a particular mobile device is discussed.

[0023] Also, in this document, the concept of authenticating a mobile device with a remote system to obtain access to a particular SE within a plurality of SEs in that remote system is discussed.

[0024] Also, in this document, the concept of connecting a mobile device to a remote service via activating a data-pass-through mode for ISO7816-4 data queries from an POS RFID reader through a mobile device NFC interface through the mobile device OS, to a data connection to a remote system containing a plurality SEs.

[0025] Also, in this document, the concept of using TCP/IP sockets to enable a communication channel between a RFID POS reader and a single SE within remote system containing a plurality of SEs.

[0026] Also, in this document, the concept of authenticating over SSL to enable a TCP/IP socket communication channel between a RFID POS reader and a single SE within a remote system containing a plurality of SEs.

[0027] In this document, a specific payment standard issued from MasterCard International will be discussed. This standard is based on reference documentation published by PayPass - Mag Stripe (V3.3).pdf and other derivations. In this specification, PayPass contactless payment card reader and card interrogation is documented. This document discusses specifically how an RFID reader interrogator would interact with a card containing a SE to extract and build Track1/Track2 equivalent data that is compatible for existing processing infrastructure, but contains the more secure and dynamic aspects of SE driven credential data.

Brief Description of the Drawings

[0028] Fig. 1 illustrates the command and response APDU (Application Protocol Data Unit) flow between a reader and an SE.

[0029] Fig. 2 illustrates the command and response APDU flow between a reader and an SE with specific details about the MasterCard PayPass application that is installed on the SE

[0030] Fig. 3 illustrates the raw data of a transaction between a reader and an SE

[0031] Fig. 4 illustrates the format for which the reader is expected to deliver the results of the previous interrogation

[0032] Fig. 5 illustrates a diagram of a mobile device that contains NFC capabilities and how that device allows access to secure elements

[0033] Fig. 6 illustrates a diagram of an addressable array of remote hosted SEs

[0034] Fig. 7 illustrates a User ID SE address lookup table

[0035] Fig. 8 illustrates an authorization flow for using a remote hosted SE

[0036] Fig. 9 illustrates a data flow diagram including authorization between a mobile device and a remote hosted SE

DETAILED DESCRIPTION

[0037] Fig. 1 describes the protocol level communication between a reader and an SE. The protocol layer is a standard protocol referred to as APDU. APDU stands for Application Protocol Data Unit and the protocol is defined by ISO/IEC 7816 specification. The APDU, ISO/IEC 7816-4 data is typically transmitted over the air on 13.56 Mhz reader to SE radio waves during a contactless or NFC transaction. There is no limitation to this however and the APDU commands are just data moving from one entity to another. The present invention uses the standard APDU commands to interact with the SE regardless if the SE is located on the mobile devices own embedded SE, a remote SE embedded into a remote system or a card. Element (1), (2), (3), and (4) show the sequential commands of a typical command and response between and SE and an interrogator. Usually multiple steps are involved with accessing a SE which require multiple APDU command queries and response for each complete transaction. This specific fig. 1 shows the general interrogation steps to access credential data on a MasterCard PayPass Magstripe application running on a SE.

[0038] Fig. 2 describes the detailed commands and responses expected when a reader interrogates a MasterCard PayPass Magstripe ver. 3.3 application running on a SE. This data is obtained through the MasterCard PayPass specification that was referenced earlier in this document. All details including abbreviations and acronyms are explained in detail through this specification document.

[0039] Fig. 3 describes an example transaction at the ISO/IEC 7816-4 protocol level (APDU) between a reader and a card using the MasterCard PayPass Magstripe application specification v. 3.3. Element (9) defines some of the initial parameters used in the transaction which include an unpredictable number issued by the reader, a transaction counter maintained on the SE. Element (10) describes the command that the reader issues to the SE to find out what applications exist on the SE. this example shows that the mastercard PayPass application responds as an active one. Next element (11) shows how the reader queries the SE to properly select the PayPass application for further processing. Element (12) shows how the reader receives the type of processing options that the PayPass

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

[0040] Fig. 4 describes how the reader (21) in Fig. 5 is expected to format the response data received from the SE into accepted Track1 and Track2 data strings that are used in existing processing systems. Element (15) shows a Track2 data string built from the card interrogation in figure 3. The CVC3(Track2) UN and ATC numbers will all vary with each transaction or interrogation of the SE. Element (16) shows a Track1 data string built from the card interrogation in figure 3. CVC3(Track1), ATC, and UN numbers will all vary with each transaction or interrogation of the SE. This data is obtained through the MasterCard PayPass specification that was referenced earlier in this document. All details including abbreviations and acronyms are explained in detail through this specification document.

