

**CONTINUOUS AUTHENTICATION FOR DIGITAL SERVICE BASED ON
CONTACTLESS CARD POSITIONING
CROSS-REFERENCE TO RELATED APPLICATIONS**

[0001] This application claims priority to U.S. Patent Application Serial No. 16/516,243, entitled “CONTINUOUS AUTHENTICATION FOR DIGITAL SERVICES BASED ON CONTACTLESS CARD POSITIONING” filed on July 18, 2019. The contents of the aforementioned patent application are incorporated herein by reference in their entirety.

TECHNICAL FIELD

[0002] Embodiments herein generally relate to computing platforms, and more specifically, to providing continuous authentication to a digital service when a contactless card is positioned proximate a computing device.

BACKGROUND

[0003] User authentication is typically required when accessing a service, such as a digital wallet, website, network, application, and the like. Commonly deployed authentication methods include password authentication, iris authentication, facial authentication, voice authentication, fingerprint authentication, vein authentication, predetermined gestures, etc.

[0004] For security reasons, these authentication methods provide limits on how long an authenticated user may stay logged-in to the service. However, requiring continuous re authentication by the user to avoid being logged-out of the service can cause undue user attention and effort, which can lead to a decreased user experience.

SUMMARY

[0005] Embodiments disclosed herein provide systems, methods, articles of manufacture, and computer-readable media for providing continuous authentication to a digital service based on proximity of a contactless card to a computing device. According to one example, a system may include a processor circuit and a memory storing instructions which when executed by the processor circuit, cause the processor circuit to receive, by an application executing on the processor circuit, a request to access a digital service, receive, by the application, a first authentication based on verification of a first set of encrypted data associated with a user account, request, by the application, a second authentication from a contactless card, and receive, by a card reader of a client device, a second set of encrypted data from a communications interface of the contactless card in response to the contactless card being activated, the second set of encrypted data generated based on a cryptographic algorithm and a diversified key, the diversified key stored in a memory of the contactless card, wherein the contactless card is activated by the client

device when the contactless card is positioned proximate the client device, and wherein the second set of encrypted data is associated with the user account. The system further includes instructions, which when executed by the processor circuit, cause the processor circuit to receive, by the application from a server, a second verification of the user account based on the second set of encrypted data, authorize, by the application, access to the digital service in response to the first and second verification of the user account, and continuously provide, by the application, a series of periodic status messages between the client device and the contactless card to verify whether the contactless card remains active, wherein authorization to access the digital service continues while the contactless card is active, and wherein authorization to access the digital service terminates when the contactless card is inactive.

[0006] According to another example, a method may include receiving, by an application executing on the processor circuit, a request to access a digital service, receiving, by the application, a first authentication based on verification of a first set of encrypted data associated with a user account, and requesting, by the application, a second authentication from a contactless card. The method may further include receiving, by a card reader of a client device, a second set of encrypted data from a communications interface of the contactless card in response to the contactless card being activated, the second set of encrypted data generated based on a cryptographic algorithm and a diversified key, the diversified key stored in a memory of the contactless card, wherein the contactless card is activated by the client device when the contactless card is positioned proximate the client device, and wherein the second set of encrypted data is associated with the user account. The method may further include receiving, by the application from a server, a second verification of the user account based on the second set of encrypted data, authorizing, by the application, access to the digital service in response to the first and second verification of the user account, and continuously providing, by the application, a series of periodic status messages between the client device and the contactless card to verify whether the contactless card remains active, wherein authorization to access the digital service continues while the contactless card is active, and wherein authorization to access the digital service terminates when the contactless card is inactive.

