

SYSTEMS AND METHODS FOR TRANSACTION CARD-BASED AUTHENTICATION

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority to U.S. Patent Application No. 17/214,073 filed March 26, 2021, the disclosure of which is incorporated herein by reference in its entirety.

FIELD OF THE INVENTION

[0002] The present disclosure relates generally to transaction security and, more specifically, to exemplary systems, methods, and computer-accessible mediums for using a transaction card to carry out a challenge response security protocol.

BACKGROUND OF THE INVENTION

[0003] The development of electronic commerce has led to the convenience of consumers and businesses alike. Transactions may be conducted between and among parties from virtually any location and at any time. Use of cards such as credit and debit cards has enhanced the ability to conduct transactions over networks, as consumers may engage in purchase transactions, or conduct other business, merely by providing credentials including a name, a card number, and other data such as, for example, a card expiration date, a card security code, or a billing zip code.

[0004] But the increasing use of cards has also resulted in increased risk of fraud or theft. Despite efforts to make card-based transactions more secure, smart cards and other devices may often be vulnerable to replay attacks in which card and/or transaction information is intercepted and subsequently used in a fraudulent manner to carry out additional transactions.

SUMMARY OF THE INVENTION

[0005] An illustrative aspect of the invention provides a method of communicating with a transaction card having a card data processor, a near card field communication (NFC) interface, and a card memory having a unique card identifier stored therein. The method comprises establishing, by a user communication device, a first NFC session with the transaction card and transmitting, by the user communication device to the transaction card, an NFC data exchange format (NDEF) WRITE TAG command including session-specific challenge information. The method further comprises transmitting, by the user communication device to the transaction card, an NDEF READ TAG command and receiving, by the user communication device from the transaction card, card-specific challenge response information. The method also comprises authenticating the transaction card using the challenge response information.

[0006] Another aspect of the invention provides a user communication device comprising a communication device data processor and an NFC interface in communication with the data processor. The NFC interface is configured for communication with one or more transaction cards. The user communication device further comprises a communication device memory accessible by the data processor and containing a card communication application with instructions to be carried out by the data processor. The communication application is configured to establish a first NFC session with a transaction card, and transmit, to the transaction card, an NDEF WRITE TAG command including session-specific challenge information. The application is further configured to transmit, to the transaction card, an NDEF READ TAG command, receive, from the transaction card, card-specific challenge response information, and authenticate the transaction card.

[0007] Another aspect of the invention provides a transaction card comprising a card

microprocessor, a near field communication (NFC) interface, and a card memory having a card identifier and one or more applets stored therein. The one or more applets include instructions for the card microprocessor to receive, from a user communication device via the NFC interface, an NDEF WRITE TAG command including challenge information and generate a digital signature using the challenge information. The one or more applets include further instructions to receive, from the user communication device via the NFC interface, an NDEF READ TAG command, and transmit, to the user communication device, the digital signature.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Figure 1 is a flow chart of actions in a method of communicating with a transaction card according to an embodiment of the invention;

[0009] Figure 2 is a flow chart of actions in a method of authenticating a communication between a transaction card and a user communication device according to an embodiment of the invention;

[0010] Figure 3 is a schematic representation of a transaction card authentication system according to an embodiment of the invention; and

[0011] Figure 4 is a block diagram of a transaction card microprocessor chip according to an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0012] The following description of embodiments provides non-limiting representative examples referencing numerals to particularly describe features and teachings of different aspects of the invention. While the invention will be described in connection with particular embodiments and environments, it will be understood that the invention is not limited to

these embodiments and environments. On the contrary, it is contemplated that various alternatives, modifications and equivalents are included within the spirit and scope of the invention as described. Further, the embodiments described should be recognized as being capable of separate implementation or of combination with other embodiments.

[0013] As used herein, the term “transaction card” refers to any identification or payment card associated with a user or user account. This may include, in particular, a credit card, debit card, or gift card, any of which may be issued by a service provider. Smart transaction cards are often used to carry out transactions through near field communication (NFC) or brief contact communication (e.g., “tapping”) with transaction processing devices. Because of inherent limitations in the transaction processing device, such cards may not be suitable for use in authentication, except as part of a low-level protocol.