[0041] Fig. 5 describes the inner architecture of a mobile device that supports NFC functionality and how that device would allow access to its attached secure elements as well as a remote secure element. Element (17) is the base band processor of the mobile device and typically runs an OS (Operating System) to control all aspects and interfaces on the device including communication access to the SIM (20), NFC controller (18), Secure IC (25), or data to the internet (27). The NFC controller (18) acts as a router to determine where the communication is routed. When a mobile NFC device is presented to an RFID POS, the ability for the mobile device to emulate a card (pretend to be a payment card) is possible. When this happens the NFC controller (18) which is controlled by the baseband processor on the mobile device (17) can be configured to route the interrogation queries

(1),(2),(3),(4),(5),(6),(7),(8) from the reader (interrogator) (21) to a secure element for processing and response. A SE application that is used in a payment transaction will be configured to respond to interrogation queries the same or similar to Fig. 1 and Fig. 2. The queries and responses illustrated in Fig. 1 and Fig. 2 are comprised of a string of data that conforms to ISO/IEC 7816 specification. The baseband controller can choose to route the queries from the reader (21) to any secure element it chooses for processing. Some of the options would include:

- a. Routing ISO/IEC 7816-4 data through the NFC interface (18) to an embedded secure IC over its proprietary connected SE interface (25)
- b. Routing ISO/IEC 7816-4 data through the NFC interface (18) through the baseband processor (17), to an attached SIM card (20)
- c. Routing ISO/IEC 7816-4 data through the NFC interface (18) through the baseband processor (17), to an attached SD, miniSD, or microSD card that contains an SE
- d. Routing ISO/IEC 7816-4 data through the NFC interface (18) through the baseband processor (17), over a data connection (27),(28),(29),(36),(35),(30) to a remote data server (32) using TCP/IP

All options a., b., c., and d. use APDU data to exchange information between the RFID reader (21) and the applications located in an SE located in the mobile device (19) or a remote SE (34). It is important to note that the remote SE (34) could also be created with software and emulated within the remote system (31). The interrogation example mapped out in fig. 3 and 4 could easily be implemented on this system in all 4 modes a., b., and c., and d. above. This suggests that the remote system SE (34) could perform the identical interrogation on a remote secure element (19).

[0042] It is important to note that this document and this figure is suggesting that at the ISO/IEC 7816-4 (APDU) level, an entire interrogation similar to those described in Fig. 1, and Fig. 2 can be carried out from a RFID POS reader (21) through an NFC enabled mobile

device (26), through a data connection over the internet (35) to a remote system (31) that contains the actual SE (34). An example of reader commands is illustrated in element (38) as a paypass reader. The paypass reader (38) shows the proper sequence of ISO/IEC 7816-4 APDU queries and responses that are pushed through the reader (21) and end up at the remote SE (38). Element (37) shows an example of APDU queries that are received by the remote SE (34) and the appropriate response that is issued as defined by the 7816-4 application for MasterCard PayPass. Elements (38) and (37) simply show how Figure 2 could be broken up so that the PayPass card could be hosted on a remote SE (34) on a remote system (31) and the paypass reader could be an RFID POS (21).

[0043] Element (31) describes a remote system with an external connection to the internet (30) and internal connections to an array or plurality of SE readers (33) that are each connected to a SE (34). A server or set of servers (32) is responsible for marrying the connections originating at the mobile NFC device (26) to the correct SE (34) within the remote system (31).

[0044] The data connection described in Fig. 5 (27),(28),(29),(36),(35),(30) is a TCP/IP connection that is offered by most cellular carriers over a cellular network and cellular towers (29) & (28). The TCP/IP connection can run socket software that allows for raw data to be transmitted from one end of the data connection (26) and the other (31) and visa versa. The data packets within the socket software can be configured to exchange data that contains ISO/IEC 7816-4 data.