[0007] According to another example, a non-transitory computer-readable storage medium having computer-readable program code embodied therewith, the computer-readable program code executable by a processor circuit, may cause the processor circuit to receive, by an application executing on the processor circuit, a request to access a digital service receive, by the application, a first authentication based on verification of a first set of encrypted data associated with a user account, and request, by the application, a second authentication from a contactless card. The computer-readable program code executable by the processor circuit may further cause

the processor circuit to receive, by a card reader of a client device, a second set of encrypted data from a communications interface of the contactless card in response to the contactless card being activated, the second set of encrypted data generated based on a cryptographic algorithm and a diversified key, the diversified key stored in a memory of the contactless card, wherein the contactless card is activated by the client device when the contactless card is positioned proximate the client device, and wherein the second set of encrypted data is associated with the user account. The computer-readable program code executable by the processor circuit may further cause the processor circuit to receive, by the application from a server, a second verification of the user account based on the second set of encrypted data, authorize, by the application, access to the digital service in response to the first and second verification of the user account, and continuously provide, by the application, a series of periodic status messages between the client device and the contactless card to verify whether the contactless card remains active, wherein authorization to access the digital service continues while the contactless card is active, and wherein authorization to access the digital service terminates when the contactless card is inactive.

[0008] An aspect of the present disclosure provides a method, comprising: receiving, by an application executing on a processor circuit of a client device, a request to access a digital service; receiving, by the application, a first authentication based on verification of a first set of encrypted data associated with a user account; requesting, by the application based on the first authentication, a second authentication from a contactless card, wherein the contactless card is activated by a magnetic field of the client device; receiving, by a card reader of the client device, a second set of encrypted data from the contactless card in response to the contactless card being activated, wherein the second set of encrypted data is based on a cryptographic algorithm and a diversified key of the contactless card, wherein the second set of encrypted data is associated with the user account; performing, by the application, the second authentication based on the second set of encrypted data; authorizing, by the application, access to the digital service in response to the first authentication and the second authentication; transmitting, by the application at each of a plurality of time periods, a respective status message of a plurality of status messages to the contactless card to verify that the contactless card is active; receiving, by the application, a first response of a plurality of responses from the contactless card in response to a first status message of the plurality of status messages; providing, by the application based on the first response, access to the digital service without requiring re-authentication; determining, by the application, that a response to a second status message of the plurality of status messages is not received from the contactless card; and terminating, by the application, access to the digital service based on the determination that the response to the second status message is not received from the contactless card.

[0009] Another aspect of the present disclosure provides a computer-readable storage medium including instructions that when executed by a processor of a client device, cause the processor to: receive, by an application, a request to access a digital service; receive, by the application, a first authentication based on verification of a first set of encrypted data associated with a user account; request, by the application based on the first authentication, a second authentication from a contactless card, wherein the contactless card is activated by a magnetic field of the client device; receive, via a card reader of the client device, a second set of encrypted data from the contactless card in response to the contactless card being activated, wherein the second set of encrypted data is based on a cryptographic algorithm and a diversified key of the contactless card, wherein the second set of encrypted data is associated with the user account; perform, by the application, the second authentication based on the second set of encrypted data; authorize, by the application, access to the digital service in response to the first authentication and the second authentication; transmit, by the application at each of a plurality of time periods, a respective status message of a plurality of status messages to the contactless card to verify that the contactless card is active; receive, by the application, a first response of a plurality of responses from the contactless card in response to a first status message of the plurality of status messages; provide, by the application based on the first response, access to the digital service without requiring re-authentication; determine, by the application, that a response to a second status message of the plurality of status messages is not received from the contactless card; and terminate, by the application, access to the digital service based on the determination that the response to the second status message is not received from the contactless card.

[0010] Another aspect of the present disclosure provides a computing apparatus comprising: a processor; a card reader; and a memory storing instructions that, when executed by the processor, cause the processor to: receive, by an application, a request to access a digital service; receive, by the application, a first authentication based on verification of a first set of encrypted data associated with a user account; request, by the application based on the first authentication, a second authentication from a contactless card, wherein the contactless card is activated by a magnetic field of the apparatus; receive, by the card reader, a second set of encrypted data from the contactless card in response to the contactless card being activated, wherein the second set of encrypted data is based on a cryptographic algorithm and a diversified key of the contactless card, wherein the second set of encrypted data is associated with the user account; perform, by the application, the second authentication based on the second set of encrypted data; authorize, by the application, access to the digital service in response to the first authentication and the second authentication; transmit, by the application at each of a plurality of time periods, a respective status message of a plurality of status messages to the contactless card to verify that the contactless card is active; receive, by the

