(12) STANDARD PATENT (11) Application No. **AU 2006294466 B2**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Device, system and method for reducing an interaction time for a contactless transaction

(51) International Patent Classification(s)
G06Q 99/00 (2006.01)

(21) Application No: **2006294466** (22) Date of Filing: **2006.09.28**

(87) WIPO No: **WO07/038743**

(30) Priority Data

(31) Number	(32) Date	(33) Country
60/807,775	**2006.07.19**	**US**
60/721,454	**2005.09.28**	**US**

(43) Publication Date: **2007.04.05**
(44) Accepted Journal Date: **2011.08.18**

(71) Applicant(s)
Visa International Service Association

(72) Inventor(s)
Aabye, Christian;Oppenlander, Carole;Ochieano, Anita;Sahota, Jagdeep Singh;Wagner, Kim;Hill, Trudy;Glendenning, Craig Allen;Chan, William Chi Yuen

(74) Agent / Attorney
Spruson & Ferguson, Level 35 St Martins Tower 31 Market Street, Sydney, NSW, 2000

(56) Related Art
US 2003/0220835
US 2005/0203856
US 2005/0033688

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 April 2007 (05.04.2007)

PCT

(10) International Publication Number
WO 2007/038743 A3

(51) International Patent Classification:
G06Q 99/00 (2006.01)

(21) International Application Number:
PCT/US2006/038047

(22) International Filing Date:
28 September 2006 (28.09.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/721,454 28 September 2005 (28.09.2005) US
60/807,775 19 July 2006 (19.07.2006) US

(71) Applicant *(for all designated States except US)*: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; 900 Metro City Boulevard, Foster City, CA 94404 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HILL, Trudy** [US/US]; 1200 East Hillsdale #18, Foster City, California 94404 (US). **SAHOTA, Jagdeep, Singh** [US/US]; 981 Coral Ridge Circle, Rodeo, California 94572 (US). **AABYE, Christian** [US/US]; 515 Trinidad Lane, Foster City, California 94404 (US). **WAGNER, Kim** [US/US]; 4397 Rivermark Parkway, Santa Clara, California 95054 (US). **OCHIEANO, Anita** [US/US]; 1975 Stanford Avenue, Menlo Park, California 94025 (US). **OPPENLANDER, Carole** [US/US]; 1975 Stanford Avenue, Menlo Park, California 94025 (US). **CHAN, William, Chi, Yuen** [US/SG]; Valley Park, #06-02, Singapore 248368 (SG). **GLENDENNING, Craig, Allen** [AU/SG]; 94a Meyer Road, Nanak Mansions 437916 (SG).

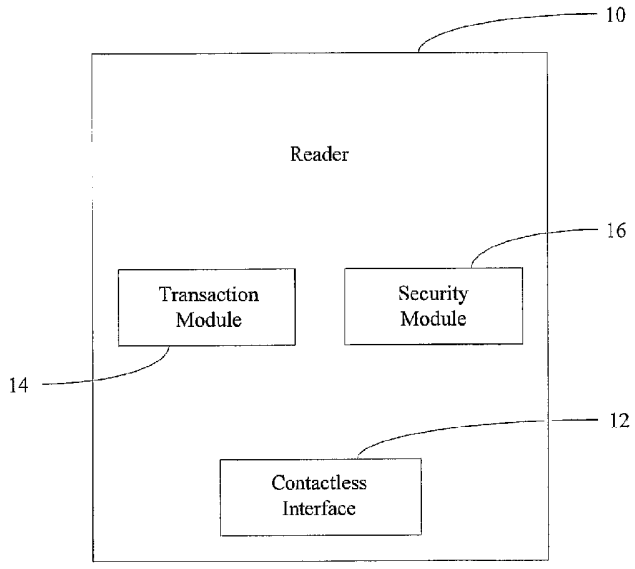
(74) Agent: **MELNIK, W. Joseph**; Pepper Hamilton LLP, One Mellon Center, 50th Floor, 500 Grant Street, Pittsburgh, Pennsylvania 15219 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,

[Continued on next page]

(54) Title: DEVICE, SYSTEM AND METHOD FOR REDUCING AN INTERACTION TIME FOR A CONTACTLESS TRANSACTION



(57) Abstract: A method. The method comprises, at a reader, performing at least one transaction-based risk management process prior to energizing a contactless interface, initiating communication with a card utilized for the contactless transaction, receiving information associated with the card, and terminating communication with the card prior to authorizing the contactless transaction.

WO 2007/038743 A3

FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
21 December 2007

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A. TITLE

DEVICE, SYSTEM AND METHOD FOR REDUCING ANINTERACTION TIME FOR A CONTACTLESS TRANSACTION

B. CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the priority benefit of United States Provisional Patent Application No. 60/721,454, filed on September 28, 2005, and United States Provisional Patent Application No. 60/807,775, filed on July 19, 2006.

C. STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH AGREEMENTS – NOT APPLICABLE

D PARTIES TO JOINT RESEARCH AGREEMENT – NOT APPLICABLE

E. INCORPORATION OF MATERIAL SUBMITTED ON CD – NOT APPLICABLE

F. BACKGROUND

[0002] This application discloses an invention that is related, generally and in various embodiments, to a device, system and method for reducing an interaction time for a contactless transaction.

[0003] Contactless and wireless communication technologies have become more widespread in recent years. In the payment industry, contactless payment has a number of advantages over both traditional magnetic stripe technologies and contact-based chip payment protocols. For example, traditional payment contact cards are known to operate relatively slowly, and magnetic stripe cards are known to not be sufficiently secure. Each of these technologies further requires a slot in a terminal reader that must be maintained by a merchant.

[0004] Contactless payment does not require a slot in which to enter the card. The consumer retains control over the card and merely positions the card near the terminal reader whenever necessary. The traditional specifications adopted by the payment industry for

contact-based chip payment generally require the consumer to position the card near the terminal reader at different times and/or for extended periods of time in order to complete a transaction. With both merchants and consumers desiring fast transaction times, contactless transactions executed in accordance with the traditional specifications fail to meet market requirements.

[0005] Merchants and consumers are also demanding that contactless transactions be more secure. Although more recently issued contactless magnetic stripe-based cards can be more secure than traditional magnetic stripe cards, such contactless magnetic stripe-based cards are typically designed only for online transactions. For contactless offline transactions executed in accordance with the traditional specifications, the transactions can be susceptible to various offline "man in the middle" types of attacks generally referred to as sleeve attacks, Trojan horse attacks, etc.

[0006] In one type of sleeve attack, a device intercepts data transmitted wirelessly from a card reader that is intended for a contactless card. The device alters the data and subsequently transmits the altered data to the card. Instead of receiving the data transmitted by the card reader, the card receives the altered data transmitted by the device. The card subsequently processes the altered data and transmits a message related to the altered data to the card reader. The card reader subsequently grants approval of the transaction based on information present in the message transmitted by the card. In another type of sleeve attack, a device intercepts data transmitted wirelessly from the card that is intended for the card reader. The device alters the data and subsequently transmits the altered data to the card reader. Instead of receiving the data transmitted by the card, the card reader receives the altered data transmitted by the device. The card reader subsequently processes the altered data and grants approval of the transaction based on information present in the altered data

transmitted by the device. In other types of sleeve attacks, the device may cause a denial of service by not forwarding intercepted data to the card or the card reader.