[0045] Fig. 6 describes a remote system that is capable of bridging a data (TCP/IP) connection through the internet (39) to a single addressable SE reader (49) and SE (50). Elements (40) and (41) show how a data link (TCP/IP) (40) can be used to pass ISO/IEC 7816-4 APDU data (41) to a remote server (42). In this example the remote system is identified on the internet through the IP address (43). The remote system is comprised of a remote server (42) that routes the connection to an internet network of attached SE Array Managers (46). The TCP/IP data (40) that enters this remote system and is routed to an internal SE Array Manager device over TCP/IP (44), contains data that uses the protocol for ISO/IEC 7816-4 APDU data (41) and (45). Each SE Array Manager (46) contains an

internally unique IP address (48) within its TCP/IP server (47). Each SE Array Manager's TCP/IP server is responsible for receiving ISO/IEC 7816-4 APDU data (45) and (51) and routing it to the appropriate addressable SE reader (49) and SE (50).

[0046] One method to create a communication channel shown in Fig. 6 from the remote system to the mobile device over TCP/IP using socket server and client methods. Identification data from the mobile device can be used to setup a socket connection all the way through the remote server socket server (42) to the SE Array Manager TCP/IP socket server (47). The data that is sent over the socket server and client can be formatted to be ISO/IEC 7816-4 APDU data. The APDU query would enter the socket server (47) and be routed to the appropriate SE reader (49) and SE (50) and the response APDU would be sent from the SE (50) and SE reader (49) back to the remote mobile device through the SE Array Manager socket server (48), the remote system socket server (42), and through the internet (39) and be received by the socket client on the remote mobile device.

[0047] Fig. 6 also describes a plurality of remote SEs that are each addressable and can be accessed by a plurality of remote mobile devices independently. The descriptions in the above paragraphs describe how a single remote mobile device would connect to a remote system and specifically a single remote SE to complete a transaction. This same scenario is intended to go on congruently through this same system to different SE's in the system from different remote mobile devices.

[0048] Fig. 7 describes a table in a database that could be used to identify which remote SE within a remote system described in Fig. 6 that a user and particular mobile device can be attached to. Element (54) is a unique row identifier in the table. Each row contains related data. The other columns of this table are the User ID (52) and the SE Address (53). The SE address is the unique address within the remote system for a particular SE. This table in Fig. 7 could be used to properly match a remote user or remote mobile device with the address of a particular SE.

[0049] Fig. 8 describes one authentication flow for allowing connection over a data connection between a mobile device and remote hosted secure element. Element (56)

describes how a mobile device that supports NFC is initiated and presented to a RFID POS reader in order to make a payment transaction. The phone is placed into a mode that is referred to as card emulation mode where the NFC interface on the phone pretends to be contactless RFID card. The phone has a bit more control to select which card is presented to the POS. The subject of this patent describes how the NFC mobile device has the ability to use a SE for the transaction that is not physically located on the mobile device. This is done by creating a data connection to a remote SE for which is used for the payment transaction. In element (57), while the phone is being placed into card emulation mode, the connection to the remote SE that will be used for emulation is attempting to connect. There is a chance that the connection is already open in which case the flow in Fig. 8 will simply allow the ISO/IEC 7816-4 APDU data to pass directly through the connection to the remote SE and back (63) successfully completing the transaction (64). There is also a chance that the connection to the remote SE does not exist and needs to be created. In order to connect to the remote system and create the final connection to the correct SE for that user or mobile device, the device must be authenticated to the remote system.

[0050] One method of authentication to the remote system is described in Fig. 8., and further detailed below. The authorization to the remote system can be initiated using HTTPS/SSL web services. The mobile device connecting to the remote system is able to pass various credentials to the remote system such as user ID, passwords, PIN, “gesture signature”, and so on securely to the remote system for mobile device validation (59), upon successful authorization and validation, the remote system opens up a communication channel to the appropriate SE within the remote system and creates a handle to that communication channel that can be used to access it from the remote mobile device. The remote system can securely pass back over HTTPS/SSL a shared encryption key and handle to the communication channel that can be used for continued communication over that communication channel through a TCP/IP data socket (62). If the authorization fails (65), the connection to the remote SE is not opened, and the process ends. When the remote device receives the shared encryption key and handle to the communication channel to a particular SE on the remote system, the ISO/IEC 7816-4 APDU queries from the RFID POS can be passed to this remote hosted SE through a socket connection and the data can be encrypted with the shared

encryption key. The remote system can decrypt the data and send it to the correct SE within the remote system. The remote system can then send the response APDU from the SE back to the remote mobile device in a similar manner. The remote mobile device and forward this response APDU back through the NFC interface to the RFID POS reader.

