

02480
032612
U.S. PTO

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.

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

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 8656046546 Email

ENCLOSED APPLICATION PARTS (check all that apply)

☐ Application Data Sheet. See 37 CFR 1.76 ☐ CD(s), Number of CDs _____

☒ Drawing(s) Number of Sheets 17 ☐ Other (specify) _____

☒ Specification (e.g. description of the invention) Number of Pages 34

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: _____

TOTAL FEE AMOUNT (\$) \$110

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 _____

TYPED or PRINTED NAME _____

REGISTRATION NO. _____

(if appropriate)

TELEPHONE _____

Docket 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>8656046546</u>	Email _____

ENCLOSED APPLICATION PARTS (check all that apply)

☐ Application Data Sheet. See 37 CFR 1.76	☐ CD(s), Number of CDs _____
☒ Drawing(s) Number of Sheets <u>17</u>	☐ Other (specify) _____
☒ Specification (e.g. description of the invention) Number of Pages <u>34</u>	

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.	\$110
☒ 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.	TOTAL FEE AMOUNT (\$)
☐ The Director is hereby authorized to charge the filing fee and application size fee (if applicable) or credit any overpayment to Deposit Account Number: _____	

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.

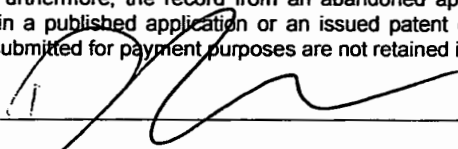
The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ 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 3/26/2012

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

TELEPHONE 865 604 6546 Docket Number: _____

File No. 10011.PV
New **PROVISIONAL APPLICATION**
Applicant(s): C. Douglas YEAGER

Date: Mar. 26, 2012

Title: REMOTE HOSTED SECURE ELEMENT REPOSITORY

Enclosures:

- (1.) Check #1134 in the amount of \$110
- (2.) Provisional Application for Patent Cover Sheet (PTO/SB/16) (2 pp.)(in duplicate)
- (3.) Specification (34 pp.)
- (4.) Drawings (17 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.

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: 10011.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] Alternatively, the present invention uses the base-band processor on the mobile device to do one or all of the following tasks:

- a. Begin a TCP/UPD/IP connection to a remote merchant website or remote merchant POS system.
- b. Interrogate an SE on a remote system in order to build or acquire pieces of card present data such as Track 1 and Track 2 data.
- c. Deliver the Track1 and Track2 data or pieces of that data directly to the remote merchant website or remote merchant POS system.

[0014] Alternatively, the present invention uses the base-band processor on the mobile device to do one or all of the following tasks:

- a. Begin a connection to a remote terminal configured to interrogate using 7816-4 data over TCP/UDP/IP.
- b. Receive queries through this remote terminal interface over TCP/UDP/IP interface from the remote terminal 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 remote terminal that is configured to receive the 7816-4 data over TCP/UDP/IP.

[0015] 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.
- d. Properly bypass a remote SE or remote SE representation and respond with static or persistent data that may represent transaction data that could be used in a contactless transaction.

[0016] 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 or remote terminal and an NFC mobile device. The interrogation may be performed as set forth by payment card standards such as MasterCard PayPass, VISA Contactless, AMEX Express Pay, and Discover Zip.

[0017] The data link or data connection and communication between the mobile device and the remote system or remote terminal stated above could be carried out over standard TCP/UDP/IP services that are currently available on mobile devices.

[0018] 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.

[0019] 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.

[0020] Some additional advantages of the present invention also include:

- a. The ability to make a card present transaction with a mobile device that does not contain NFC capability
- b. The ability to make a card present transaction with a merchant website or merchant POS that may not support NFC capability

[0021] Some additional advantages of the present invention also include the ability to substitute commonly accepted Track 1 / Track 2 specific format data elements with any open or closed loop data values and send that data over an arbitrary application AID at an RFID POS

[0022] 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.

[0023] 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/UDP/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/UDP/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.

[0024] 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.

[0025] 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.

[0026] 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.

[0027] 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.

[0028] 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.

[0029] Also, in this document, the concept of using TCP/UDP/IP sockets to enable a communication channel between a RFID POS reader and a single SE within remote system containing a plurality of SEs.

[0030] Also, in this document, the concept of authenticating over SSL to enable a TCP/UDP/IP socket communication channel between a RFID POS reader and a single SE within a remote system containing a plurality of SEs.

[0031] 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.

[0032] As with some data networks that pass TCP/UDP/IP information, there are network delays and latency that contributes to delay for round trip information to a destination. With the present invention, the data is intended to go round-trip from the mobile device to the remote SE. Many payment applications that communicate with an SE may require a plurality of queries and responses to the SE for each transaction carried out by an interrogation from the POS RFID reader. Each of these query and responses to the SE would be subject to network delays and latency. Prolonged delay during a transaction with the RFID POS could cause a worse user experience. An example of a delay was recorded during testing:

- a. Card transaction with a MasterCard PayPass plastic card and a RFID POS reader was measured to take ~200ms
- b. Card transaction with a remote SE programmed with the MasterCard PayPass application over a 3G network managed by Verizon through a mobile handset was measured to take ~600ms

[0033] The remote SE took ~400ms longer in the above example due to network latency and delay during the SE interrogation.

[0034] The concept of query/response caching will be discussed in this document. A cache is a component that transparently stores data so that future requests for that data can be served faster. The data that is stored within a cache might be values that have been computed earlier or duplicates of original values that are stored elsewhere. If requested data is contained in the cache (cache hit), this request can be served by simply reading the local cache, which is comparatively faster than accessing the remote source. Otherwise (cache miss), the data has to be recomputed or fetched from its original storage

location, which is comparatively slower. Hence, the more requests can be served from the local cache the faster the overall system performance is.

[0035] A local cache (cache system located on the mobile device) can be implemented for use in the present invention. Many of the responses to a 7816-4 APDU command or queries are static and unchanging in a payment application on a SE. For this reason, a cache system could successfully be designed to respond locally for these static information requests with the known 7816-4 APDU data responses and only query real time to the remote SE in the event the response 7816-4 APDU data is dynamic or changing with each transaction. This should limit the number of round trip data requests to the remote SE. Because each round trip request to the remote SE is subject to network delay and latency, a relatively significant total transaction time savings can be realized.

[0036] The main advantages of implementing a caching system in the current invention are:

- a. To save over-all time to perform a full transaction with a payment card application between a RFID POS reader through a mobile device to a remote SE.

[0037] In this document, similar to transaction caching above, the concept of one hundred percent transaction caching will be discussed. This is a concept that allows the mobile device to request a cache from the remote authentication system that encompasses a single entire transaction. This cache can be stored securely in non-persistent memory (RAM) and used only at the time of transaction with the remote RFID reader in the future.

[0038] Building on the concept of local caching above, the main advantage of this concept is:

- a. To allow the mobile device and remote RFID reader to interact exclusively with each other at the time of transaction without performing a remote request that may experience a network delay.

[0039] The concept of interacting with a remote terminal will be covered in this document. Just as a remote RFID interrogator or reader would interact with the mobile device, a mobile device that does not have the ability to interact with an NFC reader, by be interrogated by a remote terminal using the same data protocol (7816-4) over TCP/UDP/IP. The main advantages of this concept are:

- a. Allowing interaction with a remote SE or SE software representation that is associated with a particular device with a remote terminal
- b. Tasks that a remote terminal may implement include personalization or programming of a particular SE
- c. A remote terminal may also interrogate a remote SE that is associated with a mobile device in order to authenticate or transact with a particular application that resides on that remote SE or remote SE representation

[0040] The concept of a mobile device transacting with a remote SE or remote SE representation in order to receive Track 1 or Track 2 equivalent data or parts of that data for use with a remote merchant website or remote merchant POS system over TCP/UDP/IP will be covered in this document. Some advantages of this concept include:

- a. Using card present data for authorization of a purchase from a remote merchant website
- b. Using card present data for authorization of a purchase from a remote merchant POS terminal in the event the merchant POS terminal does not support NFC
- c. Using card present data for authorization of a purchase from a remote merchant POS terminal in the event the mobile device does not support NFC

[0041] The concept of using static or persistent magnetic stripe data and masquerading that data into a contactless transaction is discussed in this document. Some advantages of this concept include:

- a. Many existing merchant closed loop payment and open loop payment card programs do not support NFC or RFID transactions. A mobile device may be able to still use these types of cards to make a transaction with a POS or remote terminal or website.

[0042] The concept of a software representation of a SE is discussed in this document. The advantages of this concept include:

- a. Replacing a concept that is known to be a hardware concept with a software solution saves in cost as well as space requirements

[0043] The concept of masquerading various types of track data over multiple NFC or RFID applications is discussed in this document. Some advantages of this concept include:

- a. Some NFC or RFID applications such as VISA PayWave may not require input from the RFID POS terminal in order for it to build the Track 1 or Track 2 equivalent data. In this scenario, any track data value can be substituted into the format of the application in order for the end result of the Track1/Track2 data to be equivalent to an authentic magnetic stripe format for any particular application. This allows from a closed loop payment schema to be executed over the VISA PayWave AID in order to be processed uniquely as such by a merchant POS.
- b. Just as above, it is possible to do a transaction with a remote PayPass card and substitute the resulting Track1/Track2 information into the appropriate locations of the VISA PayWave AID application in order for the resulting Track1/Track2 data to be conceived by the RFID POS terminal and passed to the merchant POS as a PayPass card.
- c. In this manner a PayPass card terminal that is not local to the transaction can be used to make a transaction ahead of the actual time of transaction and passed to the merchant POS at transaction time without real time interaction with the PayPass SE. This saves network latency.

[0044] The concept of using an application within the operating system of a mobile device to emulate the 7816-4 data layer of an SE is discussed in this document. Some advantages of this concept include:

- a. Bypassing or not using SE hardware in order to make a transaction from some other form of logic on the handset
- b. Some applications that interact between the POS and a credential may not require an SE as the credential storage area. In these cases, a software application may be sufficient in handing the queries from the remote RFID POS.