[0014] The present invention provides an approach that enhances the value of a smart transaction card in carrying out a multi-factor security protocol. This approach involves a challenge response protocol that makes use of a user processing device’s ability to transmit NFC data exchange format (NDEF) WRITE and READ commands to the transaction card. In methods of the invention, the user may establish an NFC communication session between the transaction card and the user device (e.g., by tapping or otherwise bringing the user device within communication range of the card). The user device transmits a WRITE NDEF to the transaction card. The transaction card reads the information from the WRITE command and uses it to create a digital signature. The user device then transmits a READ NDEF command to the transaction card, whereupon the transaction card transmits the digital signature to the user device. The signature may be accompanied by a certificate signed by a trusted authority. The user device may then itself validate the card signature or may pass the

signature to a validation system. In either case, validation of the signature could be used for authentication of the presence of the transaction card and/or as an authentication factor in a multi-factor authentication of the user.

[0015] Figure 1 illustrates a basic method M100 of communication between a user communication device and a transaction card. The method M100 can be used as part of a user and/or card authentication process. As will be discussed in more detail hereafter, transaction cards usable in methods of the invention may have a card data processor, a near field communication interface and a card memory. The card memory may have card-unique information stored therein, including a unique card identifier. In some embodiments, the card memory may have one or more encryption keys stored therein. The user communication device may be any data processing device having near field communication capability and will typically be a network-enabled computer system. As used herein, the term network-enabled computer system (and/or device) may include, but is not limited to, any computer device, or communications device including, a server, a microprocessor or system of microprocessors, a network appliance, a personal computer (PC), a workstation, and a mobile processing device such as a smart phone, smart pad, handheld PC, or personal digital assistant (PDA). In some examples, the computer device may use instructions stored on a computer-accessible medium (e.g., a storage device such as a hard disk, floppy disk, memory stick, CD-ROM, RAM, ROM, etc., or a collection thereof). The computer-accessible medium can contain executable instructions thereon. In addition or alternatively, a storage arrangement can be provided separately from the computer-accessible medium, which can provide the instructions to the processing arrangement so as to configure the processing arrangement to execute certain exemplary procedures, processes, and methods, as

described herein. Mobile processing devices, in particular, may include NFC capabilities that allow for communication with other NFC-enabled devices by touching the devices together or bringing them into close proximity.

[0016] In some embodiments of the invention, the user communication device may be a merchant terminal or other device configured for carrying out financial and other transactions. Such merchant device may be specifically configured for carrying out transactions based on an account associated with the transaction card and/or the transaction card administrator or processor. In other embodiments of the invention, the user communication device may be a mobile device, which may be associated with a user who is a holder of an account associated with the transaction card.

[0017] At S110 of the method M100, an NFC communication session is initiated between the user communication device and the transaction card. This will typically be accomplished by tapping the card to the user communication device or otherwise bringing the card to within NFC communication range of the user communication device. The action of initiating the NFC session may be taken as part of a purchase or other transaction that involves an account associated with the transaction card. In some embodiments, however, the action may be taken as part of an authentication or authorization protocol in conjunction with a transaction that does not otherwise involve an account associated with the transaction card. For example, a purchase may be made from a merchant using another card. The merchant may require authentication of the user/account holder using the smart transaction card, whereupon NFC communication can be established between a merchant terminal and the transaction card.

[0018] In some embodiments, the action of establishing NFC communication may be carried

out in response to receiving an authentication request from a transaction processing server or authentication server. Such a request may, may be transmitted by the server in response to a request to carry out a transaction requiring verification of the presence of the transaction card or otherwise requiring authentication of the transaction card or the user. Upon receiving the authentication request, the user communication device may display or otherwise convey an instruction to initiate NFC communication with the transaction card.