application, a first response of a plurality of responses from the contactless card in response to a first status message of the plurality of status messages; provide, by the application based on the first response, access to the digital service without requiring re-authentication; determine, by the application, that a response to a second status message of the plurality of status messages is not received from the contactless card; and terminate, by the application, access to the digital service based on the determination that the response to the second status message is not received from the contactless card.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG. 1 illustrates an embodiment of a system for providing continuous authentication to a digital service.

[0012] FIGs. 2-3 illustrate embodiments for providing continuous authentication to the digital service based on proximity of a contactless card to a computing device.

[0013] FIGs. 4A-4B illustrate embodiments of a contactless card.

[0014] FIG. 5 A illustrates a side view of an embodiment of a covering for a client device.

[0015] FIG. 5B illustrates an end view of an embodiment of the covering for the client device of FIG. 5A.

[0016] FIG. 6 illustrates an embodiment of a logic flow for providing continuous authentication to a digital service.

[0017] FIG. 7 illustrates an embodiment of a computing architecture.

[0018] The drawings are not necessarily to scale. The drawings are merely representations, not intended to portray specific parameters of the disclosure. The drawings are intended to depict example embodiments of the disclosure, and therefore are not be considered as limiting in scope. Certain elements in some of the FIG.s may be omitted, or illustrated not-to-scale, for illustrative clarity. Furthermore, some reference numbers may be omitted in certain drawings.

DETAILED DESCRIPTION

[0019] The present embodiments will now be described more fully hereinafter with reference to the accompanying drawings, where some embodiments are shown. The subject matter of the present disclosure may be embodied in many different forms and are not to be construed as limited to the embodiments set forth herein. These embodiments are provided so this disclosure will be thorough and complete, and will fully convey the scope of the subject matter to those skilled in the art. In the drawings, like numbers refer to like elements throughout.

[0020] Embodiments disclosed herein provide continuous authentication of a contactless card based on proximity to a client device, such as a mobile device or personal computer. In some

embodiments, continuous activation may allow the contactless card to provide authentication with a digital service so long as the contactless card is positioned proximate a card reader of the client device. For example, a series of periodic “heartbeat” or status messages may be provided between the client device and the contactless card to verify whether the contactless card remains active, wherein authorization to access the digital service continues while the contactless card is active, and terminates when the contactless card is inactive.

[0021] In some embodiments, a device or covering over the client device may be employed to receive and position the contactless card relative to the client device. In particular, the covering may include a slot or receptacle positioned proximate the card reader of the mobile device. While the contactless card is retained within the covering, the contactless card may be continuously activated by an electromagnetic field of the client device. This continuous activation in turn may allow the contactless card to provide authentication with the digital service so long as the contactless card remains within the covering. Removal of the contactless card from the covering may result in loss of the electromagnetic field, thus terminating the authentication with the digital service.

[0022] Advantageously, providing continuous authentication using “heartbeat” or status messaging improves ease of interaction with digital services by users. For example, users can be authenticated once, and stay logged-in to the digital service based on the authentication so long as the contactless card remains active. By reducing the number of times, the user must enter authentication information, security of the card data may be enhanced.

[0023] With general reference to notations and nomenclature used herein, one or more portions of the detailed description which follows may be presented in terms of program procedures executed on a computer or network of computers. These procedural descriptions and representations are used by those skilled in the art to most effectively convey the substances of their work to others skilled in the art. A procedure is here, and generally, conceived to be a self-consistent sequence of operations leading to a desired result. These operations are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical, magnetic, or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It proves convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like. It should be noted, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to those quantities.