Brief Description of the Drawings

[0045] Fig. 1 illustrates the command and response APDU (Application Protocol Data Unit) flow between a reader and an SE.

[0046] 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

[0047] Fig. 3 illustrates the raw data of a transaction between a reader and an SE

[0048] Fig. 4 illustrates the format for which the reader is expected to deliver the results of the previous interrogation

[0049] Fig. 5 illustrates a diagram of a mobile device that contains NFC capabilities and how that device allows access to secure elements

[0050] Fig. 6 illustrates a diagram of an addressable array of remote hosted SEs

[0051] Fig. 7 illustrates a User ID SE address lookup table

[0052] Fig. 8 illustrates an authorization flow for using a remote hosted SE

[0053] Fig. 9 illustrates a data flow diagram including authorization between a mobile device and a remote hosted SE

[0054] Fig. 10 illustrates an example of caching being used during a MasterCard PayPass transaction between a RFID POS and a remote SE

[0055] Fig. 11 illustrates an example of 100% transaction caching being used during a Visa PayWave transaction between a mobile phone and the remote System Auth Server and then using the cached transaction data to make a local transaction from the RFID POS and a mobile device at a later point in time.

[0056] Fig. 12 illustrates an example of a transaction flow between a remote terminal server and a remote SE facilitated through a mobile handset entirely over TCP/UDP/IP

[0057] Fig 13 illustrates an example of a mobile device conducting a transaction with a remote SE and building T1/T2 equivalent data and sending it over TCP/UDP/IP to a remote POS terminal or merchant POS

[0058] Fig 14 illustrates an example of using a remote hosted auth server to deliver static T1/T2 data without the use of a Remote SE to a mobile handset for use in a transaction with an RFID POS at a later point in time

[0059] Fig. 15 illustrates how a system could be created to simulate a remote hosted bank of SEs within a single computer

[0060] Fig 16 illustrates how proprietary or intermingled T1/T2 data can be used over a plurality of AID applications to be delivered to the processor

[0061] Fig 17 illustrates how an operating system with individual applications could be used to simulate a SE

DETAILED DESCRIPTION

[0062] 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.

[0063] 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.

[0064] 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.

[0065] 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.

[0066] 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/UDP/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).

[0067] 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).

[0068] 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).

[0069] The data connection described in Fig. 5 (27),(28),(29),(36),(35),(30) is a TCP/UDP/IP connection that is offered by most cellular carriers over a cellular network and cellular towers (29) & (28). The TCP/UDP/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.

[0070] Fig. 6 describes a remote system that is capable of bridging a data (TCP/UDP/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/UDP/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/UDP/IP data (40) that enters this remote system and is routed to an internal SE Array Manager device over TCP/UDP/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/UDP/IP server (47). Each SE Array Manager's TCP/UDP/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).

[0071] One method to create a communication channel shown in Fig. 6 from the remote system to the mobile device over TCP/UDP/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/UDP/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.

[0072] 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.

[0073] 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.

[0074] 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.

[0075] 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/UDP/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.

[0076] 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.

[0077] 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).

[0078] Fig. 10 illustrates an example of caching being used during a MasterCard PayPass transaction between a RFID POS and a remote SE. The vertical line (78) represents the RFID POS entity. The vertical line (79) represents the mobile device. The vertical line (81) represents the remote system authentication server, and the vertical line (82) represents the remote hosted SE. The vertical line (80) represents the caching system on the mobile device.

[0079] The MasterCard PayPass specification indicates that the response to the Select PPSE APDU (83) always be the same:

- a. APDU to the card for Select PPSE APDU:

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

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

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

This would indicate that the response to this APDU can be cached and the caching system (80) can respond to this APDU without making a query all the way to the remote SE over the data network.

[0080] The MasterCard PayPass specification indicates that the response to the Select PayPass AID APDU (84) always be the same:

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

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

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

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

This would indicate that the response to this APDU can be cached and the caching system (80) can respond to this APDU without making a query all the way to the remote SE over the data network.

[0081] The MasterCard PayPass specification indicates that the response to the GPO (Get Processing Options) APDU (85) always be the same:

- a. APDU to the card for GPO APDU:

80 A8 00 00 02 83 00 00

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

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

This would indicate that the response to this APDU can be cached and the caching system (80) can respond to this APDU without making a query all the way to the remote SE over the data network.

[0082] The MasterCard PayPass specification indicates that the response to the Read Record APDU (86) always be the same for a particular card that has been personalized, but will be different from personalized card to a different personalized card:

- a. APDU to the card for Read Record APDU:

00 B2 01 0C 00

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

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

This would indicate that the response to this APDU can be cached and the caching system (80) can respond to this APDU without making a query all the way to the remote SE over the data network, UNLESS the card on the SE has changed to a different card, in which case the caching system should send this command to the remote SE for processing.

[0083] The MasterCard PayPass specification indicates that the request and the response to the Compute Cryptographic Checksum APDU (87) always will be different for each transaction. This means that this APDU will always need to be processed by the actual remote SE through the data network. Element (93) indicates the estimated or example of network processing time for this single APDU query and response (87). The over-all example in Fig. 10 illustrates how there is potentially only a single query and response that need to happen in real time over the data network (93) as a result of implementing a caching system.

[0084] In this specific example in Fig. 10, Element (88) illustrates one method to maintain the proper state of the remote SE (82) when a caching system is used. It is important that the remote SE (82) maintain the same processing state as the system is expecting when introducing a caching system. For this reason, it is important to actually issue the APDU commands to the remote SE in order to bring that SE to the appropriate system state. The dashed line illustrates how these ghost commands would need to be issued by the remote system in order for the SE to maintain an up to date state. The elements (89),(90),(91), and (92) mirror the APDU queries and responses (83),(84),(85),(86) managed by the caching system (80).

[0085] Fig. 11 illustrates a slightly different caching concept. In this figure, the entire transactional sequence with all APDU queries and responses is cached at a separate time (102) prior to the actual transaction. In this example illustrated in fig 11, the RFID POS does not initiate the initial request to the remote authentication server (97), it is initiated by the mobile device application at some prior time from the actual RFID POS transaction. When the mobile device (95) makes a request to the remote system authentication server (97), the remote system authentication server either retrieves caching information from a database or other storage system or, if needed, makes queries with a Remote SE (99) as indicated by the dotted box in the figure with a read record request (100) to the remote SE (99). This example would be pertinent in the event that the response to the read record request (100) was dynamically changing data with each individual transaction with the SE. When all known responses to the remote SE transactional query are gathered, the entire set of caching

information can be passed back to the mobile device (95) as shown in the figure element (101). In element (101) the SE responses to Select PPSE, Select PayPass, GPO, and Read Record APDU is passed back to the mobile device all at once.

[0086] Element (102) illustrates an unknown time delay until the actual start of the RFID POS transaction (103). During this time delay the cached APDU query and response data can be stored safely in non-persistent memory or RAM in a cached format (96). An alternative would be to store this data safely through encryption techniques in a persistent manner.

[0087] Elements (104),(105),(106), and (107) illustrate the real time transaction with the an RFID POS at a later time (102) than the previous interaction with the remote authentication server. In this example each and every response APDU query that the RFID POS requested was replied to locally by the mobile device cache (96).

[0088] Fig. 12 closely resembles previous fig. 9. The main difference between fig. 9 and fig. 12 is that the RFID POS (66) represented in fig. 9 is replaced by a remote terminal (108) in fig. 12. The remote terminal in fig. 12 may communicate to the mobile device with the same exact APDU data protocol, but the main difference is that instead of the communication happening over 13.56 Mhz NFC radio, the communication would happen over TCP/UDP/IP data protocol. Aside from that difference, this figure and the example depicted was meant to illustrate that the same function and communication with a remote SE is possible no matter the raw communication base band (13.56 mhz carrier, or TCP/UDP/IP)

[0089] Fig. 13 illustrates the idea of a mobile device (131) having the capability to collect card present transaction data from a remote system authentication server (123) through many different illustrations in this document and use the card present data that was achieved from the Remote SE (124) and/or remote system authentication server (123) and present that data to a remote merchant web site or remote merchant point of sale (132) in order to make a more secure transaction with that remote merchant site or POS (132). In this example the mobile device contains the logic to parse through the APDU queries and responses to the remote SE (123) and remote system authentication server (123) and create properly formatted

track 1/track 2 equivalent data (179) that represents a card present payment transaction and pass that data or parts of that data directly to the merchant remote web site or remote POS (133) in order to consummate the payment transaction.

[0090] Fig. 14 is very similar to fig. 11 with one major difference. The difference is that the Remote SE is not used or not transacted with (137) in this example. The reason for this is that it is possible to use the architecture defined in the this document to delivery standard magnetic stripe data to an RFID POS (133) or remote terminal through contactless APDU commands (139), where the actual data inside the transactions is generated from standard magnetic stripe data and stored at the remote system authentication server (136). The magnetic stripe data could be populated into the remote system authentication server by simply swiping an existing magnetic stripe card with a magnetic stripe card reader and populating that data accordingly into the server (136) database. The transaction scenario is identical to Fig. 11 including the time delay prior to the actual transaction (138)(140) and the delivery of the transactional data from the server (136). This type of data substitution is possible with existing contactless APDU commands as defined in the Visa PayPave specification. That specification allows for a transaction with an RFID POS to be made using these commands:

- a. Select AID : element (11) fig. 3
- b. GPO: element (12) fig. 3
- c. Read Record: element (13) fig. 3

[0091] The read record command for Visa Paywave indicates there may be 3 data elements with the tags:

- a. Tag 57: Track 2 Equivalent Data
- b. Tag 5F20: Cardholder Name
- c. Tag 9F1F: Track 1 Discretionary Data

[0092] Specifically Tag 57 is a required tag that presents Track 2 Equivalent Data to the POS transaction. This format of the data is processed by the RFID POS and converted into ISO7813 data format. An example of this data conversion is this:

a. Raw Tag 57 data:

1) 54 13 12 34 56 78 48 00 D0 90 61 01 90 94 99 89 92 50 3F

b. Converted to ISO 7813 format:

1) ;5413123456784800=09061019094998992503?