[0007] In one type of Trojan horse attack, malicious software embedded in the card alters valid data prior to information being sent to the card reader. The card reader ultimately grants approval of the transaction based on the altered data. In another type of Trojan horse attack, malicious software embedded in the card reader alters valid data prior to the authorization process. The card reader ultimately grants approval of the transaction based on the altered data.

[0008] For a given offline transaction, a "man in the middle" attack may be utilized to reduce the amount of the transaction as ultimately recognized by the card and the card reader. For example, for a given offline transaction involving the purchase of goods from a merchant, the card reader may wirelessly transmit data intended for the card which indicates that the value of the transaction is equal to $15. However, prior to the data being received by the card, the device intercepts the data and alters the data so that the altered data indicates that the value of the transaction is equal to only $1. Once the card subsequently receives the altered data and transmits the message related to the altered data to the card reader, the card reader subsequently grants approval of a transaction equal to only $1. Upon receiving the approval, the merchant releases the goods with the belief that the approved transaction amount was equal to $15. The difference between the actual transaction amount and the reduced transaction amount may affect the amount ultimately received by the merchant from a card issuer.

G. BRIEF SUMMARY OF THE INVENTION

[0009] It is an object of the present invention to substantially overcome, or at least ameliorate, one or more disadvantages of existing arrangements.

[0009A] In one general aspect, this application discloses a reader. According to various embodiments, the reader comprises a contactless interface and a transaction module. The transaction module is coupled to the contactless interface, and is structured and arranged to discover the presence of a contactless payment device within a predetermined distance from the reader;

energize the contactless interface upon discovery of the presence of the contactless payment device within the predetermined distance form the reader, wherein the energized contactless interface enables communication between the contactless payment device and the reader; and

process a contactless transaction with less than one-half second of interaction time between the contactless payment device and the reader; and

a security module coupled to the transaction module, wherein the security module is structured and arranged to prevent a man in the middle attack on the contactless transaction.

[0010] In another general aspect, this application discloses a card. According to various embodiments, the card comprises a transaction module structured and arranged for wireless communication, and the card is structured and arranged to operate in a chip-mode and a magnetic stripe data mode;

to cooperate with a reader to:

be discoverable by being within a predetermined distance from the reader; and

execute a contactless transaction with less than one-half second of interaction time between the card and the reader; and

a security module structured and arranged to cooperate with the reader to prevent a man in the middle attack on the contactless transaction.

[0011] In another general aspect, this application discloses a system. According to various embodiments, the system comprises a reader and a card. The reader comprises a contactless interface and a transaction module. The transaction module is structured and arranged to energize the contactless interface upon discovery of the presence of the card within a predetermined distance from the reader, wherein the energized contactless interface enables communication between the card and the reader; and

process a contactless transaction with less than one-half second of interaction time between the card and the reader; and

a security module structured and arranged to cooperate with the reader to prevent a man in the middle attack on the contactless transaction.

[0012] In another general aspect, this application discloses a method for reducing an interaction time for a contactless transaction. According to various embodiments, the method comprises, at a reader, performing at least one transaction-based risk management process prior to energizing a contactless interface, energizing the contactless interface upon discovery of the presence of a card within a predetermined distance from the reader, wherein the energized contactless interface enables communication between the card and the reader;

initiating communication with a the card utilized for the contactless transaction;

receiving information associated with the card; and

terminating communication with the card prior to authorizing the contactless transaction;

utilizing a security module structured and arranged to prevent a man in the middle attack on the contactless transaction; and

completing the contactless transaction with less than one-half second of interaction time between the card and the reader.

[0013] In another general aspect, this application discloses a method for preventing a man in the middle attack on a contactless transaction. According to various embodiments, the method comprises receiving a dynamic signature that comprises an application transaction counter, a terminal unpredictable number, a transaction amount, a transaction currency code, and a card unpredictable number. The method also comprises receiving a card unpredictable number, recalculating the dynamic signature utilizing the card unpredictable number, and authorizing the contactless transaction offline if the dynamic signature is validated.

[0014] Aspects of the invention may be implemented by a computing device and/or a computer program stored on a computer-readable medium. The computer-readable medium may comprise a disk, a device, and/or a propagated signal.

H. DESCRIPTION OF DRAWINGS

[0015] Various embodiments of the invention are described herein by way of example in conjunction with the following figures.

[0016] Figure 1 illustrates various embodiments of a reader for reducing an interaction time for a contactless transaction;

[0017] Figure 2 illustrates various embodiments of a system for reducing an interaction time for a contactless transaction;

[0018] Figure 3 illustrates various embodiments of a method for reducing an interaction time for a contactless transaction;

[0019] Figure 4 is a simplified flow diagram illustrating various embodiments of a preliminary transaction processing step of the method of Figure 3;

[0020] Figure 5 is a simplified flow diagram illustrating various embodiments of an application selection step of the method of Figure 3;

[0021] Figure 6 is a simplified flow diagram illustrating various embodiments of an authorization step of the method of Figure 3; and

[0022] Figure 7 illustrates various embodiments of a method for reducing an interaction time for a second contactless transaction.

I. DETAILED DESCRIPTION OF THE INVENTION

[0023] It is to be understood that at least some of the figures and descriptions of the invention have been simplified to focus on elements that are relevant for a clear understanding of the invention, while eliminating, for purposes of clarity, other elements that those of ordinary skill in the art will appreciate may also comprise a portion of the invention. However, because such elements are well known in the art, and because they do not necessarily facilitate a better understanding of the invention, a description of such elements is not provided herein.

[0024] Figure 1 illustrates various embodiments of a reader 10 for reducing an interaction time for a contactless transaction. The reader 10 may be any type of device that is structured and arranged to communicate with another device via a contactless interface. According to various embodiments, the reader 10 may be a merchant device that is integrated into a point-of-sale device, or a merchant device that is separated from but in communication with a point-of-sale device. As used herein, the phrase "interaction time" refers to the interaction time between the reader 10 and another device, and does not include the time required to go online for authorization or for the reader to validate a static or dynamic signature for offline data authentication. The reader 10 may be utilized with existing payment system infrastructure for markets which require transaction times faster than those associated with traditional payment protocols. According to various embodiments, the reader 10 may be utilized to reduce the interaction time to less than approximately 500 milliseconds.

[0025] The reader 10 comprises a contactless interface 12, and a transaction module 14 coupled to the contactless interface. The transaction module 14 is structured and arranged to process a contactless transaction with less than one-half of a second of interaction time between the reader 10 and another device. The transaction module 14 may also be structured and arranged to perform static data authentication and/or dynamic data authentication as

described in more detail hereinbelow. According to various embodiments, the reader 10 further comprises a security module 16 coupled to the transaction module 14. The security module 16 is structured and arranged to prevent a "man in the middle" attack on a contactless transaction.