[0019] In embodiments of the invention, the user communication device may include an application for transmitting standardized NDEF messages for communication with NFC-enabled devices. Such methods are used, in particular, for communication with standardized tags (e.g., Radio Frequency Identification (RFID) tags) and include “WRITE TAG” commands for assigning information to a tag and “READ TAG” commands for reading information from a tag. At S120 of the method M100, the user communication device transmits a WRITE TAG command to the transaction card. The WRITE TAG command includes challenge information for use by the transaction card in generating a challenge response. The challenge information may be or include information that is unique to the NFC session. This may include, for example, a one-time, random or pseudo-random or otherwise unpredictable number. The challenge information may be generated by the user communication device or by a requesting processing or authentication server. In some embodiments, the challenge information may be included in an authentication request received by the user communication device from a processing or authentication server. In other cases, the user communication device may transmit NFC session information to a requesting server and receive session-specific challenge information in return.

[0020] The user communication device transmits a READ TAG command to the transaction

card at S130, and, at S140, receives a transmitted READ TAG response from the transaction card. In some embodiments of the invention, the READ TAG command must be sent to the transaction card within the same NFC communication session as the WRITE TAG command. In such embodiments, termination of the NFC session prior to the READ TAG command would result in termination without authentication of the transaction card. In these circumstances, card authentication would require a new NFC session and new challenge information. In other embodiments, however, the method M100 may include termination of the NFC session (e.g., by removal of the transaction card from NFC communication range) and initiation of a second NFC communication session prior to the action of transmitting the READ TAG command. In some embodiments, such termination and re-initiation of NFC communication may be an allowable occurrence while in others, it may be required.

[0021] Whether a single NFC session or multiple sessions are used, the method M100 may include a time limit for transmitting the READ TAG command. This time limit may be based on a predetermined maximum time interval between the transmitting of the WRITE TAG command and the transmitting of the READ TAG command. In embodiments where multiple NFC sessions are allowed or required, a maximum time interval between termination of the first session and initiation of the second session may be specified.

[0022] The READ TAG response includes challenge response information that is unique to the transaction card. This may include, for example, a card identifier. The challenge response information may be or include information that is generated by the transaction card's data processing chip using information that is permanently assigned and/or wired into a memory of the transaction card. In particular embodiments, the challenge response information may include information that is encrypted by the card data processing chip. The

challenge response information may also include a digital authentication certificate from a trusted source. Such a certificate may be used as a public key in encrypting and decrypting the challenge response information.

[0023] At S150, the transaction card is authenticated using the challenge response information. In some embodiments, the authentication action may be carried out entirely by the user communication device. This may include comparing card-unique information to previously stored card information. Alternatively or in addition, authentication may include decrypting information encrypted by the transaction card data processor. Successful decryption would indicate a positive authentication of the transaction card. The foregoing approach may require, however, that one or more private encryption keys stored in the transaction card memory would also need to be available to the user communication device. To avoid this requirement, in some embodiments, the user communication device may transmit some or all of the challenge response information to an authentication-requesting server or directly to an authentication server having access to card-specific encryption keys. In such embodiments, the user communication device may receive back an authentication response indicating that the transaction card has been authenticated or that authentication failed.

[0024] In embodiments where authentication is carried out by the user communication device, the method M100 may further include transmitting the results of the authentication to a requesting processing server or authentication server.

[0025] Figure 2 illustrates a basic method M200 for a smart transaction card to authenticate communication with a user communication device according to an illustrative embodiment of the invention. A typical transaction card usable to carry out the method M200 has a card data

processor, an NFC interface, and a card memory having a unique card identifier stored therein. In some embodiments, the card memory may also have one or more card-unique encryption keys stored therein. At S210, of the method M200, an NFC communication session is established between the card data processor and a user communication device. The user communication device may be, for example, a merchant transaction terminal, a mobile user device, or other network-enabled device or system. The NFC communication session may be initiated by tapping the card to the user communication device or otherwise bringing the card to within NFC communication range of the user communication device. At S220, the card data processor receives a WRITE TAG command from the user communication device via the card's NFC interface. The WRITE TAG command includes challenge information, which may be or include information that is unique to the NFC session. This may include, for example, a one-time, random or pseudo-random or otherwise unpredictable number.