[0093] As you can see above the data is almost a direct conversion, just adding the start sentinel ‘;’, the end sentinel ‘?’ and substituting the ‘D’ for the ‘=’ and removing the trailing padding ‘F’ gives the ISO7813 equivalent data. ISO 7813 data is used to send out for authentication processing for both magnetic stripe cards and contactless cards. Because of this, the actual data in Tag 57 could be gathered and populated from a regular magnetic stripe card as described in Fig. 14 tasks in the remote system auth server (136).

[0094] Extrapolating this concept displayed in Fig. 14 further, it would be possible to substitute any Track 2 data into tag 57 of the read record APDU response. Some substitution examples would be:

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

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

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

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

[0095] Fig. 15 illustrates the similarities from a hardware based SE (156) and a software representation of an SE (157). In the hardware based SE side of the figure (156), you will notice that the SE is literally a “chip” that could be mounted to a circuit board or located in a

physical plastic card or a SIM module, each form factor would have both a power (145) and ground (146) lines, and would also include a data line (150) that is configured to be half duplex communication over various serial data rates (149). The SE is a fully functional processor chip (147) that includes ROM, RAM, communications controller, EEPROM or persistent memory and a processor. It could easily locate and communicated to from a Network Server (148) provided the correct conversion hardware is in place to do so. The APDU data communication that is typical SE communication standard could then be extended to the Internet (152) over TCP/UDP/IP protocol.

[0096] The right side of fig. 15 shows how the function of the SE could easily be handled virtually (157) by a single computer or bank of computers. In this configuration, there is no separate hardware that is the SE, this hardware representation is actually done so entirely in software and contained inside a computer (153) with software function representations of each SE (154). The communication format of APDU 7816-4 structure can even be represented within the software of the computer (155). A typical computer or server has all the necessary components to complete the SE representation such as ROM, RAM, Persistent Memory, and a processor. The software architecture within the computer (153) can be arranged as such to divide and address many different SE representations (154) within a single computer. In the same manner the hardware based SE (156) was exposed to the Internet over TCP/UDP/IP, the software representation of the SE can also be exposed to the Internet.

[0097] The goal of Figure 15 is to illustrate how either architecture (156) and (157) could be seen as interoperable to the external world over the Internet. Fig. 15 also suggests that a software representation of SEs could be more scalable than using many hardware versions.

[0098] Fig. 16 illustrates how a merchant POS computer (165) is typically connected to both a RFID POS terminal (162) and a traditional magnetic strip terminal (164). The POS computer (165) is generally configured to receive ISO7813 Track 1/Track2 data (166) representations from either the RFID POS or the magnetic stripe terminal. At that point the POS computer (165) analyzes the data (166) to determine how to process it for purchase authorization. It may make a decision (167) based on the data (166) to process it as a "closed

loop” or proprietary merchant card (168), or an “open loop” payment card that can be used at many different merchant locations like MasterCard, VISA, AMEX, and DiscoverCard (169). The data within the data (166) is the main factor as to how this decision is made. Many times the first digit of the PAN (156) helps determine the type of card that is being used. PAN that starts with:

- a. 5 – is a MasterCard
- b. 4 – is a VISA
- c. 6 – is a DISCOVER
- d. 3 – is AMEX
- e. 0,2,3,7,8,9 is proprietary

[0099] Other format analysis techniques may also be used to determine type of card and how to process it. PAN analysis (156) is just one method.

[00100] Fig. 16 also shows 2 different types of cards being presented for payment. Element (163) is a traditional magnetic stripe card that is swiped at the swipe terminal (164). The magnetic data is scraped off of the stripe of the card and delivered to the POS computer (165) in ISO7813 format. Similarly the RFID POS terminal (162) delivers data to the POS computer (165) in ISO7813 format. Prior to the RFID POS (162) delivery to the POS terminal (166), the RFID POS (162) does a bi-directional interaction with the RFID card (157) or NFC mobile device (157) over the 13.56 Mhz radio interface (170).

[00101] The RFID POS (162) terminal is normally configured to interrogate a small subset of cards that may be in the field. For example, it may only look for cards that support 4 different applications such as:

- a. MasterCard (AID: a0000000041010) (159)
- b. VISA (AID: a0000000031010) (158)

c. AMEX (AID: a00000002501) (160)

d. DISCOVER (AID: a0000003241010) (161)

[00102] The RFID POS (162) uses AID Application Identifiers in order to determine which application is supported by the remote card (157). Most of the time, those applications are the ones listed above. It is possible, however, to deliver ANY track2 equivalent data through at least one of these application identifiers. It would be possible to deliver any track 2 equivalent data over Visa PayWave AID (a0000000031010). The technical details of this are outlined in the detailed description for Fig. 14. Essentially it makes it possible to deliver merchant based closed loop track 2 equivalent data over existing RFID POS terminal configured only to use open loop payment application AIDs.

[00103] Fig. 17 illustrates how interaction with a RFID POS (170) could happen completely independent of an SE within a mobile device operating system that supports independent applications. Fig. 17 illustrates the communication between the mobile device (171) and the RFID POS (170) through 13.56 Mhz radio (172) and APDU data structure (172). Fig. 17 also illustrates how SEs may be embedded (174) or attached to the phone (173) with a SIM card or (175) with a microSD card. The concept depicted in Fig. 17 bypasses options (173),(174),and (175) in order to emulate the SE responses strictly through software emulation within the operating system (176) through an individual application (177). The OS (176) may contain multiple applications that use different aspects of the mobile device and may also control which applications are allowed to use different hardware related features of the mobile device (171). In this example, App2 (178) and App1(177) both reside on the mobile device operating system (171). This example shows how the APDU data exchange is between RFID POS (170) and App1 (177). The data exchange bypasses the hardware layer and enters the operating system and is directed to the particular App1(177). App1 (177) contains the logic available to communicate with the RFID POS (170) and exchange transaction data (172).

[00104] 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

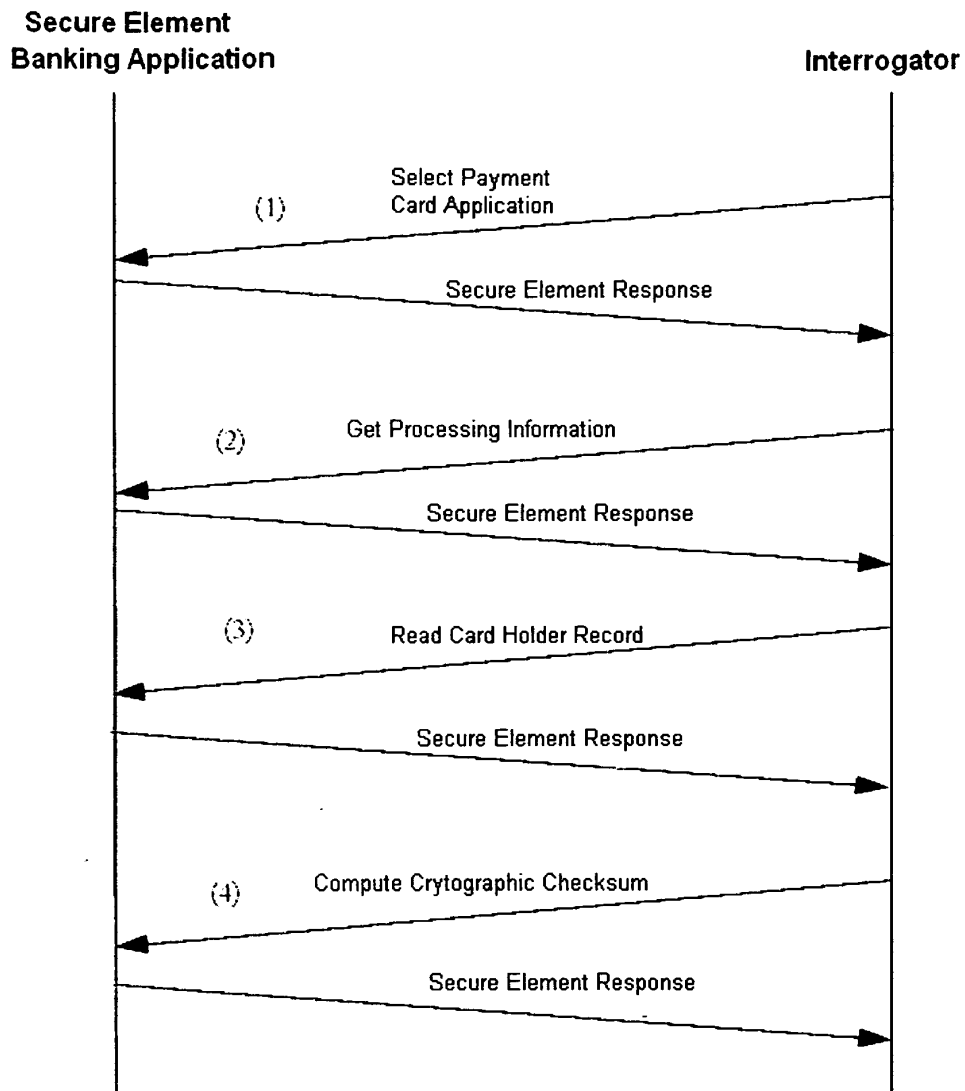
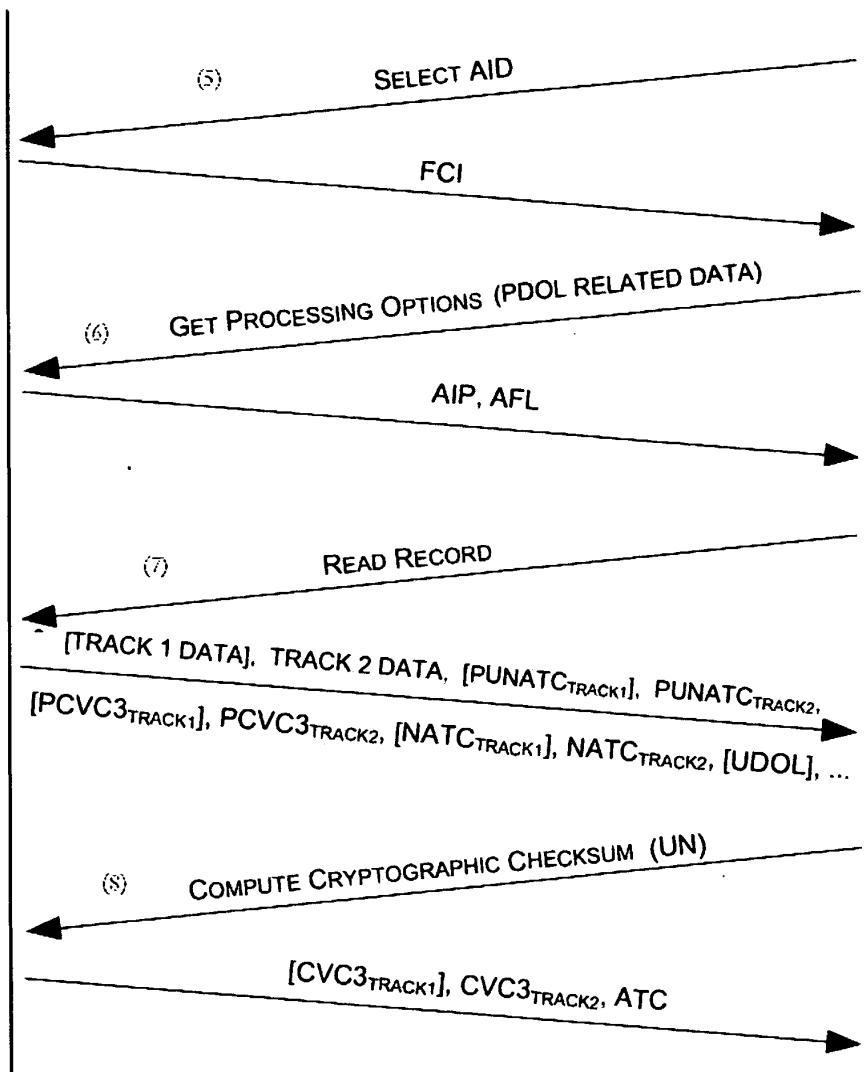