[0026] Each of the modules 14, 16 may be implemented in hardware or in firmware. According to various embodiments, the modules 14, 16 may be implemented as software applications, computer programs, etc. utilizing any suitable computer language (e.g., C, C++, Delphi, Java, JavaScript, Perl, Visual Basic, VBScript, etc.) and may be embodied permanently or temporarily in any type of machine, component, physical or virtual equipment, storage medium, or propagated signal capable of delivering instructions to a device. The software code may be stored as a series of instructions or commands on a computer-readable medium such that when a processor reads the medium, the functions described herein are performed. As used herein, the term "computer-readable medium" may include, for example, magnetic and optical memory devices such as diskettes, compact discs of both read-only and writeable varieties, optical disk drives, and hard disk drives. A computer-readable medium may also include memory storage that can be physical, virtual, permanent, temporary, semi-permanent and/or semi-temporary. A computer-readable medium may further include one or more propagated signals, and such propagated signals may or may not be transmitted on one or more carrier waves. Although the modules 14, 16 are shown in Figure 1 as two separate modules, one skilled in the art will appreciate that the functionality of the modules 14, 16 may be combined into a single module.

[0027] Figure 2 illustrates various embodiments of a system 20 for reducing an interaction time for a contactless transaction. The system 20 comprises the reader 10 and a card 22. As used herein, the term "card" refers to any type of device that can communicate with the reader 10 over the contactless interface 12. According to various embodiments, the

card 22 may be a smartcard, a mobile phone, a personal digital assistant, etc. The card 22 is structured and arranged to communicate with the reader 10 via the contactless interface 12. According to various embodiments, the card 22 comprises a transaction module 24 structured and arranged to cooperate with the reader 10 to execute the contactless transaction. The card 22 may further comprise a security module 26 structured and arranged to cooperate with the reader 10 to prevent a "man in the middle attack" on the contactless transaction. The modules 24, 26 may be similar to the modules 14, 16 of the reader 10. According to various embodiments, the card 22 may be a dual mode card which is structured and arranged to operate in either a chip-mode or in a magnetic stripe data mode (utilizing Track 2 equivalent data). The mode of operation utilized by the card 22 may be determined by the card 22 based on the capabilities of the reader 10.

[0028] The system 20 may further comprise a network 28 coupled to the reader 10 and an issuer 30. The network 28 may be any suitable type of network as known in the art, may be coupled to the reader 28 in any suitable manner know in the art, and may be coupled to the issuer 30 in any suitable manner known in the art. The network 28 may include any type of delivery system including, but not limited to a local area network (e.g., Ethernet), a wide area network (e.g. the Internet and/or World Wide Web), a telephone network (e.g., analog, digital, wired, wireless, PSTN, ISDN, GSM, GPRS, and/or xDSL), a packet-switched network, a radio network, a television network, a cable network, a satellite network, and/or any other wired or wireless communications network configured to carry data. The network 28 may include elements, such as, for example, intermediate nodes, proxy servers, routers, switches, and adapters configured to direct and/or deliver data.

[0029] Figure 3 illustrates various embodiments of a method 40 for reducing an interaction time for a contactless transaction. The method 40 may be implemented by the system 20 of Figure 2. The method 40 comprises the general steps of preliminary transaction

processing 42, discovery processing 44, application selection 46, application processing 48, and transaction authorization 50.

[0030] To minimize the interaction time between the card 22 and the reader 10 for a given transaction, the preliminary transaction processing step 42 is performed by the reader 10 before requesting that the card 22 be presented. During the preliminary transaction processing step 42, the reader 10 performs certain transaction-based risk management processes. For example, according to various embodiments, the reader 10 may obtain the transaction amount and compare the transaction amount to a transaction limit, a floor limit, a card holder verification method limit, etc. Once the preliminary transaction processing step 42 is completed, the reader 10 may prompt a cardholder to present the card 22. Based on the preliminary transaction processing, the reader 10 may request that the transaction be terminated, processed online, or processed offline. A simplified flow diagram illustrating various embodiments of the preliminary transaction processing step 42 is shown in Figure 4.

[0031] The discovery processing step 44 follows the preliminary transaction processing step 42. Once the card 22 is presented and is within range of the reader 10, the reader 10 energizes the contactless interface 12 and establishes communication with the card 22 via the contactless interface 12 during the discovery processing step 44. If the reader 10 detects multiple contactless cards 22 within its range, the reader 10 may indicate this condition to a cardholder and may request that only one card 22 be presented for the transaction. In addition, a reader 10 may abort a transaction during the discovery processing step 44 and de-energize the contactless interface 12 upon a merchant command or after a pre-defined timeout period.

[0032] The application selection step 46 follows the discovery processing step 44. During the application selection step 46, the reader 10 transmits a first command message (e.g., SELECT PPSE) to the card 22. The first command message may serve as a request for

a list of application identifiers, application labels and application priority indicators for applications that are supported by the card 22 and are accessible via the contactless interface 12. Responsive to the first command message, the card 22 builds such a list and transmits the list to the reader 10. According to various embodiments, the list may be provided within file control information (FCI) transmitted to the reader 10. The reader 10 then utilizes the list transmitted by the card 22 to build a list of applications common to the reader 10 and the card 22. After building the list of common applications, the reader 10 transmits a second command message (e.g., SELECT AID) to the card 22. The second command message may serve as a request to conduct the transaction utilizing a specific application from the list of common applications. According to various embodiments, the specific application may be the common application having the highest priority as indicated by the application priority indicators previously transmitted by the card 22. Responsive to the second command message, the card 22 transmits a request the reader 10 to provide various details concerning the capabilities of the reader 10 and transaction specific requirements of the reader 10. According to various embodiments, the requested details may be provided in a list of terminal data objects (e.g., PDOL) associated with the reader 10. If the list of terminal data objects includes a particular data element (e.g., terminal transaction qualifiers), the process advances to the application processing step 48. Otherwise, the reader 10 may terminate the transaction or attempt to process the transaction over another interface. A simplified flow diagram illustrating various embodiments of the application selection step 46 is shown in Figure 5.

[0033] During the application processing step 48, the reader 10 transmits a third command message (e.g., GPO) to the card 22 responsive to the card's request for details concerning the capabilities of the reader 10 and transaction specific requirements of the reader 10. The third command message is structured such that it can be utilized in lieu of three separate commands required by previous specifications. By reducing the number of

commands and responses required to complete the contactless transaction, the interaction time required between the card 22 and the reader 10 is further minimized. The third command message may comprise values for any number of data elements requested by the card 22. Various data element values indicate the type of transactions supported by the reader 10, whether offline and/or online processing is supported or required by the reader 10, which cardholder verification methods are supported or required by the reader 10, etc. The data elements may comprise terminal transaction qualifiers, the transaction amount, a terminal unpredictable number, a transaction currency code, and any other data requested by the card 22 in its response to the second command message.

[0034] Based on the type of transactions supported by the reader 10, the card 22 then performs a number of risk-management processes associated with a particular transaction type. According to various embodiments, the risk-management processes may include checking an internal card indicator to protect against transaction tearing, comparing a value of an application currency code to a value of a transaction currency code, comparing the number of personal identification number entries to a predetermined limit, determining whether a cardholder verification method is required, comparing the transaction amount to a low value limit associated with the card 22, comparing the transaction amount to a cumulative total transaction amount associated with the card 22, comparing a value of a consecutive transaction counter to a value of a consecutive transaction limit, etc. By performing the recited risk management processes at this point in the transaction, as opposed to being performed at a later point in accordance traditional specifications, the interaction time between the card 22 and the reader 10 is further minimized. Based on the risk-management processing, the card 22 may request that the transaction be terminated, processed online, or processed offline.