[0026] At S230, the card data processor uses the challenge information to generate a challenge response. The challenge response information may be or include a card-unique and/or session-unique signature. In particular embodiments, the signature may be or include information from the challenge information that has been encrypted by the card processor using one or more card-unique encryption keys. A public key (e.g., a trusted source certificate) may also be used in the encryption. The challenge response may also include a card identifier and/or a public key used in the encryption of challenge information.

[0027] The card data processor receives a READ TAG command from the user communication device via the card NFC interface at S240 and transmits the challenge response back to the user communication device at S250.

[0028] With reference now to Figure 3, an exemplary transaction card authentication system 100 according to an embodiment of the invention may include a user device 110, a transaction card 150, a processing server 120 and a card information database 140. The user device 110 may communicate with the processing server 120 via a network 105. The processing server 120 and/or user device 110 may also communicate with an authentication server 130. Although Figure 3 illustrates certain components connected in certain ways, system 100 may include additional or multiple components connected in various ways. In particular, the system 100 may include multiple user devices 110 and multiple transaction cards 150.

[0029] The systems and components of the system 100 may be or include network-enabled computer devices and systems that are configured for processing account-related transactions. In particular, these systems may be configured to execute one or more software applications to, for example, receive data as input from an entity accessing the network-enabled computer system, process received data, transmit data over a network, and receive data over a network in order to process transactions originating from a merchant transaction device or an account holder's device. The various network-enabled computer systems may also include one or more software applications to transmit notifications to account holders (e.g., via the account holders' computer systems or mobile devices). It will be understood that the depiction in Figure 3 is an example only, and the functions and processes described herein may be performed by any number of network-enabled computers. It will also be understood that where the illustrated system 100 may have only a single instance of certain components, multiple instances of these components may be used. The system 100 may also include other devices not depicted in Figure 3.

[0030] In the example embodiments presented herein, an account holder may be any individual or entity that desires to conduct a transaction (which may be, but is not limited to a financial transaction) with a merchant using a transaction account. An account may be held by any place, location, object, entity, or other mechanism for holding money or performing transactions in any form, including, without limitation, electronic form. An account may be associated with one or more transaction cards such as, for example, a credit or debit card or a prepaid card.

[0031] The various components of the system 100 may, in particular, be configured for processing transactions involving the use of a transaction card such as the smart transaction card 150. The transaction card 150 may be any device having a processor configured for communicating via NFC and carrying out digital transactions and having a memory in which identification and encryption information can be stored. This may include chip-carrying transaction cards (“smart” cards), and mobile and non-mobile user computing devices. As illustrated in Figures 3 and 4, a typical transaction card 150 that is usable in various embodiments of the invention is a smart card with a microprocessor chip 151. The microprocessor chip 151 includes processing circuitry for storing and processing information, including a microprocessor 152 and a memory 156. It will be understood that the processing circuitry may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamper-proofing hardware, as necessary to perform the functions described herein. The memory 156 may be a read-only memory, write-once read-multiple memory or read/write memory, e.g., RAM, ROM, and EEPROM, and the chip 151 may include one or more of these memories. The memory 156 may be configured to store

one or more software applications for execution by the microprocessor 152. Information associated with an account may also be stored in the memory 156. In particular, the memory 156 may have permanently stored therein a unique alphanumeric identifier and one or more public and private card encryption keys.

[0032] The microprocessor chip 151 further includes an NFC interface 154 configured for establishing communication with the user device 110 or other devices when the card 150 is within a predetermined NFC range. In some embodiments, the NFC interface 154 may comprise a radio frequency identification chip configured to communicate via NFC or other short-range protocols. In some embodiments, the microprocessor chip 151 may include circuitry configured for communication with the user device 110 via other means such as Bluetooth, satellite, Wi-Fi, wired communications, and/or any combination of wireless and wired connections.

[0033] In particular embodiments, the memory 156 of the chip 151 microprocessor chip 151 may have stored therein one or more applets with instructions for generating encrypted information and transmitting it to a receiving device (e.g., the user device 110) via the NFC interface 154. Such encrypted information may be or include an encrypted verification block or signature that may be used by the user device 110 or the processing server 120 to authenticate and verify the presence of the transaction card 150.