Fig. 2

—Command – Response APDU Flow

PayPass card

PayPass reader



Transaction Processing

(2)

CVC3TRACK1: 2 least significant bytes of
DES3(KD_{TRACK1}) [77 80 00 00 08 99 00 5E]

CVC3TRACK2: 2 least significant bytes of
DE83(KD_{ctrl}) 199 D3 00 00 08 99 00 5E1

- **SELECT PPSE Command**

- **SELECT AID Command**

- **GET PROCESSING OPTIONS Command**

- **READ RECORD Command**

- **COMPUTE CRYPTOGRAPHIC CHECKSUM Command**

Mastercard, Ex1003, p. 42

Fig. 4

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

```

CVC3TRACK2 in base 10: 47250          (15)
ATC in base 10:      94
=> track 2 data:    54 13 12 34 56 78 48 00 D0 90 61 01
                   9 094 99 899 250      3 F
                   ↑↑↑   ↑↑↑ ↑↑↑      ↑
                   ATC    UN CVC3TRACK2 nUN

```

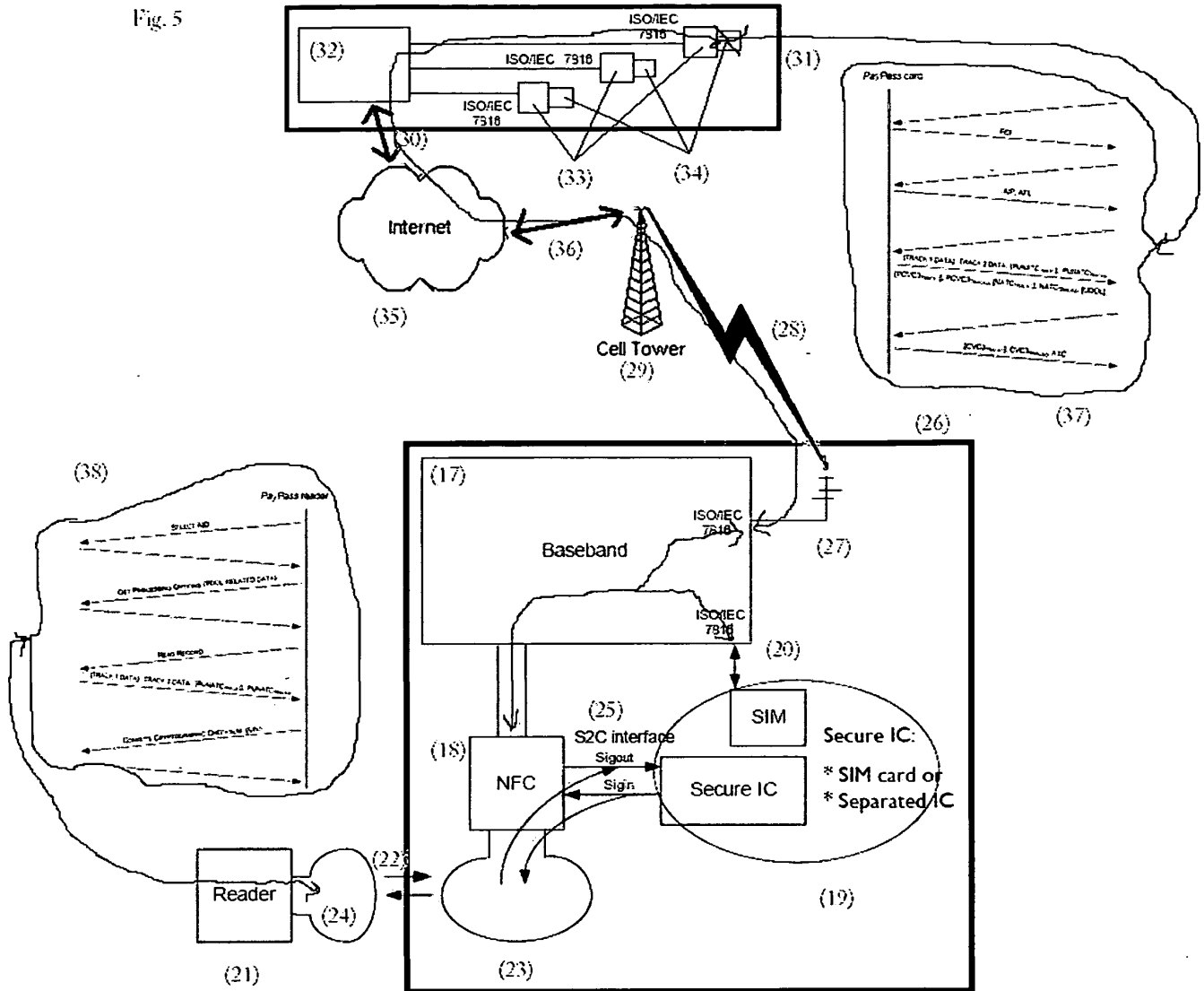
The *PayPass* reader generates the track 1 data to be included in the authorization message as follows:

```

CVC3TRACK1 in base 10: 64455          (16)
ATC in base 10:      94
=> track 1 data:    42 35 34 31 33 31 32 33 34 35 36 37 38 34 38 30
                   30 5E 53 55 50 50 4C 49 45 44 2F 4E 4F 54 5E 30
                   39 30 36 31 30 31 33 33 34 35 35 33 33 33 30 39
                   34 32 32 32 32 32 38 39 39 31 31 31 31 33
ASCII dump:        B5413123456784800^SUPPLIED/NOT^0906101
                   334553330942222289911113
                   ↑↑↑   ↑↑↑   ↑↑↑   ↑
                   CVC3TRACK1 ATC      UN      nUN