[0035] Following the completion of the risk-management processes, the card 22 builds the appropriate response to the third command message and transmits the response to the reader 10. The information included in the response may vary depending on whether the card 22 desires the transaction to be authorized online, authorized offline, or terminated. For example, when the card 22 desires the transaction to be authorized online, the response may include an application transaction counter (ATC) that indicates the number of transactions processed by the card, an application cryptogram generated by the card 22 utilizing the application transaction counter and terminal data (e.g., the terminal unpredictable number and the transaction amount) included in the third command message, an application interchange profile (AIP) that indicates support for risk management features, issuer application data, and Track 2 equivalent data, and various other data elements.

[0036] When the card 22 desires the transaction to be authorized offline, the response to the third command message may include an application transaction counter (ATC) that indicates the number of transactions processed by the card. The response may also include a dynamic signature generated by the card 22 utilizing the application transaction counter, terminal data (e.g., the terminal unpredictable number, the transaction amount, and the transaction currency) included in the third command message, and a card unpredictable number. The response may further include an application cryptogram generated by the card 22 utilizing the application transaction counter and terminal data (e.g., the terminal unpredictable number and the transaction amount) included in the third command message. In addition, the response may include an application file locator (AFL) that indicates the location of files and records related to the application, an application interchange profile (AIP) that indicates support for risk management features, issuer application data, and various other data elements. According to various embodiments, the card 22 may increment the application transaction counter prior to its calculation of the application cryptogram and the

dynamic signature. If the size of the dynamic signature exceeds a predetermined threshold, the dynamic signature may be returned in authorization step 50 in response to a fourth command message described hereinbelow. According to various embodiments, the application cryptogram generated by the card 22 comprises fewer data elements than application cryptograms utilized by previous specifications. By utilizing fewer data elements to generate the application cryptogram, overall processing time is reduced and the interaction time between the card 22 and the reader 10 is further minimized.

[0037] The authorization step 50 follows the application processing step 48. After the reader 10 receives the response to the third command message from the card 22, the card 22 may be removed from the range of the reader 10 when the transaction is to be authorized online. Therefore, the card 22 is not required to remain within range of the reader 10 while online authorization is requested and performed. By being able to remove the card 22 at this point in the transaction process, the interaction time between the card 22 and the reader 10 is further minimized. The reader 10 may then send the application cryptogram, provided by the card 22 in response to the third command message, online to the issuer 30. Based on a response subsequently received from the issuer 30, the reader 10 approves or declines the transaction.

[0038] When the transaction is to be authorized offline, the reader 10 transmits a fourth command message (e.g., READ RECORD) to the card 22 after receiving the response to the third command message from the card 22. The fourth command message may serve as a request for the records indicated in the application file locator (AFL) provided by the card 22 in response to the third command message. Responsive to the fourth command message, the card 22 transmits the appropriate records to the reader 10. When the last record is received by the reader 10, the card 22 may be removed from the range of the reader 10. Therefore, the card 22 is not required to remain within range of the reader 10 while offline

authorization is performed. By being able to remove the card 22 at this point in the transaction process, the interaction time between the card 22 and the reader 10 is further minimized. The reader 10 may then check whether the card 22 is expired. If the reader 10 determines that the card 22 is not expired, the reader 10 may then perform offline data authentication. The type of offline data authentication performed, static data authentication (SDA) or dynamic data authentication (DDA), is determined based on the application interchange profile (AIP) provided by the card 22 in response to the third command message.

[0039] For static data authentication, the reader 10 attempts to validate the static signature provided by the card 22 in the response to the third command message. Static data authentication involves validating important application data to ensure that the data has not been fraudulently altered. If the static signature is validated, the transaction is approved offline. Otherwise, the transaction may be sent online or terminated. For dynamic data authentication, the reader 10 attempts to validate the dynamic signature provided by the card 22 in response to the third command message. Dynamic data authentication involves validating important application data to ensure that the data has not been fraudulently altered and that the card 22 is genuine. According to various embodiments, the validation of the dynamic signature may comprise utilizing the application transaction counter (ATC) and the terminal unpredictable number provided by the card 22 in the response to the third command message to recalculate the dynamic signature. According to other embodiments, the validation of the dynamic signature may comprise utilizing a card unpredictable number received from the card to recalculate the dynamic signature. If the dynamic signature is validated, the reader 10 generates a clearing message which includes the cryptogram provided by the card 22 in the response to the third command message and other related data. Otherwise, the transaction may be sent online or terminated. According to various embodiments, if the dynamic signature is not validated, the reader 10 may send the

transaction online utilizing the cryptogram previously received from the card 22. Thus, the reader 10 may generate an online request with an offline cryptogram. A simplified flow diagram illustrating various embodiments of the authorization step 50 is shown in Figure 6.

[0040] As described hereinabove, the method 40 may be utilized to minimize the interaction time between the card 22 and the reader 10 for a contactless transaction to less than approximately 500 milliseconds. To prevent an offline sleeve attack on the contactless transaction, various embodiments of the method 40 may utilize a novel type of dynamic data authentication. For offline transactions, the card 22 may utilize the application transaction counter (ATC) and the card unpredictable number, along with the terminal unpredictable number, the transaction amount and the transaction currency code included in the third command message (e.g., GPO) to create the dynamic signature. The application file locator (AFL), which is subsequently sent with the dynamic signature to the reader 10 in the response to the third command message, points to records containing the RSA certificates and data related to dynamic data authentication. Therefore, during the authentication step 50, the reader 10 may read an issuer certificate, a contactless card certificate, and data related to dynamic data authentication. According to various embodiments, the reader 10 may utilize the application transaction counter (ATC), the card unpredictable number, the terminal unpredictable number, the transaction amount and the transaction currency code received from the card 22 in response to the fourth command message to recalculate the dynamic signature for validation purposes. In instances where the contactless transaction has been subjected to a sleeve attack, the recalculation will not match the dynamic signature previously received from the card 22. For such instances, the reader 10 may decline or terminate the contactless transaction.

[0041] Figure 7 illustrates various embodiments of a method 60 for reducing an interaction time for a second contactless transaction that occurs following the request for

online authorization at step 50 of method 40. According to various embodiments, the method 60 may comprise a portion of the method 40. The method 60 may be implemented by the system 20 of Figure 2. The method 60 may be utilized to minimize the interaction time between the card 22 and the reader 10 for the second contactless transaction to less than approximately 500 milliseconds. According to various embodiments, the method 60 comprises the general steps of second transaction request 62, application selection 64, application processing 66, and transaction approval 68.

[0042] The second contactless transaction is not a financial transaction. As the second contactless transaction comprises the card 22 being presented within range of the reader 10 for a second time, the process may be referred to as card return processing. Prior to the start of the process, during the first transaction described hereinabove, both the reader 10 and the card 22 may indicate to one another that they support card return processing. For example, the reader 10 and the card 22 may indicate their support of card return processing during the application selection step 46 of the first transaction.