[0051] Fig. 9 illustrates the authorization and communication process in more detail. The vertical line (66) represents the RFID POS entity. The vertical line (67) represents the mobile device. The vertical line (68) represents the remote system authentication server, and the vertical line (69) represents the remote hosted SE.

[0052] To open a communication socket between the RFID POS (66) and the remote SE (69), authorization over SSL is initiated and credentials are sent to the server (70). The server verifies the credentials and sends back a successful response (71) which contains a handle to a communication channel and an encryption key. The mobile device can then open a channel to the remote SE. At that point APDU query and response APDUs can be sent securely between the RFID POS reader and the remote POS and back. Element (72) shows how the APDU query is emitted from the RFID POS reader to the mobile phone (72) which encrypts that APDU query and forwards it on to the remote system (73) and on to the remote SE (74). The return APDU response from the SE is delivered back to the RFID POS in a similar manner (75),(76),(77).

[0053] ABSTRACT

A method and apparatus for creating a remotely hosted plurality of secure elements that can be connected to a single mobile NFC device and interrogated by a RFID POS reader through the mobile NFC device over a data connection between that mobile NFC device and remote hosted secure element.

Fig. 1

-Command – Response APDU Flow

Secure Element
Banking Application

Interrogator

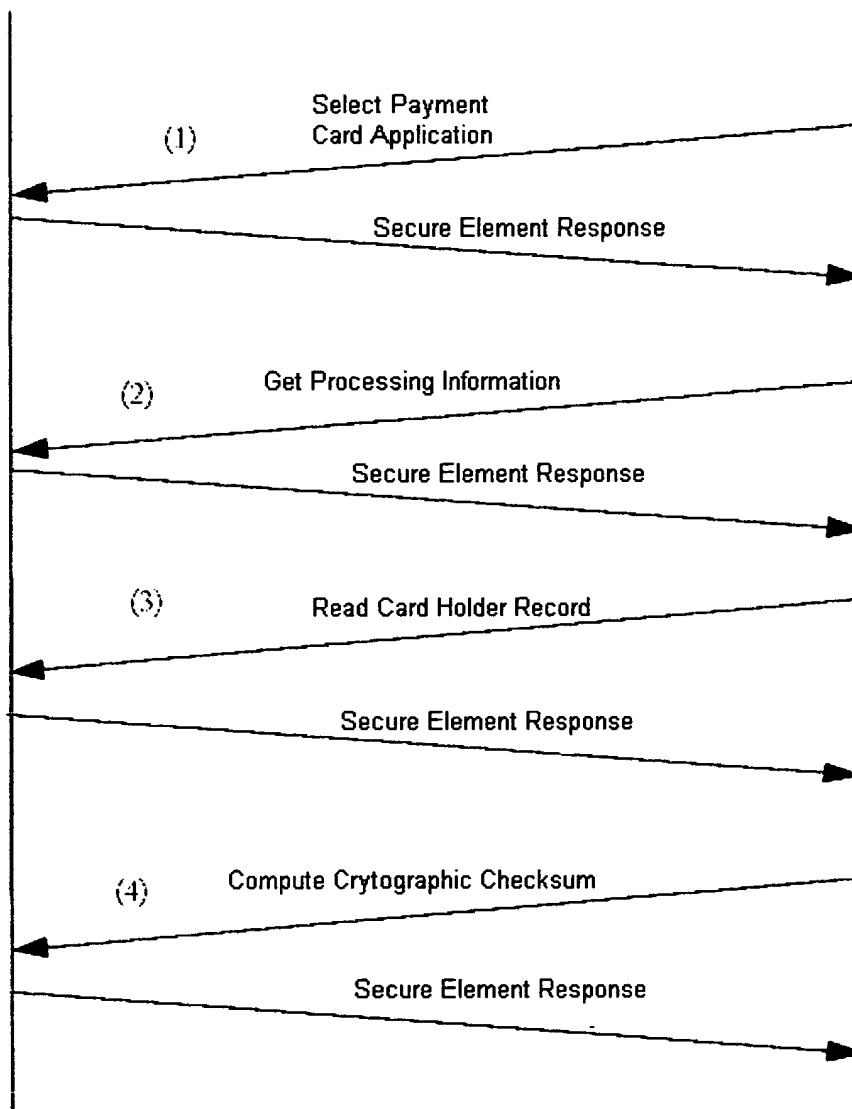


Fig. 2

—Command – Response APDU Flow

PayPass card

PayPass reader

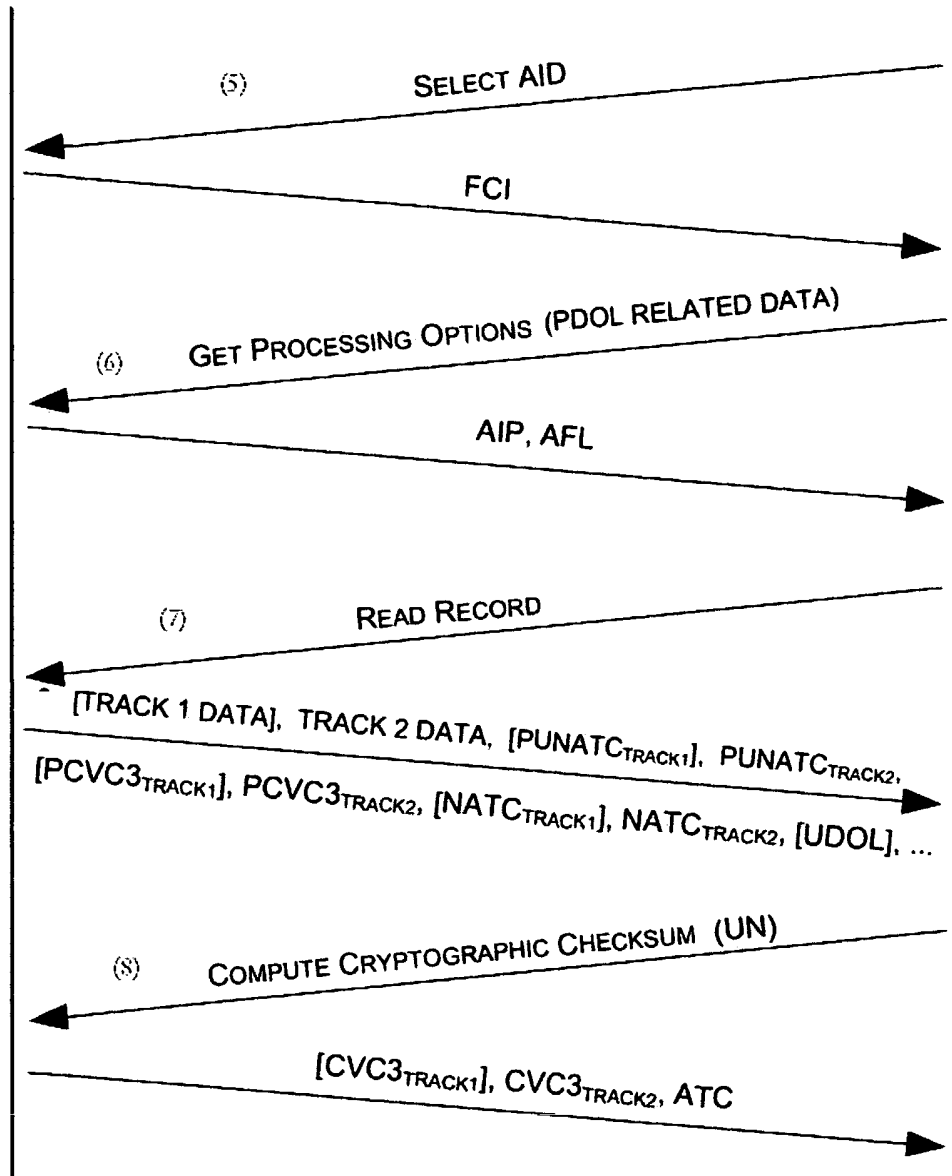


Fig. 3

Transaction Processing

```

nUN:      3
UN:       00 00 08 99
(9)  ATC:      00 5E
      CVC3TRACK1: 2 least significant bytes of
                        DES3(KDCVC3) [77 80 00 00 08 99 00 5E]
      CVC3TRACK1: FB C7
      CVC3TRACK2: 2 least significant bytes of
                        DES3(KDCVC3) [99 D3 00 00 08 99 00 5E]
      CVC3TRACK2: B8 92

```

- **SELECT PPSE Command**

```

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

```

- **SELECT AID Command**

```

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

```

- **GET PROCESSING OPTIONS Command**

```

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

```

- **READ RECORD Command**

```

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

```

- **COMPUTE CRYPTOGRAPHIC CHECKSUM Command**

```

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