[0034] The memory 156 may, in particular, have an authentication application stored therein having instructions for the data processor 152 to establish an NFC communication session with a user communication device 110 and receive, via the NFC interface 154, a WRITE TAG command transmitted by the user communication device 110. The application may be configured to recognize the WRITE TAG command as an authentication challenge and, upon

such recognition, to generate a challenge response based on challenge information included therein. The challenge response may include challenge response information that is unique to the transaction card. This may include, for example, a card identifier. The challenge response information may be or include information that is generated by the data processor 152 using information that is permanently or temporarily stored in the card memory 156. In particular embodiments, the authentication application is configured to cause the processor 152 to generate a digital signature that may be unique to the transaction card 150 and/or the NFC session. The digital signature and/or other challenge response information may be or include a cryptogram encrypted using challenge information received in the WRITE TAG command by the card data processing chip. The cryptogram may be created by the processor 152 using one or more of the public and private encryption keys stored in the memory 156. The challenge response information may also include a digital authentication certificate retrieved from the memory 156.

[0035] The authentication application may also be configured to receive a READ TAG command via NFC from the user communication device 110. In response, the application may transmit the challenge response via the NFC interface 154. In some embodiments, the authentication application may be configured so that the action of generating a digital signature and/or other challenge response information is not carried out unless or until a READ TAG command is received. In such embodiments, the actions of generating the challenge response information and transmitting the challenge response information may both be done in response to receiving the READ TAG command. In some embodiments, either or both of these actions may be conditioned on a time interval between the WRITE TAG command and the READ TAG command being less than a specified maximum time

interval. If the maximum time interval is exceeded, the microprocessor 152 may transmit a “timed out” error message to the user communication device 110 via the NFC interface 154.

[0036] In some embodiments, the authentication application may be configured to terminate the authentication procedure if the NFC session with the user communication device 110 is ended prior to receiving the READ TAG command. In other embodiments, the application may allow or require termination of the initial NFC session after the WRITE TAG command is received and subsequent establishment of a second NFC session in which the READ TAG command is received. As before, transmission of the challenge response may be conditioned on the READ TAG command being received within a maximum time interval after the WRITE TAG command.

[0037] The user communication device 110 may be any computer device or communications device including a server, a network appliance, a personal computer (PC), a workstation, and a mobile interface device such as a smart phone, smart pad, handheld PC, or personal digital assistant (PDA). The user communication device 110 may also be a transaction terminal (e.g., a merchant or bank terminal) used for carrying out financial transactions and other interactions with an account holder. The user device 110 includes an on-board data processor 111 in communication with a memory module 113, a user interface 114, a network communication interface 112, and an NFC interface 116. The user device 110 may optionally include an image capturing device 115 (e.g., a digital camera). The data processor 111 may include a microprocessor and associated processing circuitry, and can contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamper-proofing hardware, as necessary to perform the functions described herein. The

memory 113 can be a read-only memory, write-once read-multiple memory or read/write memory, e.g., RAM, ROM and EEPROM, and the user device 110 can include one or more of these memories.

[0038] The user interface 114 of the device 110 includes a user input mechanism, which can be any device for entering information and instructions into the user device 110, such as a touch-screen, keyboard, mouse, cursor-control device, microphone, stylus, or digital camera. The user interface 114 may also include a display, which can be any type of device for presenting visual information such as a computer monitor, a flat panel display, and a mobile device screen, including liquid crystal displays, light-emitting diode displays, plasma panels, and cathode ray tube displays.

[0039] The network communication interface 112 is configured to establish and support wired or wireless data communication capability for connecting the device 110 to the network 105 or other communication network. The communication interface 112 can also be configured to support communication with a short-range wireless communication interface for communication via a short-range system such as Bluetooth.

[0040] The user device NFC interface 116 is configured for establishing near field communication with other NFC-enabled devices including, in particular, the data processing chip 151 of the transaction card 150. The NFC interface 116 is further configured for transmitting information to and receiving information transmitted by the data processing chip 151 via the chip NFC interface 154.