[0043] After the request for online authorization at step 50 of method 40, either the reader 10 or the card 22 (via the cardholder) may request the second contactless transaction during the second transaction request step 62. According to various embodiments, the reader 10 may request the second contactless transaction during the second transaction request step 62 when an issuer response to the online authorization request comprises a message to be delivered to the card 22. Such a message may be utilized to provide updates or counter resets to the card 22, or to block the account. For example, in an online authorization response, the issuer 30 may include a script message in the response which requests that the card 22 be presented for a second time. In this manner, the issuer 30 may be able to subsequently block the account, replenish offline spending capability, increase the offline spending limit, etc. even if the card 22 has not requested that such actions be taken. To prompt the cardholder to

present the card 22 for a second time, the reader 10 may display a message indicating that additional card processing time is required, a message requesting to please present the card again, etc.

[0044] According to other embodiments, the card 22 may request the second transaction in order to receive a reload when card offline spending capability becomes low. For example, when card offline spending capability becomes low, the card 22, via the cardholder, may request a reload by requesting an online authorization and providing the current available spending amount. To ensure that the card 22 being presented is the same card 22 which was presented for the first transaction, the card 22 may be authenticated during the second transaction request step 62.

[0045] The application selection 64 step follows the second transaction request step 62. The application selection step 64 of method 60 may be similar to the application selection step 46 of the method 40 described hereinabove. During the application selection step 64, the reader 10 transmits a command message (e.g., SELECT VSDC AID) to the card 22. The command message may serve as a request to conduct the second transaction utilizing a specific application from the list of common applications previously built by the reader 10. Responsive to the command message, the card 22 transmits a PDOL to the reader 10. The PDOL may be similar to the PDOL transmitted to the reader 10 during the application selection step 46 of the method 40 described hereinabove. If the PDOL includes a particular data element (e.g., terminal transaction qualifiers), the process advances to the application processing step 66.

[0046] The application processing step 66 follows the application selection step 64. The application processing step 66 may be similar to the application processing step 48 of the method 40 described hereinabove, but is different in that no financial transaction processing is involved. During the application processing step 66, the reader 10 transmits another

command message (e.g., GPO) to the card 22. Upon receipt of the command message, the card 22 builds an appropriate response and transmits the response to the reader 10.

[0047] The transaction approval step 68 follows the application processing step 66. According to various embodiments, if the issuer 30 decides to reload the offline spending capability associated with the card 22, the issuer 30 may transmit a response cryptogram and approve the transaction or include a script message with a message authentication code (MAC). The cryptogram or the MAC may serve to ensure that the updates, counter resets, etc. are only made to cards 22 associated with the issuer 30.

[0048] As described hereinabove, the method 60 may be utilized to change card risk parameters, card counters, card status, etc. For example, with respect to changing card risk parameters, the method 60 may be utilized to increase the offline spending limit, increase the single transaction limit, allow the card to perform transactions in two or more different currencies, change the currency conversion rate utilized, etc. With respect to changing card counters, the method 60 may be utilized, for example, to reset the offline available spending amount, etc. With respect to changing the card status, the method 60 may be utilized to block or unblock a particular application. One skilled in the art will appreciate that the method 60 may be utilized to change other parameters, counters, etc.

[0049] While several embodiments of the invention have been described herein by way of example, those skilled in the art will appreciate that various modifications, alterations, and adaptions to the described embodiments may be realized without departing from the spirit and scope of the invention defined by the appended claims. For example, according to various embodiments, the reader 10, system 20 and/or the method 40 described hereinabove may be modified to prevent analogous types of "sleeve attacks" on wireless handsets, USB fobs, and other devices which utilize the wireless transmission of information. Additionally,

various embodiments of the method 60 may be utilized to process transactions related to currency conversions, loyalty programs, etc.

The claims defining the invention are as follows:

1. A reader, comprising:

a contactless interface;

a transaction module coupled to the contactless interface, wherein the transaction module is structured and arranged to;

discover the presence of a contactless payment device within a predetermined distance from the reader;

energize the contactless interface upon discovery of the presence of the contactless payment device within the predetermined distance form the reader, wherein the energized contactless interface enables communication between the contactless payment device and the reader; and

process a contactless transaction with less than one-half second of interaction time between the contactless payment device and the reader; and

a security module coupled to the transaction module, wherein the security module is structured and arranged to prevent a man in the middle attack on the contactless transaction.

2. The reader of claim 1, wherein the transaction module is structured and arranged to perform static data authentication.

3. The reader of claim 1, wherein the transaction module is structured and arranged to perform dynamic data authentication.

4. A card, comprising:

a transaction module structured and arranged;

for wireless communication, wherein the card is structured and arranged to operate in a chip-mode and a magnetic stripe data mode;

to cooperate with a reader to:

be discoverable by being within a predetermined distance from the reader; and

execute a contactless transaction with less than one-half second of interaction time between the card and the reader; and

a security module structured and arranged to cooperate with the reader to prevent a man in the middle attack on the contactless transaction.

5. A system, comprising:

a card;

a reader, comprising:

a contactless interface;

a transaction module coupled to the contactless interface, and structured and arranged to:

energize the contactless interface upon discovery of the presence of the card within a predetermined distance from the reader, wherein the energized contactless interface enables communication between the card and the reader; and

process a contactless transaction with less than one-half second of interaction time between the card and the reader; and

a security module structured and arranged to cooperate with the reader to prevent a man in the middle attack on the contactless transaction.

6. The system of claim 5, wherein the card comprises a transaction module structured and arranged to cooperate with the reader to execute the contactless transaction.

7. The system of claim 6, wherein the card further comprises a security module structured and arranged to cooperate with the reader to prevent a man in the middle attack on the contactless transaction.

8. The system of claim 5, further comprising a network coupled to the reader.

9. The system of claim 8, wherein the network is further coupled to an issuer.

10. A method for reducing an interaction time for a contactless transaction, the method comprising:

at a reader,

performing at least one transaction-based risk management process prior to energizing a contactless interface;

energizing the contactless interface upon discovery of the presence of a card within a predetermined distance from the reader, wherein the energized contactless interface enables communication between the card and the reader;

initiating communication with the card utilized for the contactless transaction;

receiving information associated with the card; and

terminating communication with the card prior to authorizing the contactless transaction;

utilizing a security module structured and arranged to prevent a man in the middle attack on the contactless transaction; and

completing the contactless transaction with less than one-half second of interaction time between the card and the reader.

11. The method of claim 10, wherein the interaction time is between the card and the reader.

12. The method of claim 10, wherein performing the at least one transaction-based risk process comprises comparing a transaction amount to a predetermined value.

13. The method of claim 10, wherein receiving information associated with the card comprises receiving information associated with at least one application supported by the card.

14. The method of claim 10, wherein receiving information associated with the card comprises receiving at least one of the following:

a cryptogram; and

a dynamic signature.

15. The method of claim 10, wherein terminating communication with the card comprises terminating communication with the card prior to performing an online authorization.

16. The method of claim 10, wherein terminating communication with the card comprises terminating communication with the card prior to performing an offline authorization.

17. The method of claim 15, further comprising:

receiving a request for a second contactless transaction;

re-establishing communication with the card; and

completing the second contactless transaction with less than one-half second of interaction between the card and the reader.

18. The method of claim 17, wherein receiving the request comprises receiving a request for a non-financial transaction.

19. The method of claim 17, wherein completing the second transaction comprises transmitting a message which changes at least one card risk parameter.

20. The method of claim 17, wherein completing the second transaction comprises transmitting a message which changes at least one card counter.