```

Fig. 4

The *PayPass* reader generates the track 2 data to be included in the authorization message as follows:

```

CVC3TRACK2 in base 10: 47250
ATC in base 10: 94 (15)
=> track 2 data: 54 13 12 34 56 78 4E 00 D0 90 61 01
                  9 094 99 899 250 3 F
                  ↑↑↑ ↑↑↑ ↑↑↑ ↑
                  ATC UN CVC3TRACK2 nUN

```

The *PayPass* reader generates the track 1 data to be included in the authorization message as follows:

```

CVC3TRACK1 in base 10: 64455
ATC in base 10: 94 (16)
=> track 1 data: 42 35 34 31 33 31 32 33 34 35 36 37 38 34 38 30
                  30 5E 53 55 50 50 4C 49 45 44 2F 4E 4F 54 5E 30
                  39 30 36 31 30 31 33 33 34 35 35 33 33 33 30 39
                  34 32 32 32 32 32 38 39 39 31 31 31 31 33
ASCII dump: B5413123456784800^SUPPLIED/NOT^0906101
              3345533309422222289911113
              ↑↑↑ ↑↑↑ ↑↑↑ ↑
CVC3TRACK1 ATC UN nUN

```

Fig. 5

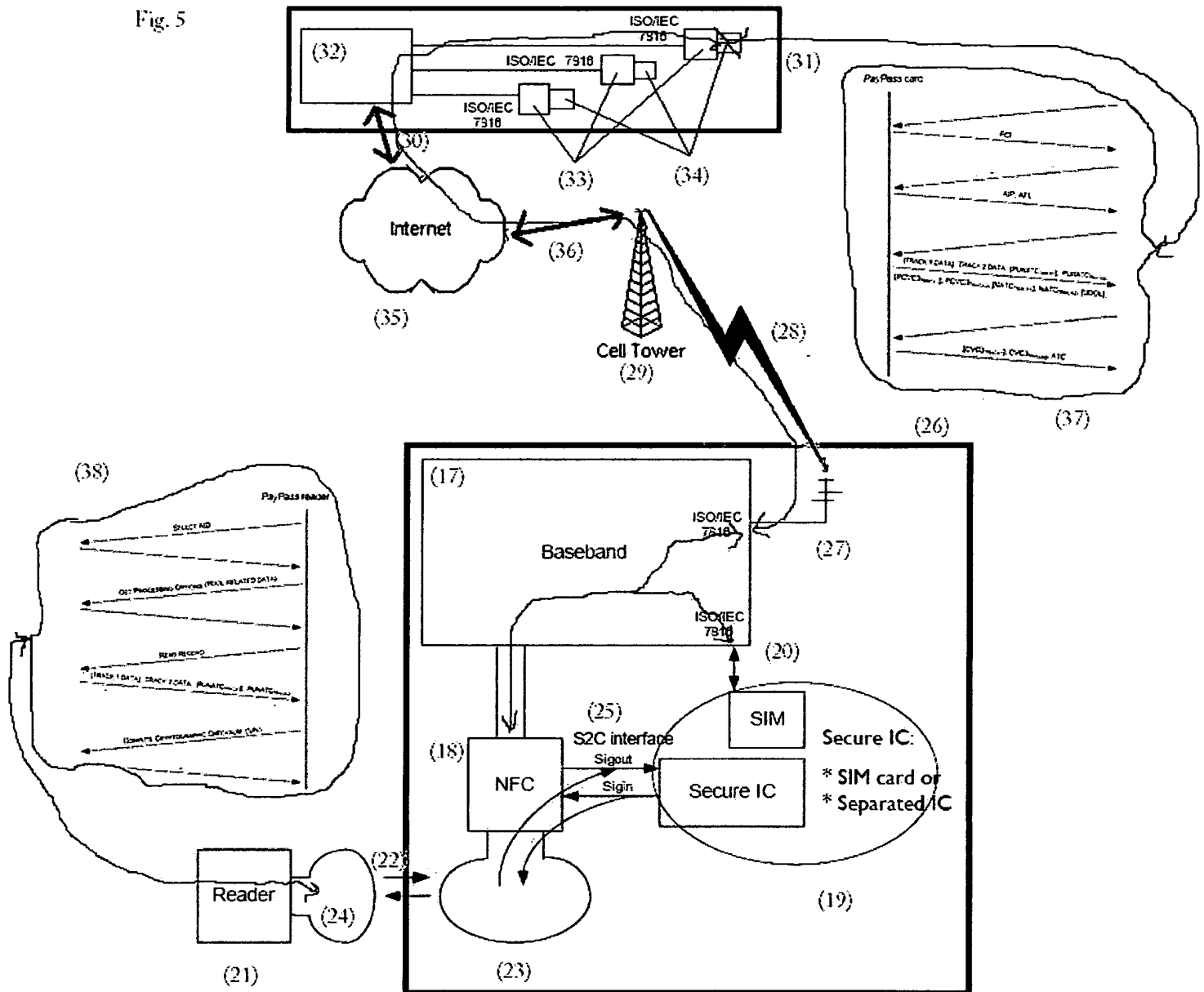


Fig. 6

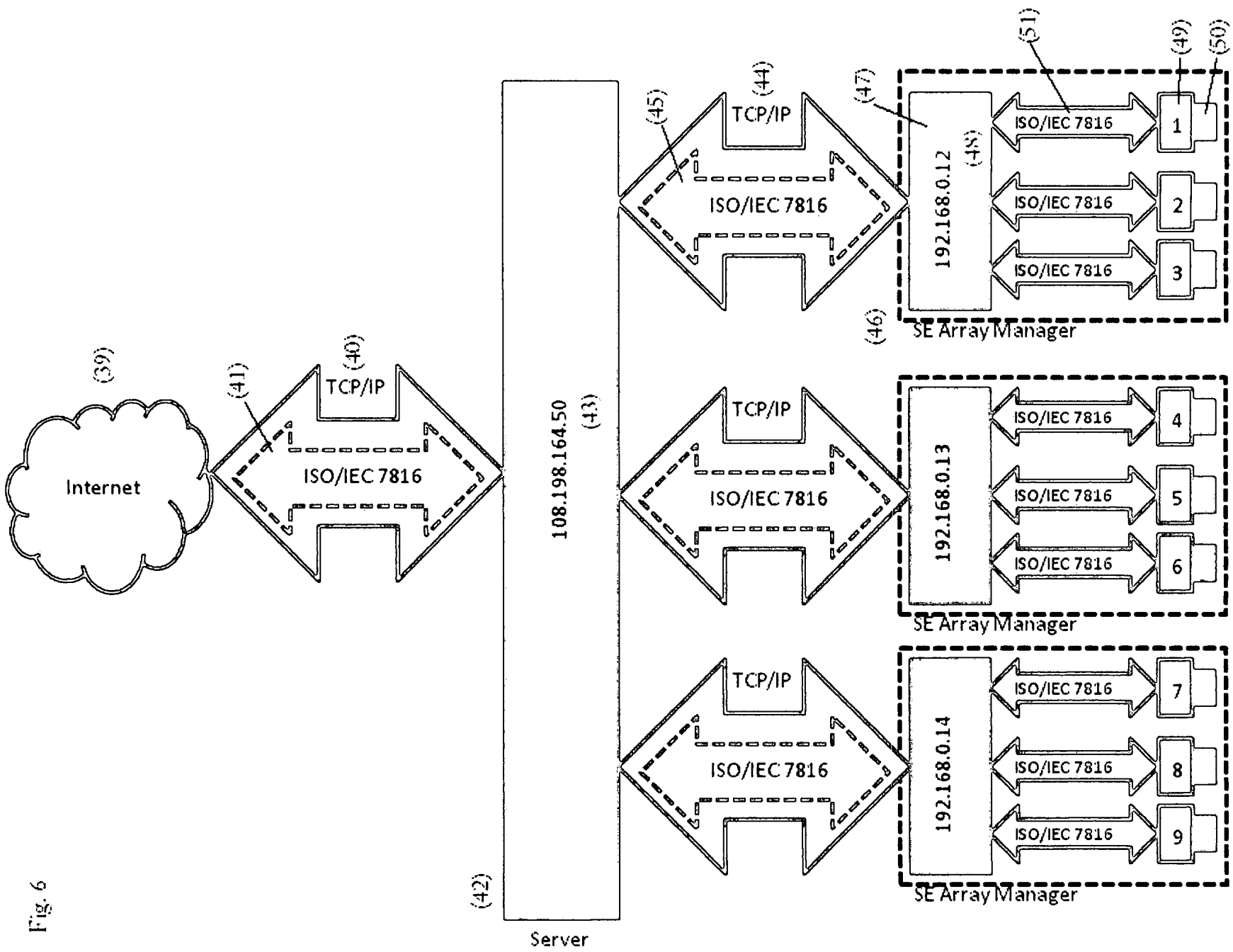


Fig. 7

(52)		(53)
	User ID	SE Address
(54)	1 doug@elementalknowledge.com	7
	2 ravi@intel.com	6
	3 tom@intel.com	8
	4 ken@intel.com	2
	5 mark@intel.com	4
	6 greg@intel.com	9
	.	.
	.	.
	.	.