[0041] In embodiments of the invention, the memory 113 may have stored therein one or more applications usable by the data processor 111 to conduct and/or monitor transactions between the user device 110 and one or more processing servers 120 and authentication

servers 130 over the network 105 and/or one or more merchant transaction terminals (not shown) via NFC, short-range communication, or the network 105. These applications may include instructions usable by the data processor 111 to identify transaction events, store event data in the memory 113, and communicate event data to the servers 120, 130. Some applications may also include instructions relating to receiving and interpreting instructions from the one or more processing servers 120 or the one or more authentication servers 130.

[0042] In particular embodiments, the memory 113 may include one or more applets configured for writing NDEF formatted information to NFC enabled tag devices (e.g., RFID tags) and/or for reading formatted information from such devices. These applets may include, in particular, instructions for executing a WRITE TAG command that causes formatted information to be transmitted to and stored in a memory of a receiving tag and instructions for executing a READ TAG command that causes formatted information to be transmitted by the tag and received by the user device 110. The memory 113 may also have stored therein a card communication application that can invoke the NDEF applets for use in a communication session with the transaction card 150. The card communication application may include instructions for the data processor 111 to establish a first NFC session with the transaction card 150 via the NFC interface 116 and then to transmit an NDEF WRITE TAG command to the transaction card 150 via the NFC interface 116. The application may also include instructions to assemble or receive session-specific challenge information that may be formatted for transmission via the NDEF WRITE TAG command. Such challenge information could include, for example, a session identifier or time stamp to differentiate the NFC session from other sessions. The challenge information may instead or in addition include information specific to an intended transaction card 150, the presence of which is

required for completion of an authentication or authorization process. The challenge information may be generated by the data processor 111 using information received by the data processor 111 from a processing server 120 or authentication server 130 via the network communication interface 112 and/or information stored in the memory 113.

[0043] In some embodiments, the application may be configured to receive an authentication request from a transaction processing server 120 or authentication server 130. Such a request may, may be transmitted by the server in response to a request to carry out a transaction requiring verification of the presence of a particular transaction card 150 or otherwise requiring authentication of the transaction card 150 or the user. Such a request may include challenge information to be included in the WRITE TAG command. The application may be further configured to display information and instructions to the user of the user communication device 110 via the user interface 114. User instructions could include, for example, an instruction to initiate NFC communication with the transaction card 150.

[0044] The card communication application may further include instructions for the data processor 111 to transmit an NDEF READ TAG command to the transaction card 150 and to receive formatted response information from the transaction card 150 in return. The response information may include a card identifier and/or challenge response information constructed by the transaction card 150 using the challenge information. The application may also include instructions for the data processor 111 to use the challenge response information to authenticate the transaction card 150. This may be accomplished by direct comparison of the challenge response information to expected response information stored in the memory 113 or received from a requesting processing server 120 or authentication server 130.

[0045] In some embodiments, the action to authenticate the transaction card 150 may include transmitting the challenge response information to the authentication server 130 and receiving an authentication response back from the authentication server 130. In some embodiments, the challenge response information may be transmitted directly to the authentication server 130 via the network 105. In other embodiments, the user communication device 110 may transmit the challenge response information to the processing server 120 via the network 105 and the processing server 120, in turn, transmits the challenge response information to the authentication server 130.

[0046] In some embodiments, the challenge response information authentication may include information encrypted by the transaction card using card or account-associated encryption keys. In such embodiments, the card communication application may be configured to retrieve the required encryption key(s) from the memory 113 and to use them to decrypt the encrypted information. The application may condition authentication of the card 150 on successful decryption of the challenge response information.

[0047] The communication application may be configured to, upon establishing an authentication result, transmit the authentication result to the processing server 120, the authentication server 130, or other requesting system via the network 105.

[0048] The processing server 120 is a system of one or more network-enabled processing servers configured for processing transactions for an account associated with the transaction card 150. The processing server 120 is configured for selective communication with one or more user communication devices 110 (e.g., account holder mobile or other devices and merchant transaction terminals) via the network 105. The processing server 120 may be configured to store and retrieve account and transaction information in an account

information database (not shown) and transaction card information in the card information database 140. The processing server 120 may receive transaction processing requests from any of the user devices 110 and is configured to use information from such requests to make determinations as to whether the requested transaction should be processed.