21. The method of claim 17, wherein completing the second transaction comprises transmitting a message which changes at least one card status.

22. The method of claim 10, wherein utilizing a security module structured and arranged to prevent for preventing a man in the middle attack on the contactless transaction comprises :

receiving a dynamic signature that comprises an application transaction counter, a terminal unpredictable number, a transaction amount, a transaction currency code, and a card unpredictable number;

receiving a card unpredictable number;

recalculating the dynamic signature utilizing the card unpredictable number; and

authorizing the contactless transaction offline if the dynamic signature is validated.

23. The method of claim 22 further comprising:

receiving a cryptogram that comprises an application transaction counter, a transaction amount, and a terminal unpredictable number; and

requesting the transaction be processed online with the cryptogram if the dynamic signature is not validated.

24. A reader substantially as hereinbefore described with reference to any one of the embodiments as that embodiment is shown n the accompanying drawings.

DATED this Twenty second Day of July, 2011

Visa International Service Association

Patent Attorneys for the Applicant

SPRUSON & FERGUSON

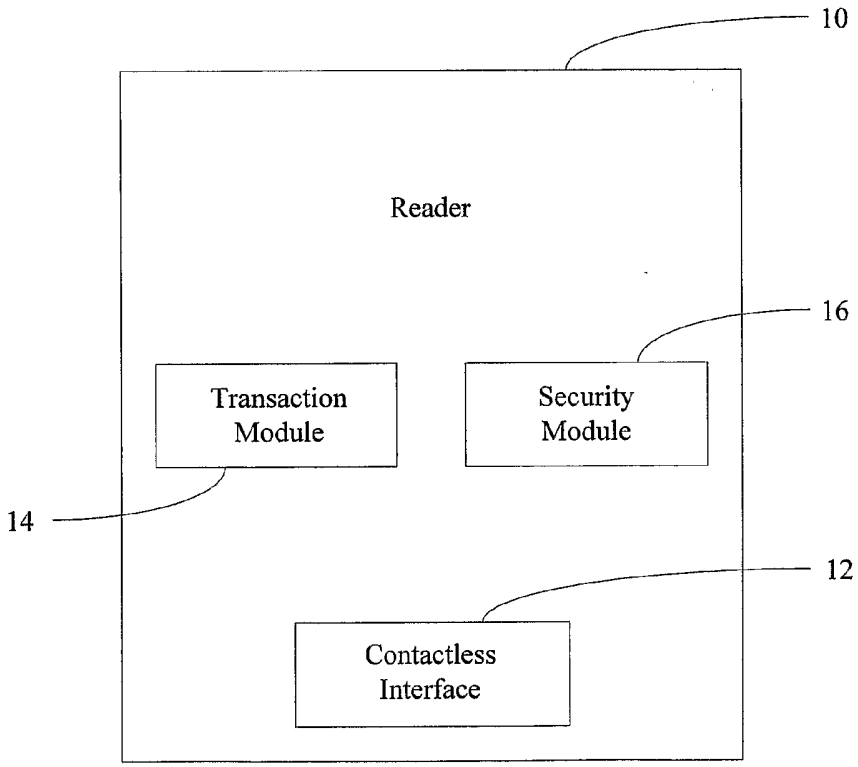

10
Reader
16
Transaction Module
Security Module
14
12
Contactless Interface

FIG. 1

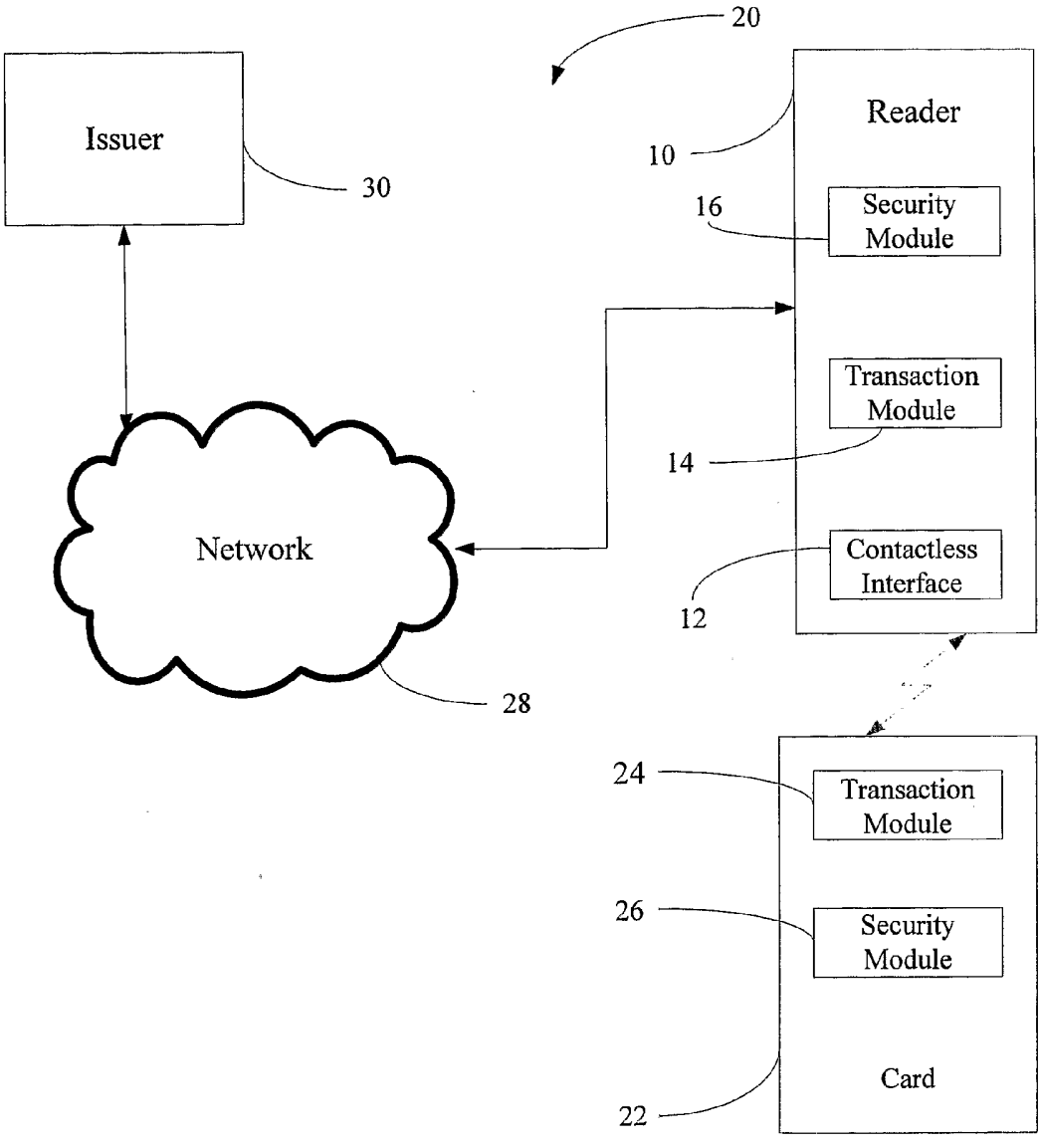

20
Issuer
30
Reader
10
16
Security Module
Transaction Module
14
Network
Contactless Interface
12
28
24
Transaction Module
26
Security Module
Card
22