```

Fig. 5



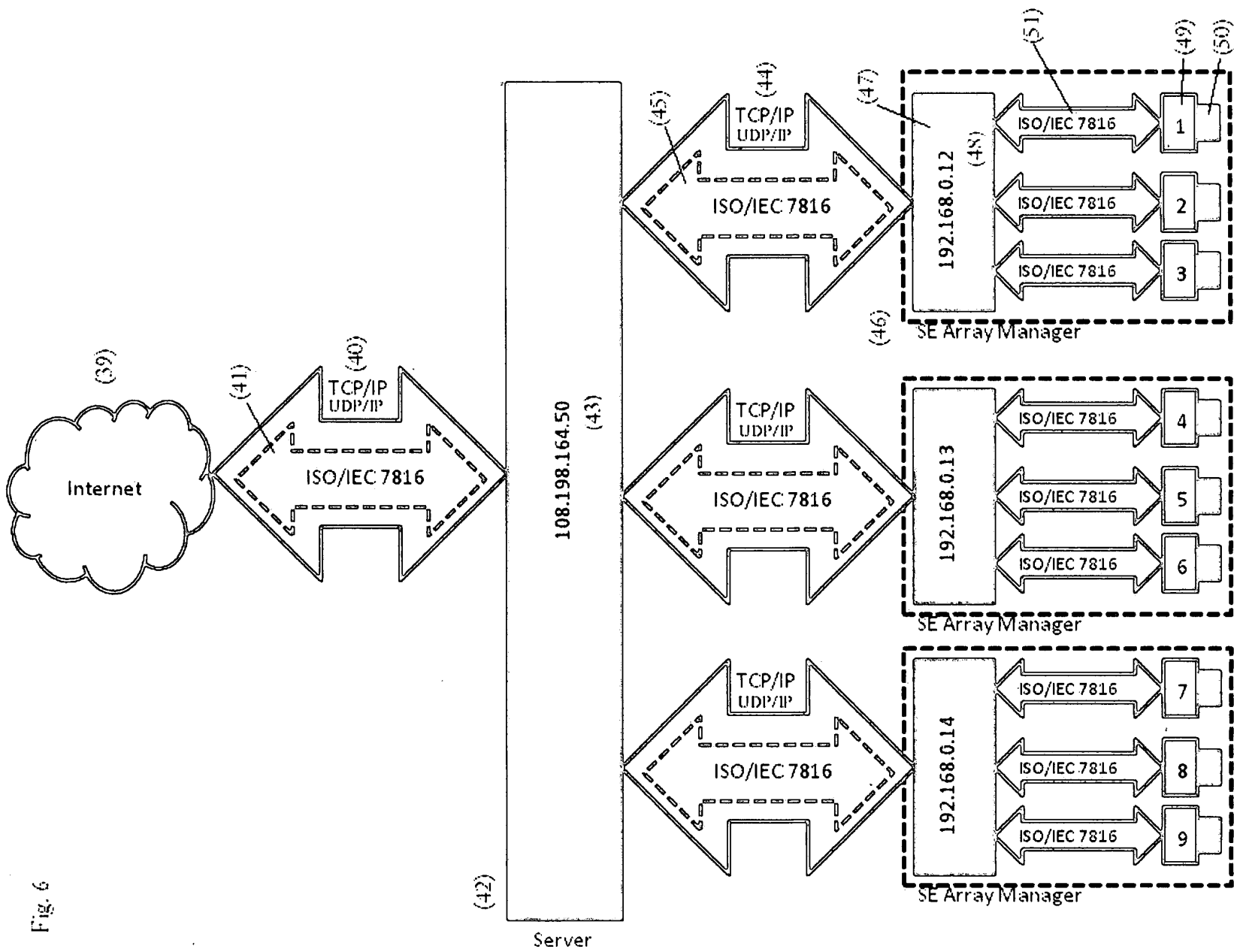


Fig. 6

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 (55)	4
	6 greg@intel.com	9
	.	.
	.	.
	.	.