Fig. 8

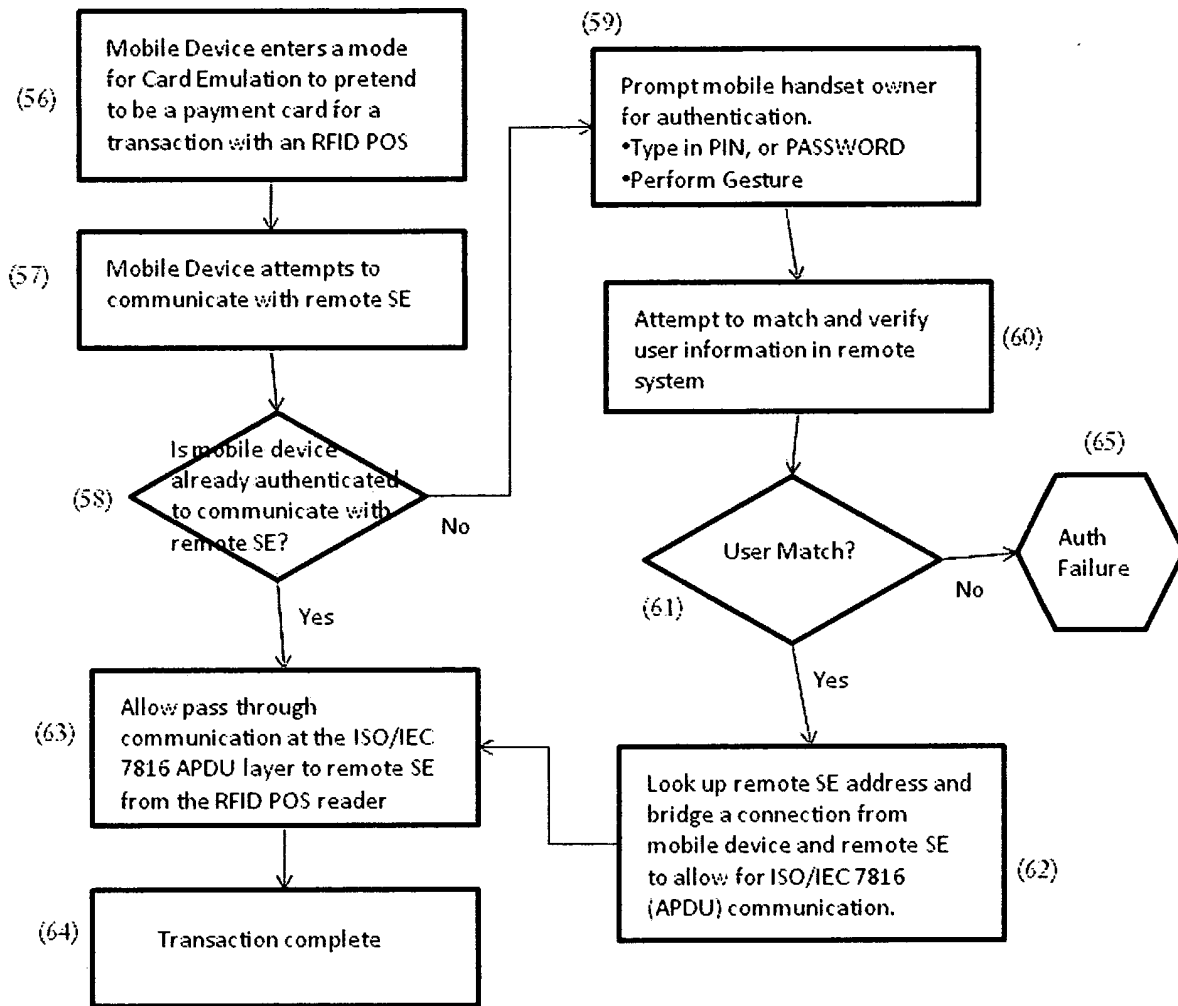


Fig. 9