[0024] Further, these manipulations are often referred to in terms, such as adding or comparing, which are commonly associated with mental operations performed by a human

operator. However, no such capability of a human operator is necessary, or desirable in most cases, in any of the operations described herein that form part of one or more embodiments. Rather, these operations are machine operations. Useful machines for performing operations of various embodiments include digital computers as selectively activated or configured by a computer program stored within that is written in accordance with the teachings herein, and/or include apparatus specially constructed for the required purpose or a digital computer. Various embodiments also relate to apparatus or systems for performing these operations. These apparatuses may be specially constructed for the required purpose. The required structure for a variety of these machines will be apparent from the description given.

[0025] Reference is now made to the drawings, wherein like reference numerals are used to refer to like elements throughout. In the following description, for the purpose of explanation, numerous specific details are set forth in order to provide a thorough understanding thereof. It may be evident, however, that the novel embodiments can be practiced without these specific details. In other instances, well known structures and devices are shown in block diagram form in order to facilitate a description thereof. The intention is to cover all modification, equivalents, and alternatives within the scope of the claims.

[0026] FIG. 1 depicts a schematic of an exemplary system 100, consistent with disclosed embodiments. As shown, the system 100 includes one or more contactless cards 101, one or more client devices 110, and one or more servers 120. The contactless cards 101 are representative of any type of identification and/or payment card, such as a credit card, debit card, ATM card, gift card, and the like. The contactless card 101 may include one or more chips (not depicted), such as a radio frequency identification (RFID) chip, configured to communicate with the client device 110 via NFC, the EMV standard, or other short-range protocols in wireless communication. Although NFC is used as an example communications protocol, the disclosure is equally applicable to other types of wireless communications, such as the EMV standard, Bluetooth, and/or Wi-Fi. The client device 110 is representative of any type of network-enabled computing devices, such as smartphones, tablet computers, wearable devices, laptops, portable gaming devices, and the like. The server 120 is representative of any type of computing device, such as a server, workstation, compute cluster, cloud computing platform, virtualized computing system, and the like.

[0027] As shown, a memory 102 of the contactless card may include card data 103, a counter 104, a master key 105, a diversified key 106, a unique customer identifier 107, and a data store of account numbers 108. The card data 103 generally includes account-related information, such as information used to process a payment using the contactless card 101. For example, the card data 103 may comprise an account number, an expiration date, a billing address, and a card

verification value (CVV). The account number may be any type of account number, such as a primary account number (PAN), a virtual account number, and/or a token generated based on the PAN. Other types of account numbers are contemplated, and the use of the account number or other types of card data 103 should not be considered limiting of the disclosure. The card data 103 may further include names, billing address, shipping address, and other account-related information. As described in greater detail herein, the contactless card 101 may provide the card data 103 and/or a record from the account numbers 108 to an account application 113 to provide authentication/access to a digital service 114.

[0028] As shown, a memory 111 of the client device 110 includes an instance of an operating system (OS) 112. Example operating systems 112 include the Android® OS, iOS®, Linux®, and Windows® operating systems. As shown, the OS 112 may include the account application 113, the digital service 114, one or more other applications 115, and a clipboard 116. In embodiments wherein the digital service is a banking application or website, the account application 113 may allow users to perform various account-related operations, such as viewing account balances, purchasing items, and processing payments. Initially, a user must authenticate using authentication credentials to access the account application 113. For example, the authentication credentials may include a username and password, biometric credentials, and the like. As will be described in greater detail below, to access the account application 113 and/or the digital service 114, the user must also satisfy a secondary authentication based on data exchanged between the client device 110 and the contactless card 101.

[0029] The digital service 114 may include one or more services including, but not limited to, a client device application (e.g., banking, social media, music streaming, gaming, etc.), a website, a messaging service (e.g., e-mail, text, etc.), and many others. Embodiments herein are not limited in this context. In some embodiments, the digital service 114 is associated with the account application 113. For example, the digital service 114 may be installed on the client device 110, operable with the account application 113.

[0030] As shown, the server 120 includes a data store of account data 124 and a memory 122. The account data 124 may include account-related data for one or more users and/or accounts. The account data 124 may include at least a master key 105, counter 104, a customer ID 107, an associated contactless card 101, account holder name, account billing address, one or more shipping addresses, one or more card numbers, and biographical information for each account. The memory 122 may include a management application 123 and instances of the card data 103, the counter 104, master key 105, and diversified key 106 for one or more accounts from the account data 124.