Fig. 8

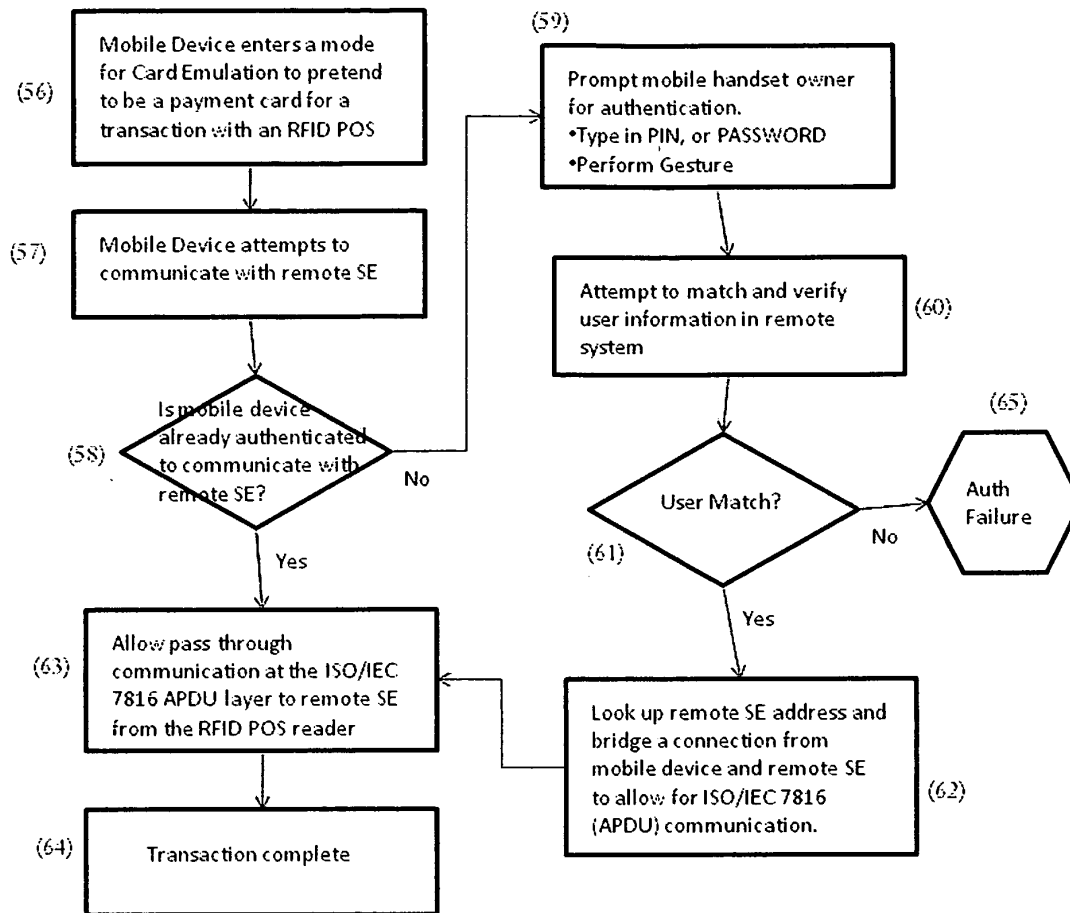


Fig. 9

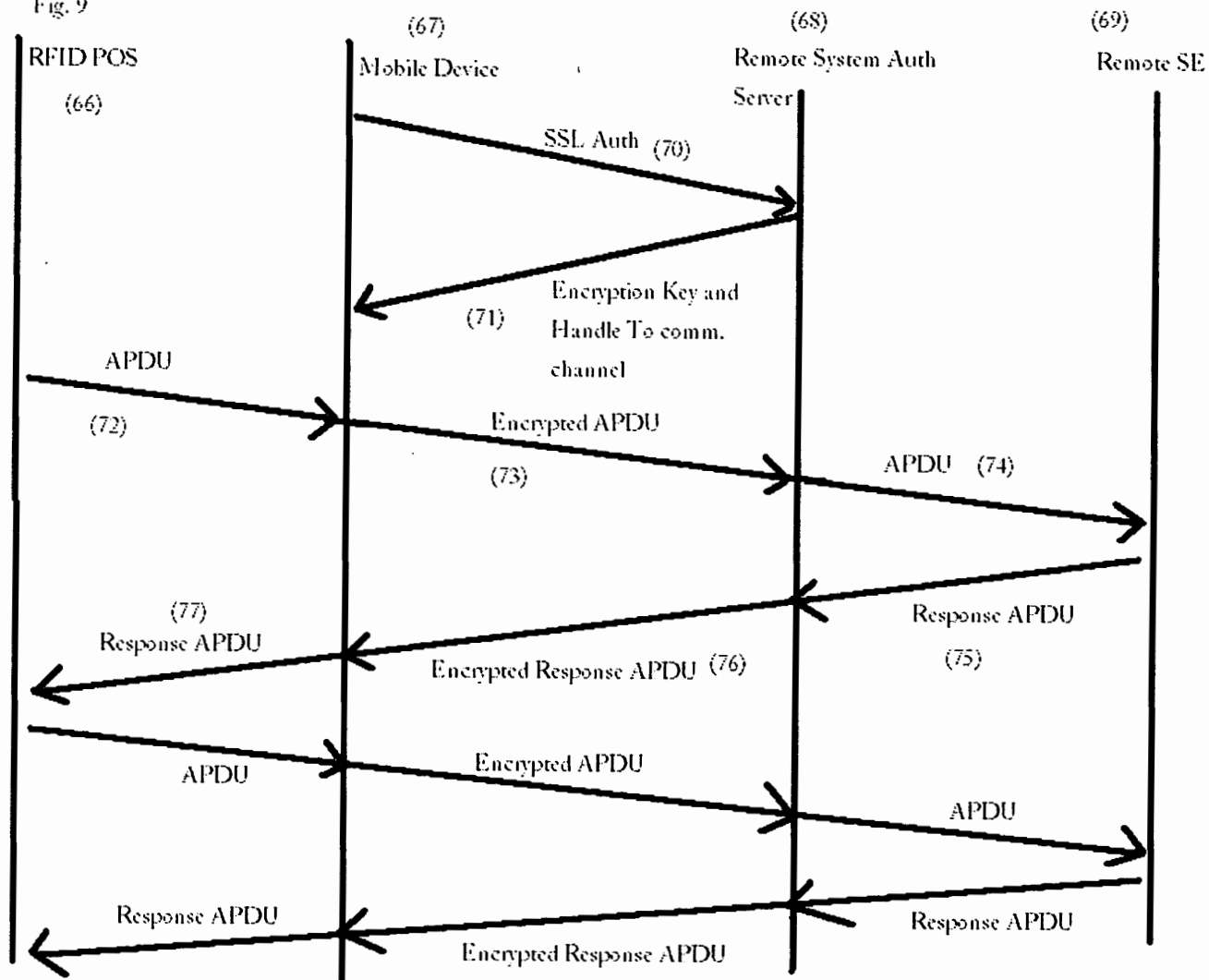


Fig. 10

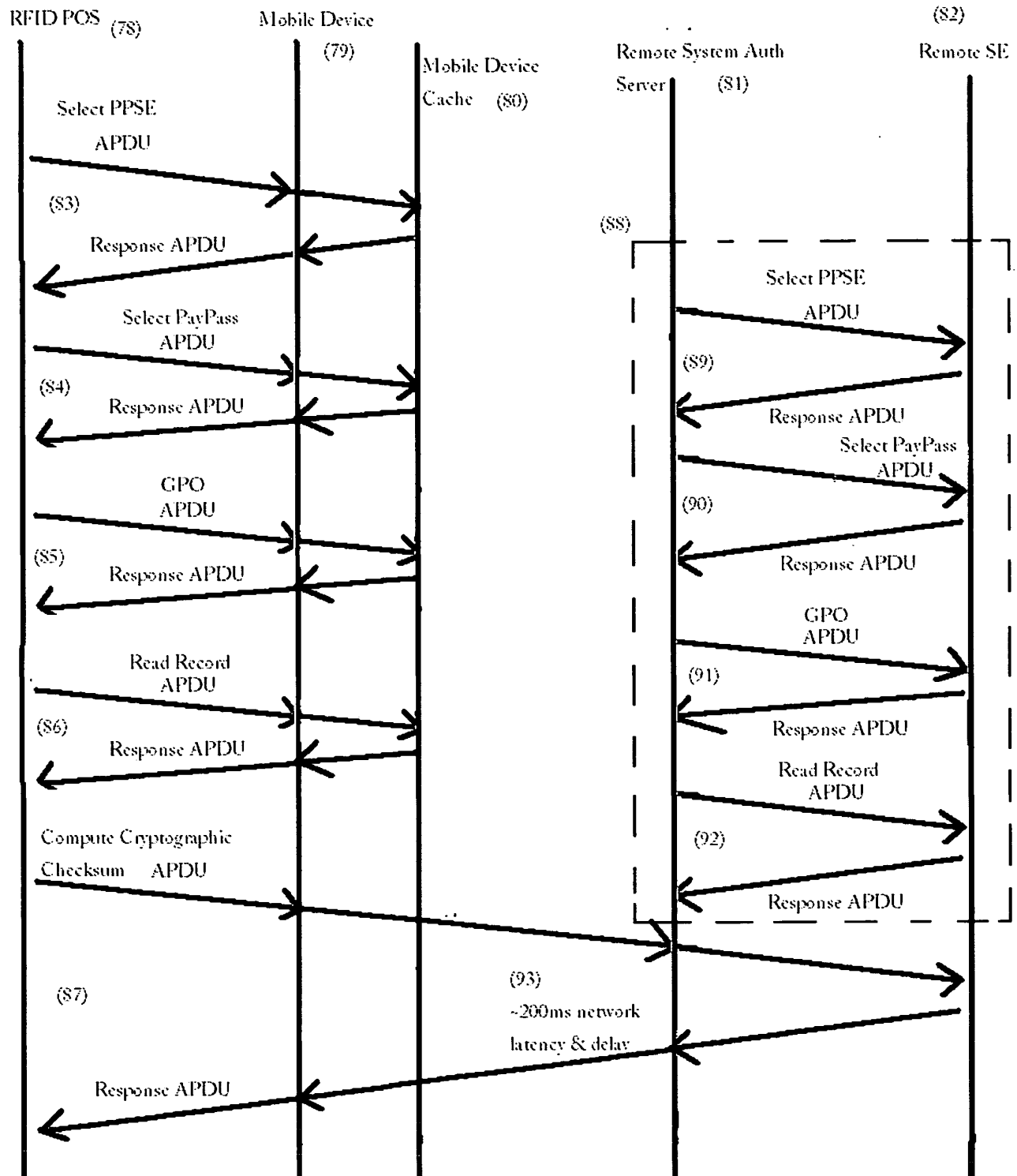


Fig. 11

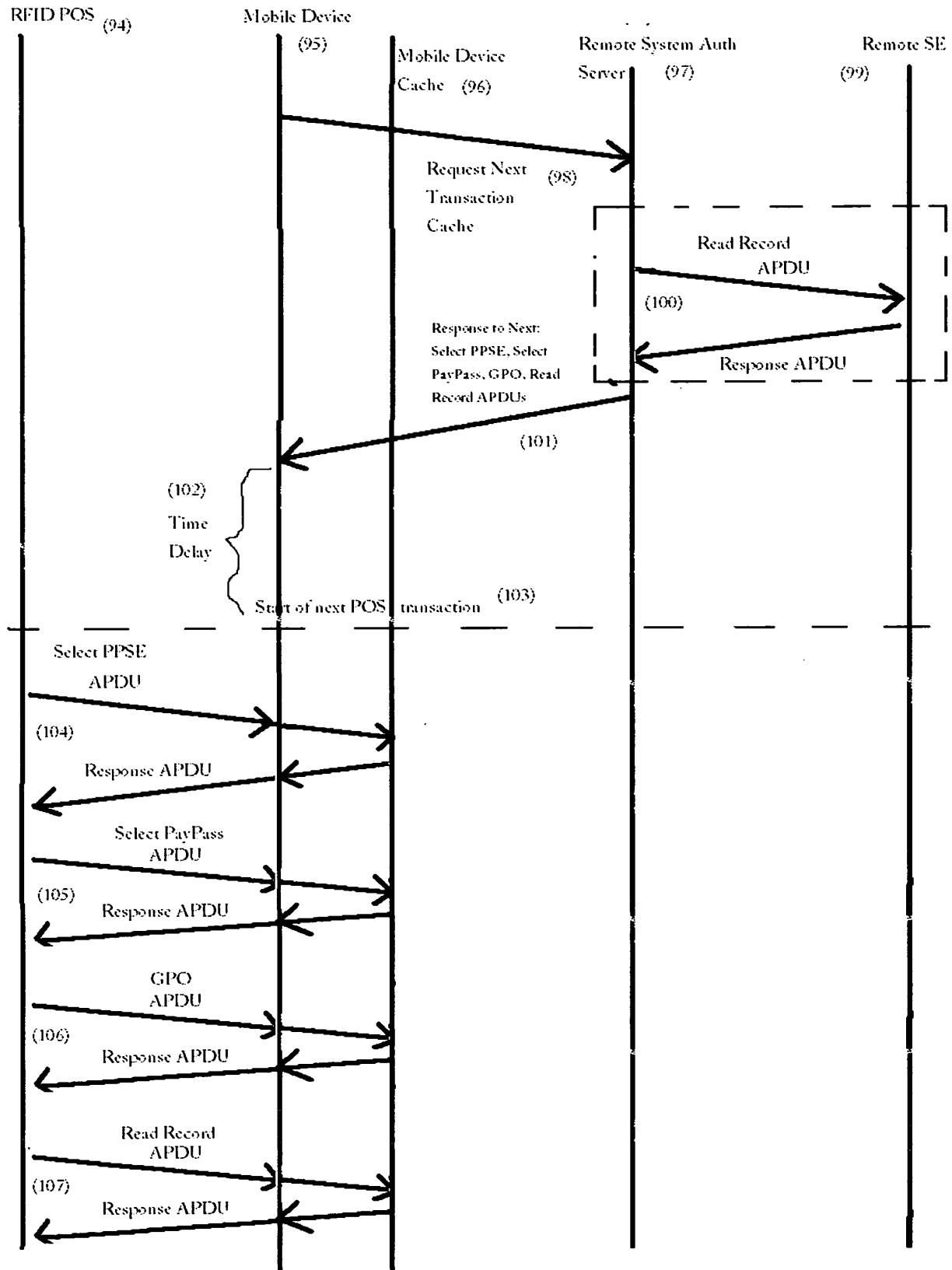


Fig. 12