[0049] In some embodiments, the processing server 120 may require verification of the presence of an authorized transaction card 150 in order to process a transaction. In some such embodiments, the processing server may transmit a verification request to a user communication device 110 that is associated with the card 150 or its associated account. In other embodiments, the processing server 120 may transmit the request to a user communication device 110 (e.g., a merchant terminal) that is associated with the transaction to be processed. In either case, the verification request includes instructions for the user communication device 110 to establish an NFC communication session between the user communication device 110 and the transaction card 150 for verifying that the card 150 is in the possession of the account holder and/or in the presence of the transaction requester. In some embodiments, the verification is conducted by the user communication device 110 and the processing system 120 merely receives a response from the device 110 indicating a verification result. In some embodiments, however, the user communication device 110 may not conduct the verification and, instead, transmits to the processing server 120 challenge response information received from the transaction card 150. The processing server 120 may be configured to use the challenge response information to complete the authentication/verification of the transaction card 150. In some embodiments, however, the processing server 120 may forward the challenge response information to the authentication server 130 for completion of the authentication/verification process.

[0050] In some embodiments, the processing server 120 may generate challenge information that may be included in the verification request for submission by the user communication device 110 to the card 150. The challenge information may include card and/or transaction specific information. It may instead or in addition include an unpredictable challenge value such as a random or pseudo-random number.

[0051] The authentication server 130 may be a system of one or more network-enabled processing servers configured for selective communication with the user communication device 110 and/or the processing server 120 via the network 105. The authentication processor 130 may also be able to access the card information database 140 via the network 105 either directly or through the processing server 120. The authentication server 130 may be configured for transmitting card authentication requests to and receiving authentication responses from the user communication device 110. The authentication server 130 may be configured to generate challenge information for inclusion in an authentication request. Such challenge information may be or include card-specific information obtained from the card database 140. The challenge information may also or instead include one-time request or transaction-specific information to be used by the transaction card 150 to generate challenge response information. The authentication server 130 may be further configured to receive an authentication request response from the user communication device 110, the response including challenge response information generated by the transaction card 150. The authentication server 130 may be configured to use the challenge response information to verify that such information was generated by the expected transaction card 150.

[0052] The card database 140 may have stored therein one or more data records associated with the transaction card 150. In some embodiments, these records may include one or more

private encryption keys assigned to the transaction card 150 and stored in the card memory 156. The one or more encryption keys may be accessed by the processing server 120 or the authentication server 130 as needed for decryption of card-encrypted information included in the challenge response information. The processing server 120 and/or the authentication server 130 may be configured for using the decryption keys and one or more public keys associated with the transaction card to decrypt the card-encrypted information to verify that the challenge response information was provided by the expected transaction card 150. In some embodiments, a public encryption key may be part of or included with the challenge response information.

[0053] The present invention provides a significant improvement in transaction security by providing enhanced security to the process of assuring the presence of an authenticated transaction card. By using session-specific information in combination with card-specific information to authenticate the presence of a particular account-associated card, the invention makes it difficult or impossible for an intercepting entity to use the information in a replay attack. The methods may be further enhanced by having the card itself encrypt session-specific information using private encryption keys available only from the card and a limited access card database.

[0054] It will be readily understood by those persons skilled in the art that the present invention is susceptible to broad utility and application. Many embodiments and adaptations of the present invention other than those herein described, as well as many variations, modifications and equivalent arrangements, will be apparent from or reasonably suggested by the present invention and foregoing description thereof, without departing from the substance or scope of the invention.

CLAIMS

What is claimed is:

1. A method of communicating with a transaction card having a card data processor, a near card field communication (NFC) interface, and a card memory having a unique card identifier stored therein, the method comprising:
 - establishing, by a user communication device, a first NFC session with the transaction card;
 - transmitting, by the user communication device to the transaction card, an NFC data exchange format (NDEF) WRITE TAG command including session-specific challenge information;
 - transmitting, by the user communication device to the transaction card, an NDEF READ TAG command;
 - receiving, by the user communication device from the transaction card, card-specific challenge response information; and
 - authenticating the transaction card using the challenge response information.
2. A method according to claim 1 wherein the card-specific challenge response information comprises card-encrypted information.
3. A method according to claim 2 wherein the action of authenticating the transaction card includes:
 - attempting to decrypt the card-encrypted information using at least one card-unique key associated with the unique card identifier; and
 - responsive to a successful decryption of the card-encrypted information, establishing a positive authentication result.