[0031] The system 100 is configured to implement key diversification to secure data, which may be referred to as a key diversification technique herein. Generally, the server 120 (or another computing device) and the contactless card 101 may be provisioned with the same master key 105 (also referred to as a master symmetric key). More specifically, each contactless card 101 is programmed with a distinct master key 105 that has a corresponding pair in the server 120. For example, when a contactless card 101 is manufactured, a unique master key 105 may be programmed into the memory 102 of the contactless card 101. Similarly, the unique master key 105 may be stored in a record of a customer associated with the contactless card 101 in the account data 124 of the server 120 (and/or stored in a different secure location). The master key 105 may be kept secret from all parties other than the contactless card 101 and server 120, thereby enhancing security of the system 100.

[0032] The master key 105 may be used in conjunction with the counter 104 to enhance security using key diversification. The counter 104 comprises values that are synchronized between the contactless card 101 and server 120. The counter 104 value may comprise a number that changes each time data is exchanged between the contactless card 101 and the server 120 (and/or the contactless card 101 and the client device 110). To enable NFC data transfer between the contactless card 101 and the client device 110, the account application 113 may communicate with the contactless card 101 when the contactless card 101 is sufficiently close to a card reader 118 of the client device 110. Card reader 118 may be configured to read from and/or communicate with contactless card 101 (e.g., via NFC, Bluetooth, RFID, etc.). Therefore, example card readers 118 may include NFC communication modules, Bluetooth communication modules, and/or RFID communication modules.

[0033] For example, a user may bring the contactless card 101 to the client device 110, thereby bringing the contactless card 101 sufficiently close to the card reader 118 of the client device 110 to enable NFC data transfer between the contactless card 101 and the card reader 118 of the client device 110. In some embodiments, the client device 110 may trigger the card reader 118 via an application programming interface (API) call. In addition and/or alternatively, the client device 110 may trigger the card reader 118 based on periodically polling the card reader 118. More generally, the client device 110 may trigger the card reader 118 to engage in communications using any feasible method. In some embodiments, the contactless card 101 may be powered/activated in response to a magnetic field of the client device 110.

[0034] After communication has been established between client device 110 and contactless card 101, the contactless card 101 may generate a message authentication code (MAC) cryptogram. In some examples, this may occur when the contactless card 101 is read by the account application 113. In particular, this may occur upon a read, such as an NFC read, of a near

field data exchange (NDEF) tag, which may be created in accordance with the NFC Data Exchange Format. For example, a reader, such as the account application 113 and/or the card reader 118, may transmit a message, such as an applet select message, with the applet ID of an NDEF producing applet. Upon confirmation of the selection, a sequence of select file messages followed by read file messages may be transmitted. For example, the sequence may include “Select Capabilities file”, “Read Capabilities file”, and “Select NDEF file”. At this point, the counter 104 value maintained by the contactless card 101 may be updated or incremented, which may be followed by “Read NDEF file.” At this point, the message may be generated which may include a header and a shared secret. Session keys may then be generated. The MAC cryptogram may be created from the message, which may include the header and the shared secret. The MAC cryptogram may then be concatenated with one or more blocks of random data, and the MAC cryptogram and a random number (RND) may be encrypted with the session key. Thereafter, the cryptogram and the header may be concatenated, and encoded as ASCII hex and returned in NDEF message format (responsive to the “Read NDEF file” message). In some examples, the MAC cryptogram may be transmitted as an NDEF tag, and in other examples the MAC cryptogram may be included with a uniform resource indicator (e.g., as a formatted string). The contactless card 101 may then transmit the MAC cryptogram to the client device 110, which may then forward the MAC cryptogram to the server 120 for verification as explained below. However, in some embodiments, the client device 110 may verify the MAC cryptogram. Embodiments herein are not limited in this context.