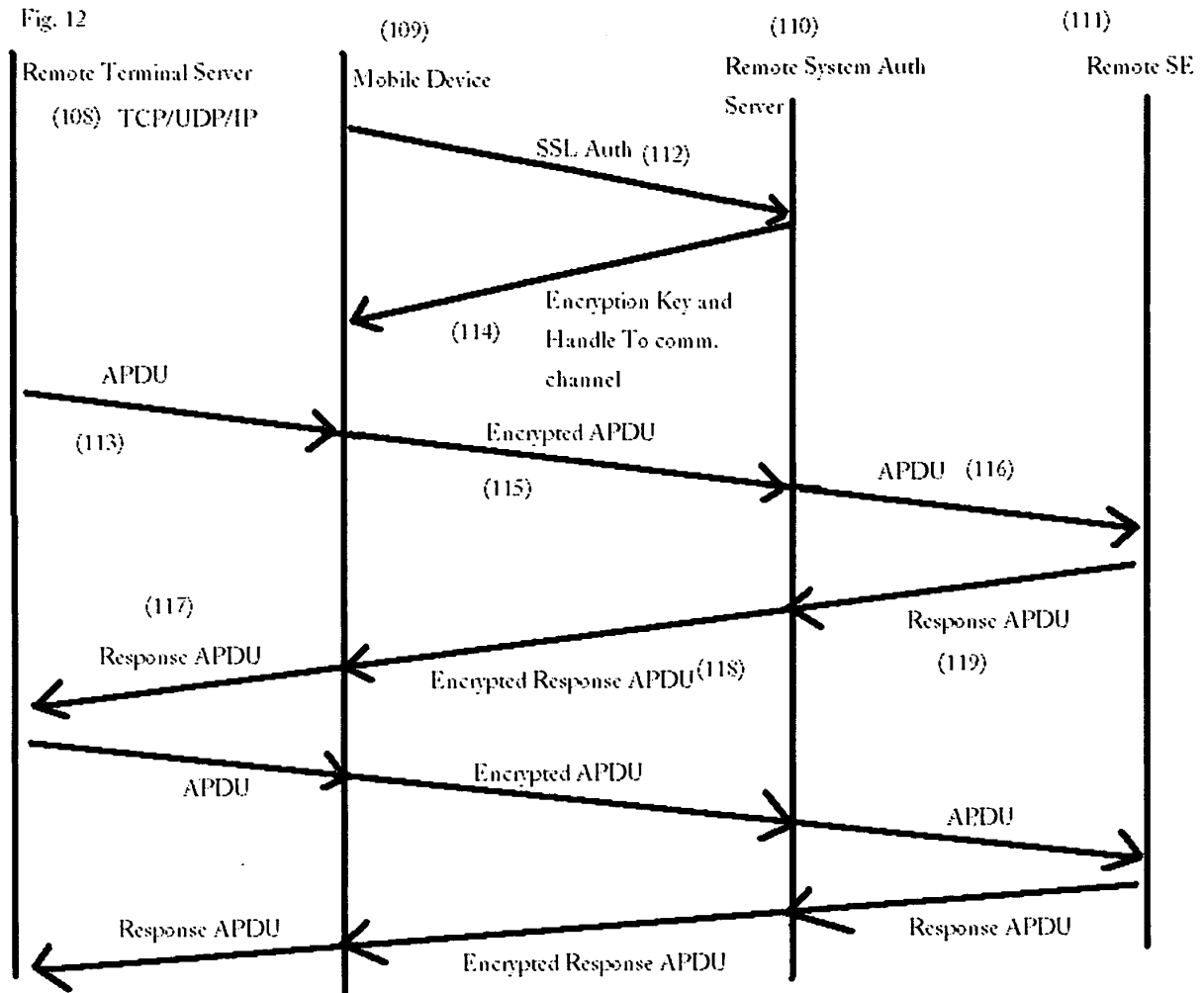


Fig. 13

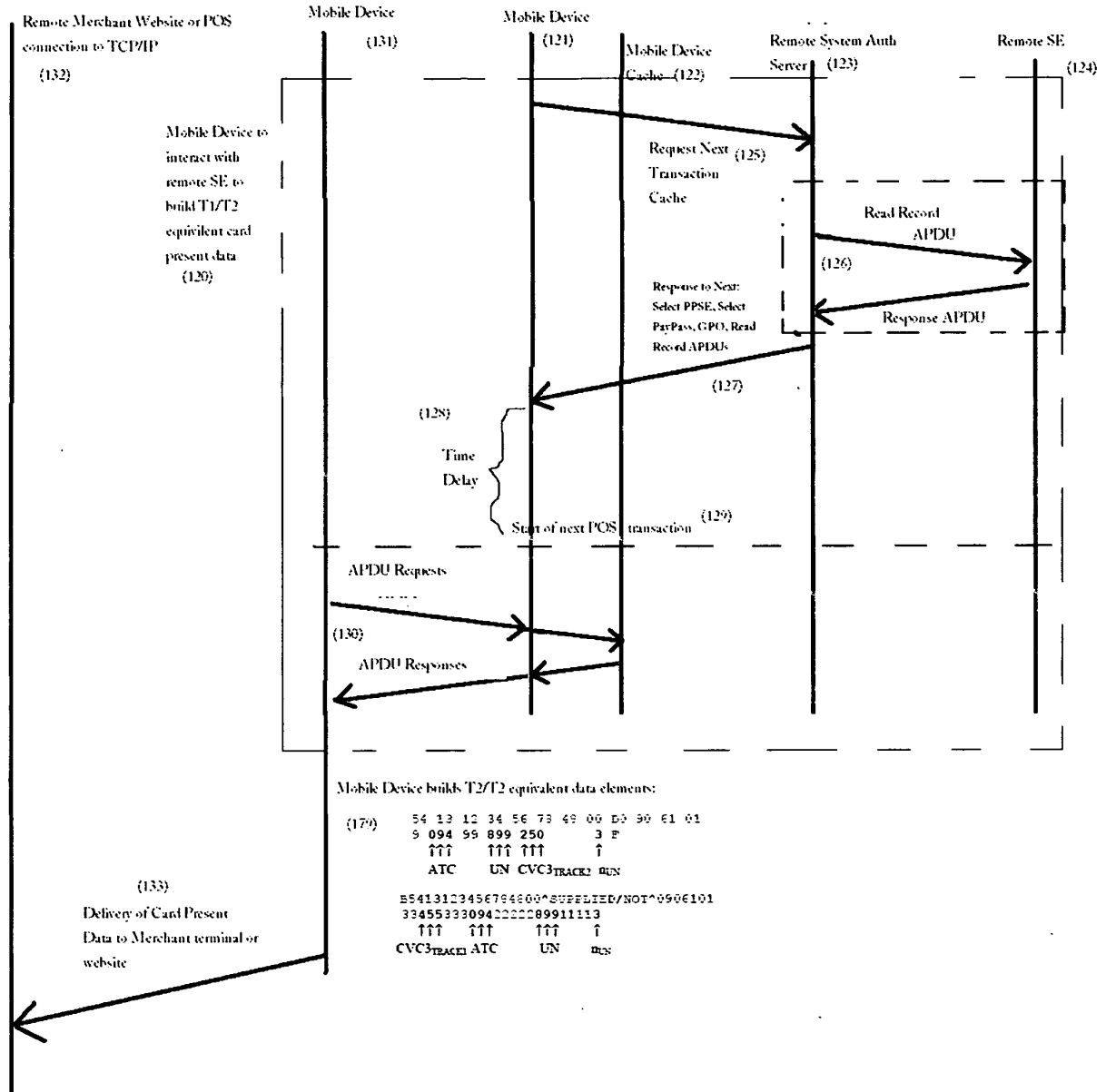


Fig. 14

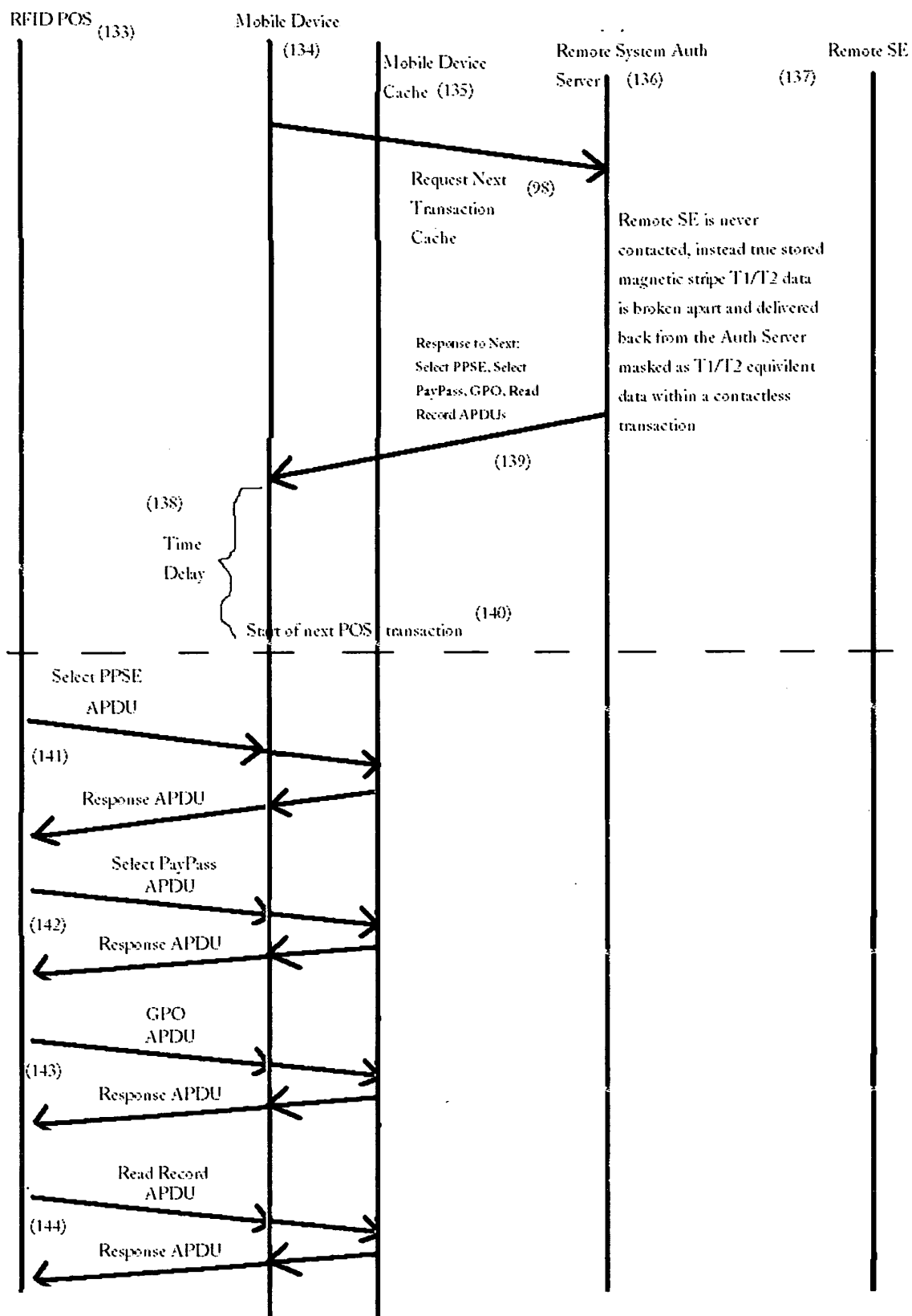
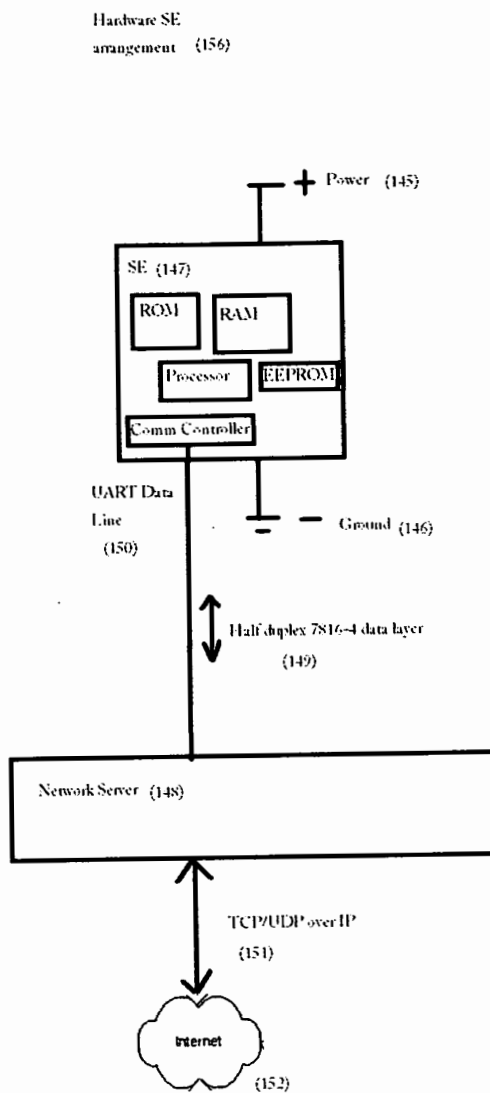


Fig. 15



Software SE arrangement (virtual SE) (157)