FIG. 2

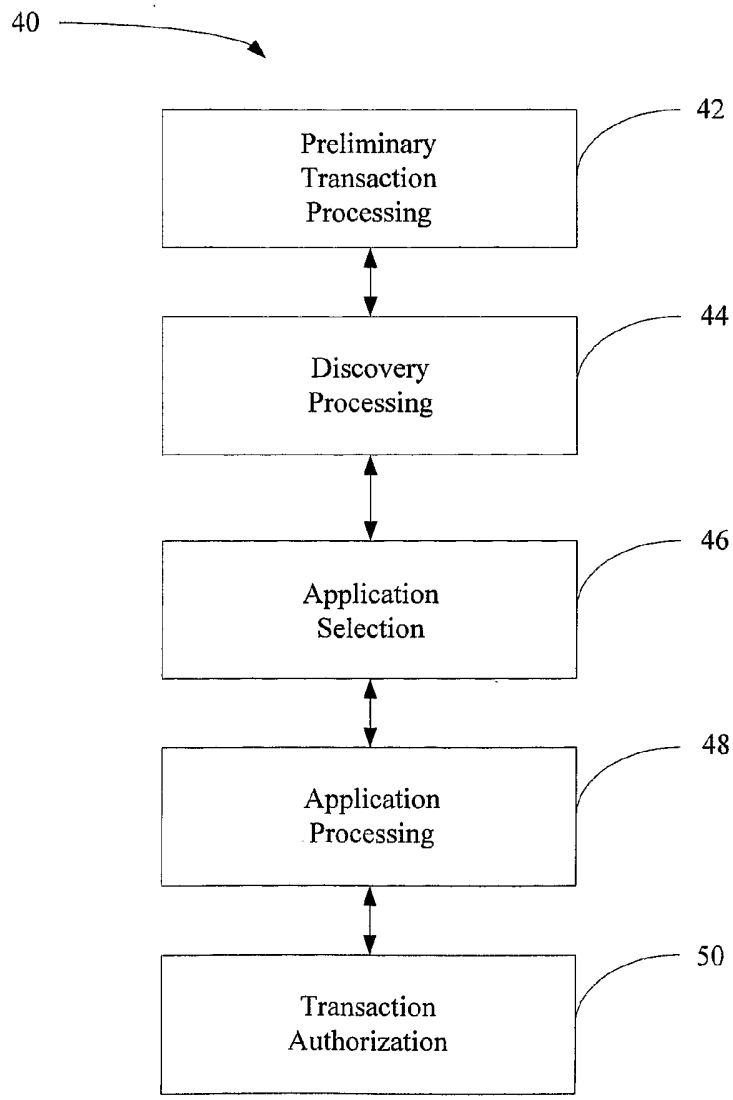

40
Preliminary Transaction Processing
42
Discovery Processing
44
Application Selection
46
Application Processing
48
Transaction Authorization
50

FIG. 3

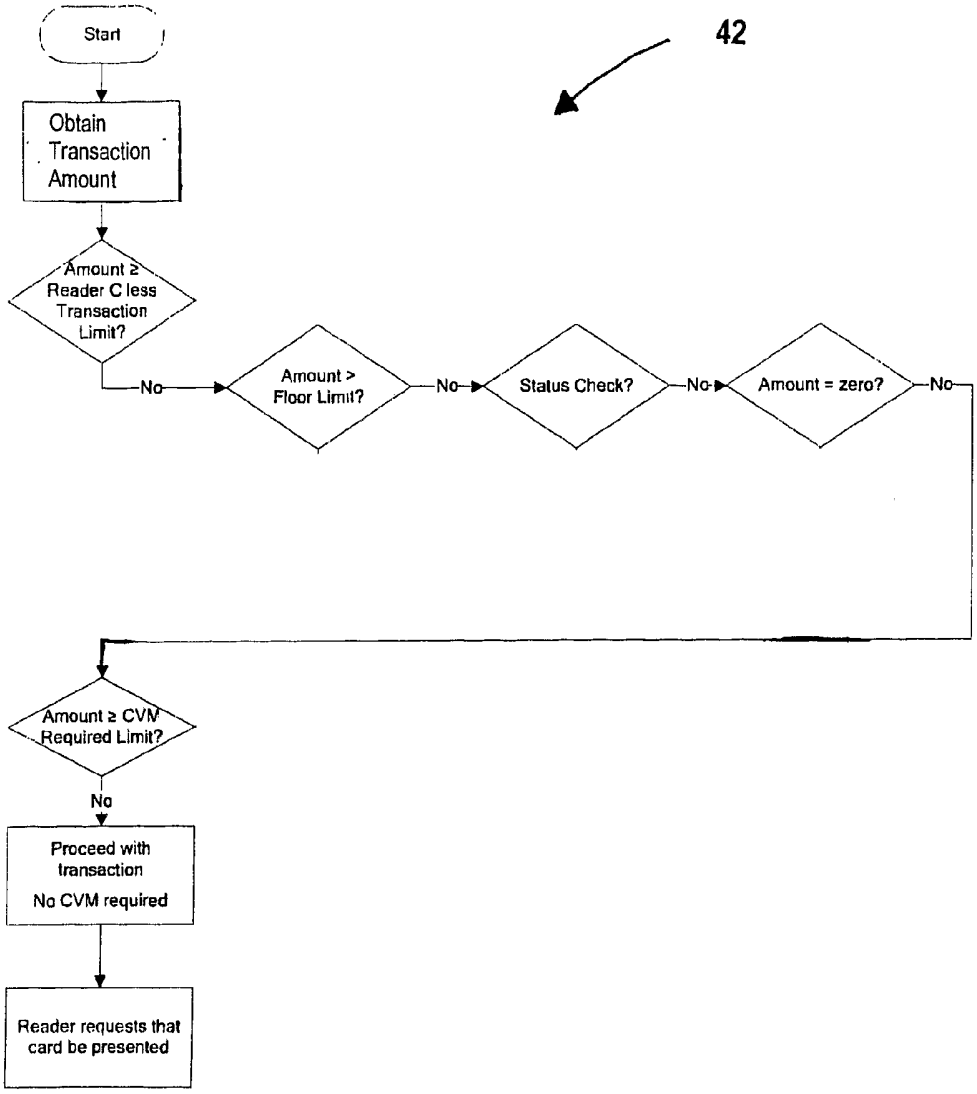

42
Start
Obtain Transaction Amount
Amount ≥ Reader C less Transaction Limit?
No
Amount > Floor Limit?
No
Status Check?
No
Amount = zero?
No
Amount ≥ CVM Required Limit?
No
Proceed with transaction
No CVM required
Reader requests that card be presented