4. A method according to claim 2 wherein the card-specific challenge response information further comprises a digital authentication certificate.
5. A method according to claim 1 wherein the session-specific challenge information is or includes a random or pseudo-random number generated for the session.
6. A method according to claim 1 wherein the session-specific challenge information is generated by and the action of authenticating is carried out by the user communication device.
7. A method according to claim 1 further comprising:
 - receiving the session-specific challenge information by the user communication device from an authentication server.
8. A method according to claim 7 wherein the action of authenticating the transaction card comprises:
 - transmitting the challenge response information to the authentication server; and
 - receiving an authentication result from the authentication server.
9. A method according to claim 1 further comprising, prior to the action of transmitting the READ TAG command:
 - terminating the first NFC session; and
 - establishing, by the user communication device within a predetermined time interval after termination of the first NFC session, a second NFC session with the transaction card.
10. A user communication device comprising:
 - a communication device data processor;
 - a near field communication (NFC) interface in communication with the data processor

and configured for communication with one or more transaction cards; and
a communication device memory accessible by the data processor and containing a card
communication application with instructions to be carried out by the data processor,
the communication application being configured to

establish a first NFC session with a transaction card,
transmit, to the transaction card, an NFC data exchange format (NDEF)
WRITE TAG command including session-specific challenge
information,
transmit, to the transaction card, an NDEF READ TAG command,
receive, from the transaction card, card-specific challenge response
information, and
authenticate the transaction card.

11. A user communication device according to claim 10 wherein the card-specific challenge
response information comprises card-encrypted information and the communication
application is configured to, as part of the action to authenticate:

attempt to decrypt the card-encrypted information using at least one card-unique key
associated with the transaction card, and
responsive to a successful decryption of the card-encrypted information, establish a
positive authentication result.

12. A user communication device according to claim 10 wherein the communication
application is further configured to generate a random or pseudo-random number for
inclusion in the session-specific challenge information.

13. A user communication device according to claim 10 further comprising:
- a network communication interface in communication with the communication device data processor and configured for selective communication with an authentication server via a network,
 - wherein the communication application is further configured to
 - receive the session-specific challenge information from the authentication server.
14. A user communication device according to claim 13 wherein the communication application is further configured to, as part of the action to authenticate:
- transmit the challenge response information to the authentication server; and
 - receive an authentication result from the authentication server.
15. A user communication device according to claim 10 wherein the communication application is further configured to
- determine a time interval between the action of transmitting the READ TAG command and receiving the card-specific challenge response information, and
 - carry out the action of authenticating the transaction card only if the time interval is less than a predetermined maximum communication interval.
16. A user communication device according to claim 10 wherein the communication application is further configured to, prior to the action to transmit the READ TAG command:
- terminate the first NFC session; and
 - establish a second NFC session with the transaction card.

17. A user communication device according to claim 16 wherein the action to establish the second NFC session is taken within a predetermined time interval after the action to terminate the first NFC session.

18. A transaction card comprising:

a card microprocessor;

a near field communication (NFC) interface;

and a card memory having a card identifier and one or more applets stored therein, the one or more applets including instructions for the card microprocessor to

receive, from a user communication device via the NFC interface, an NFC data exchange format (NDEF) WRITE TAG command including challenge information,

generate a digital signature using the challenge information,

receive, from the user communication device via the NFC interface, an NDEF READ TAG command, and

transmit, to the user communication device, the digital signature.

19. A transaction card according to claim 18 wherein

the card memory has at least one card-unique encryption key stored therein, and

the digital signature is or includes a cryptogram encrypted using at least a portion of the challenge information and the at least one card-unique encryption key.

20. A transaction card according to claim 19 wherein

the card memory has at least one public key certificate stored therein and the one or

more applets include instructions for the card microprocessor to transmit the at least one public key certificate with the card identifier and the digital signature.