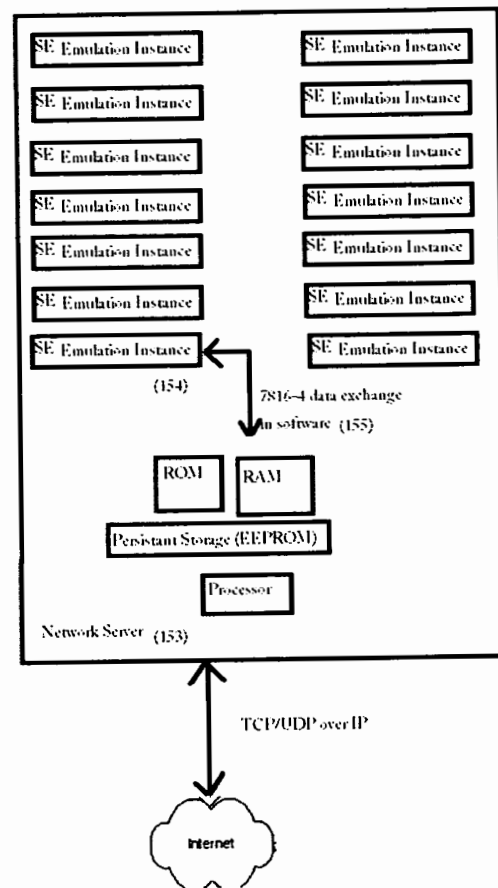


Fig. 16

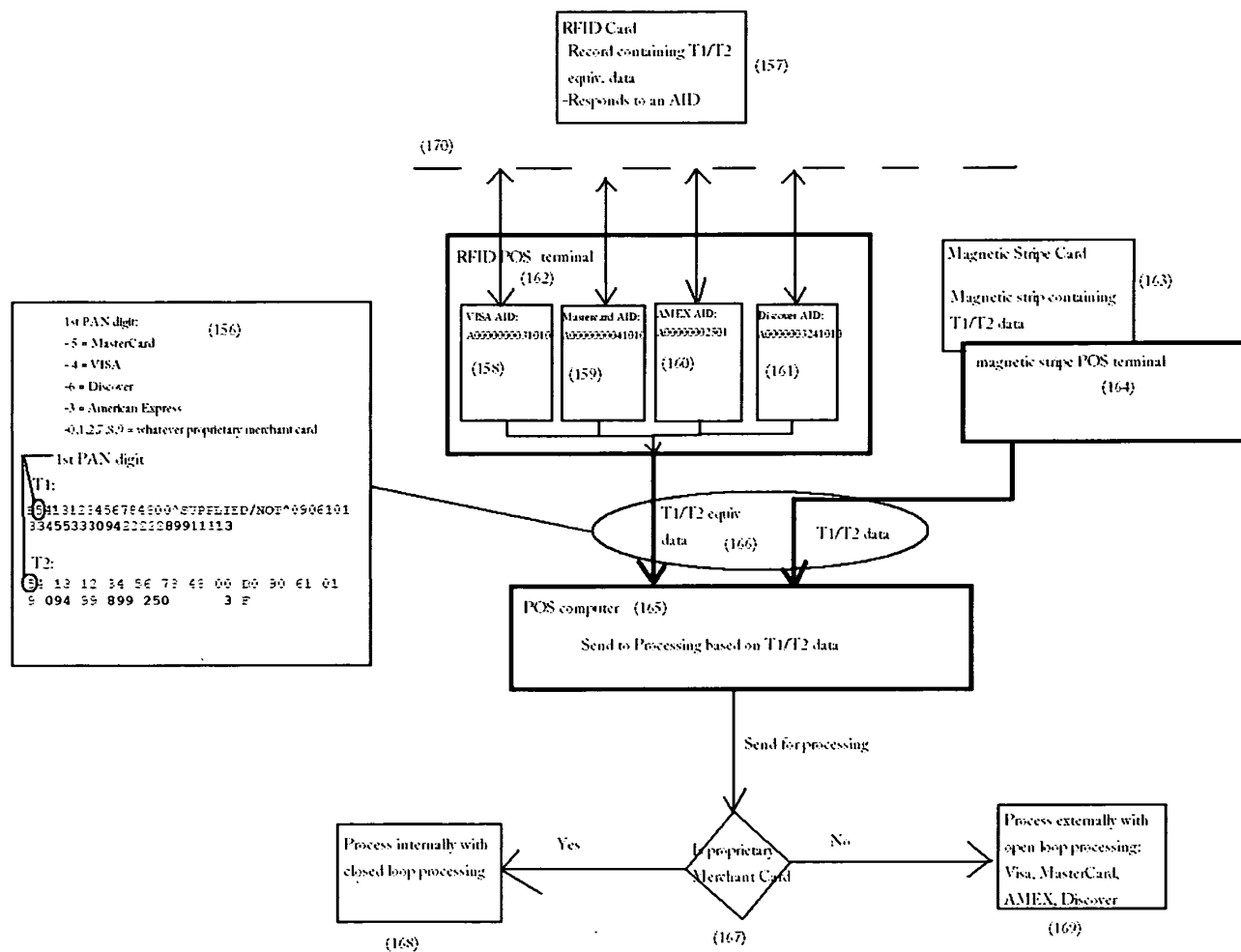
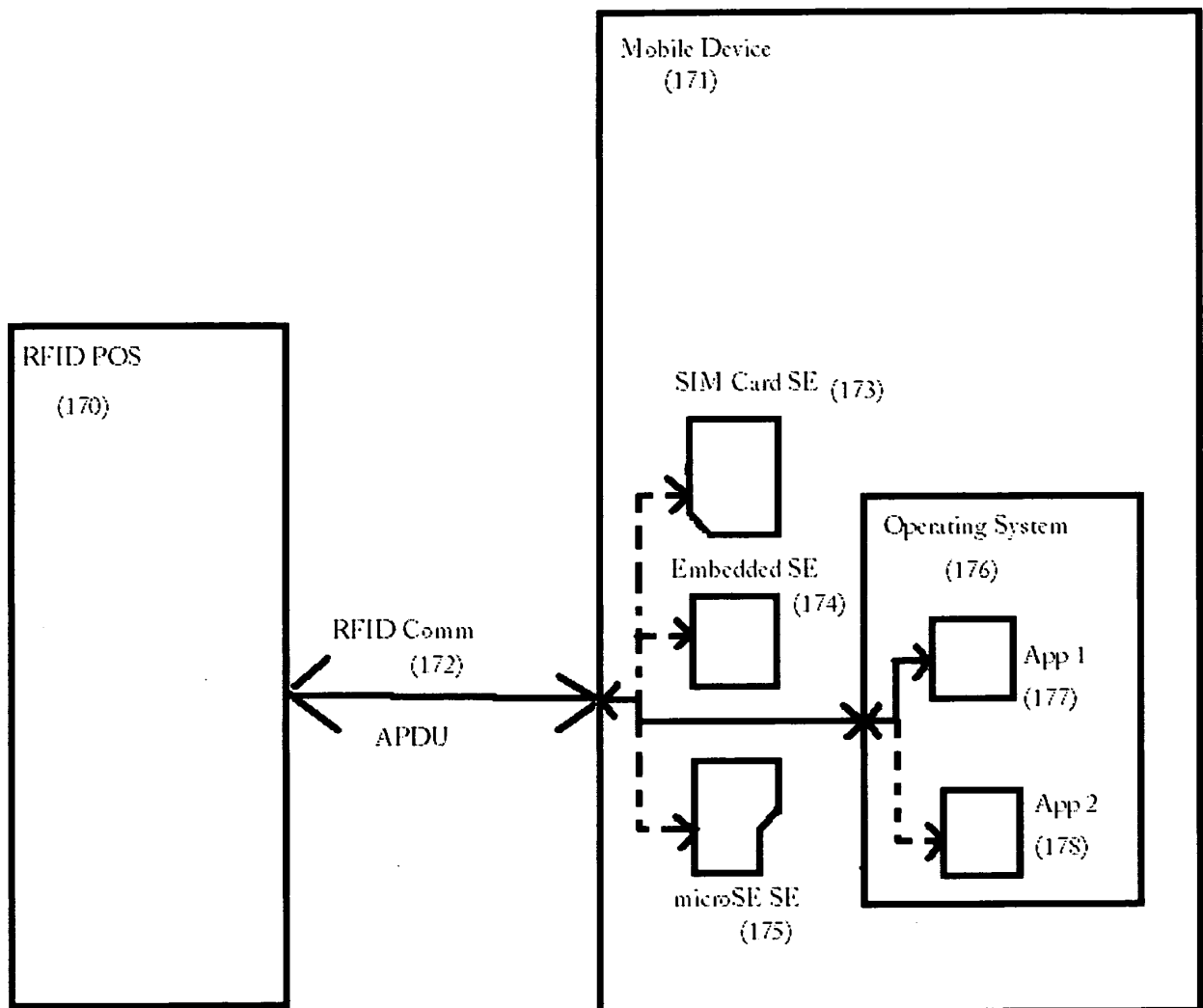


Fig. 17



PATENT APPLICATION SERIAL NO. _____

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

03/28/2012 EEKUBAY1 00000040 61685863

01 FC:2005 110.00 DP

PTO-1556
(5/87)

*U.S. Government Printing Office: 2002- 489-267/69033

Notice of Fee Due

Date:

03-28-12

Application Number:

61685863

A fee is due for the attached document for the reason indicated below. Please check the application for the appropriate authorization to charge a deposit account. If an authorization is present, please charge the appropriate fee*. If an authorization is not present, notify the applicant of the fee deficiency.

***If the fee due is for any of the filing fees, check for authorization to charge the surcharge. If authorization is present, charge the surcharge for late payment of the filing fees as well.**

☒ Insufficient payment by check or money order.

☐ Insufficient funds in deposit account _____ at _____:_____ (time).

☐ Insufficient payment by credit card.

☐ Declined credit card _____:_____ (time).

☒ No authorization to charge a deposit account.

Fee code(s) to be applied:

<u>2005</u>	<u>125.00</u>
<u>2005</u>	<u>170.00</u>

Amount in holding fee code:

<u>1506</u>	
<u>1622/2622</u>	
<u>1999</u>	

Total remaining due from applicant:

15.00

RAM Operator

E.E