Fig. 4

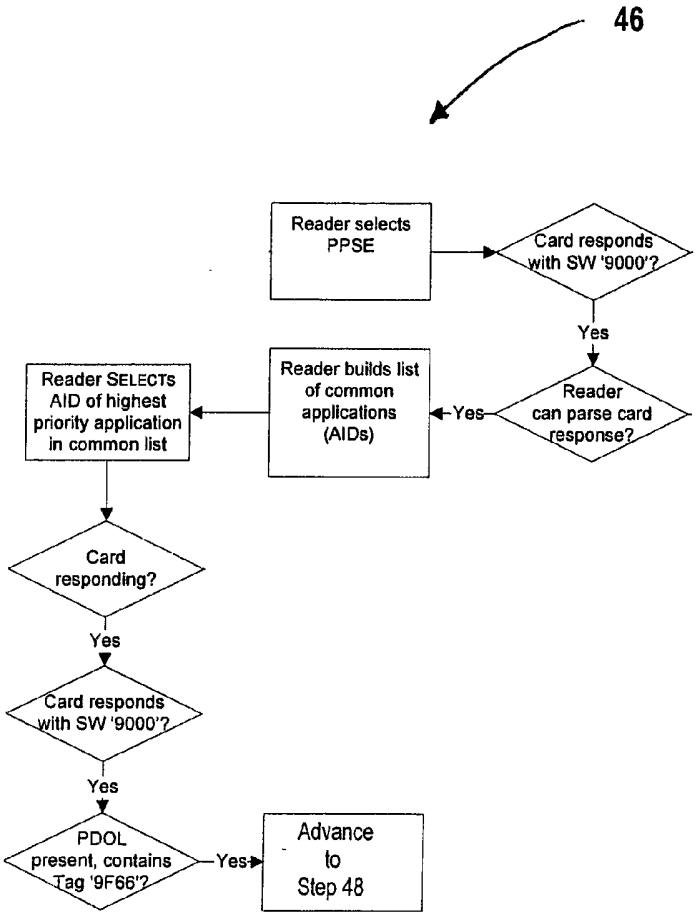

46
Reader selects PPSE
Card responds with SW '9000'?
Yes
Reader can parse card response?
Yes
Reader builds list of common applications (AIDs)
Reader SELECTS AID of highest priority application in common list
Card responding?
Yes
Card responds with SW '9000'?
Yes
PDOL present, contains Tag '9F66'?
Yes
Advance to Step 48

Fig. 5

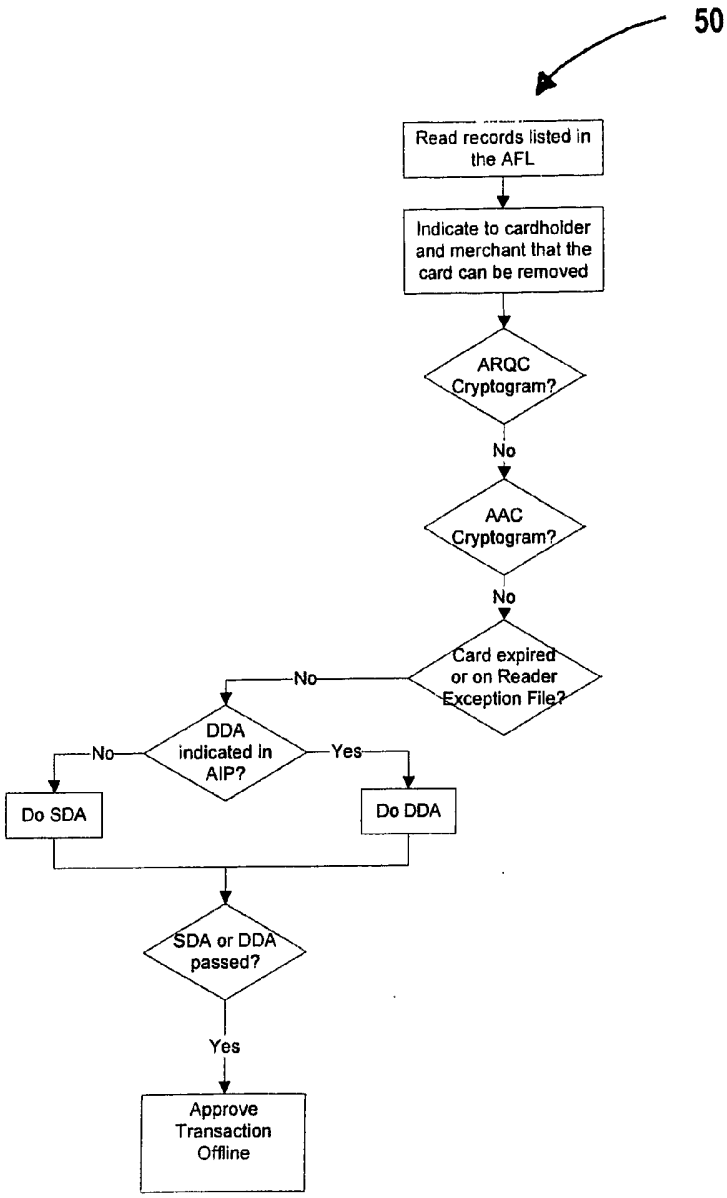

50
Read records listed in the AFL
Indicate to cardholder and merchant that the card can be removed
ARQC Cryptogram?
No
AAC Cryptogram?
No
Card expired or on Reader Exception File?
No
DDA indicated in AIP?
No
Yes
Do SDA
Do DDA
SDA or DDA passed?
Yes
Approve Transaction Offline

Fig. 6

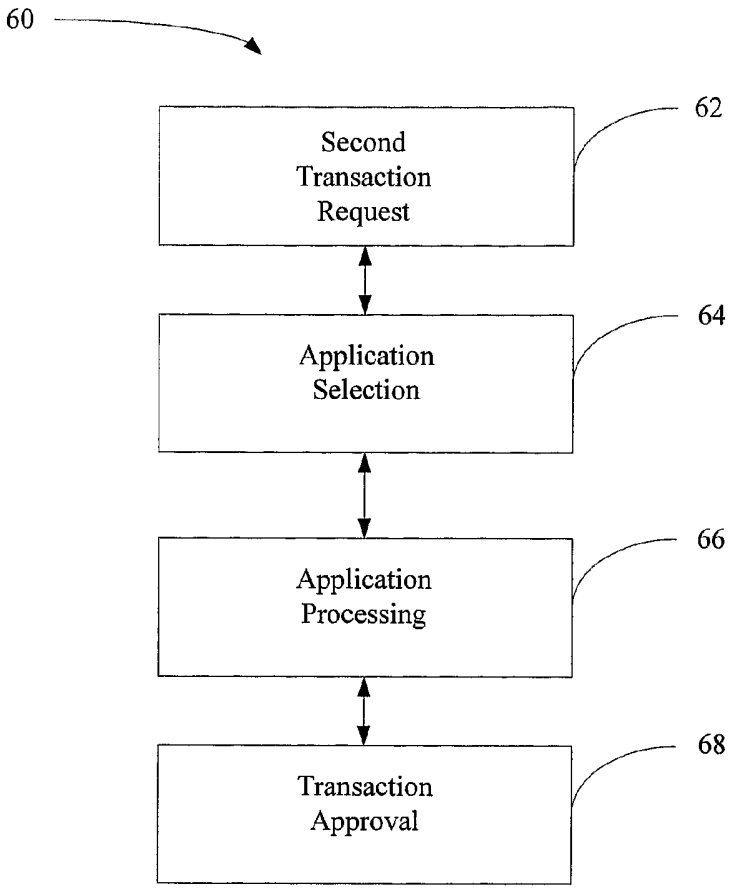

60
Second Transaction Request
62
Application Selection
64
Application Processing
66
Transaction Approval
68

FIG. 7