[0035] More generally, when preparing to send data (e.g., to the server 120 and/or the client device 110), the contactless card 101 may increment the counter 104 value. The contactless card 101 may then provide the master key 105 and counter 104 value as input to a cryptographic algorithm, which produces a diversified key 106 as output. The cryptographic algorithm may include encryption algorithms, hash-based message authentication code (F1MAC) algorithms, cipher-based message authentication code (CMAC) algorithms, and the like. Non-limiting examples of the cryptographic algorithm may include a symmetric encryption algorithm such as 3DES or AES128; a symmetric F1MAC algorithm, such as F1MAC-SF1A-256; and a symmetric CMAC algorithm such as AES-CMAC. The contactless card 101 may then encrypt the data (e.g., the customer identifier 107 and any other data) using the diversified key 106. The contactless card 101 may then transmit the encrypted data (e.g., the encrypted customer ID 109) to the account application 113 of the client device 110 (e.g., via an NFC connection, Bluetooth connection, etc.). The account application 113 of the client device 110 may then transmit the encrypted data to the server 120 via the network 130. In at least one embodiment, the contactless card 101 transmits the counter 104 value with the encrypted data. In such embodiments, the

contactless card 101 may transmit an encrypted counter 104 value, or an unencrypted counter 104 value.

[0036] Upon receiving the encrypted customer ID 109, the management application 123 of the server 120 may perform the same symmetric encryption using the counter 104 value as input to the encryption, and the master key 105 as the key for the encryption. As stated, the counter 104 value may be specified in the data received from the client device 110, or a counter 104 value maintained by the server 120 to implement key diversification for the contactless card 101. The output of the encryption may be the same diversified key value 106 that was created by the contactless card 101. The management application 123 may then decrypt the encrypted customer ID 109 received via the network 130 using the diversified key 106, which reveals the data transmitted by the contactless card 101 (e.g., at least the customer identifier 107). Doing so allows the management application 123 to verify the data transmitted by the contactless card 101 via the client device 110, e.g., by comparing the decrypted customer ID 107 to a customer ID in the account data 124 for the account.

[0037] Although the counter 104 is used as an example, other data may be used to secure communications between the contactless card 101, the client device 110, and/or the server 120. For example, the counter 104 may be replaced with a random nonce, generated each time a new diversified key 106 is needed, the full value of a counter value sent from the contactless card 101 and the server 120, a portion of a counter value sent from the contactless card 101 and the server 120, a counter independently maintained by the contactless card 101 and the server 120 but not sent between the two, a one-time -passcode exchanged between the contactless card 101 and the server 120, and a cryptographic hash of data. In some examples, one or more portions of the diversified key 106 may be used by the parties to create multiple diversified keys 106.

[0038] As shown, the server 120 may include one or more hardware security modules (F1SM) 125. For example, one or more F1SMs 125 may be configured to perform one or more cryptographic operations as disclosed herein. In some examples, one or more F1SMs 125 may be configured as special purpose security devices that are configured to perform the one or more cryptographic operations. The F1SMs 125 may be configured such that keys are never revealed outside the F1SM 125, and instead are maintained within the F1SM 125. For example, one or more F1SMs 125 may be configured to perform at least one of key derivations, decryption, and MAC operations. The one or more HSMs 125 may be contained within, or may be in data communication with, server 120.

[0039] As stated, the key diversification technique may be used to perform secure operations using the contactless card 101. For example, once the management application 123 verifies the encrypted customer ID 109 using key diversification, the management application 123 may

transmit an account number, expiration date, and/or CVV associated with the account to the account application 113 of the client device 110. The management application 123 may further include other information (e.g., first name, last name, shipping address, billing address, other account information, etc.). The account number may be a PAN, a virtual account number, and/or a token generated based on the PAN. The account application 113 may decrypt the received data (if encrypted) and provide the account number, expiration date, billing address, and/or CVV to an API of the digital service 114.

[0040] In another embodiment, the card data 103 is read directly from the contactless card 101, which may be useful if the client device 110 does not have a connection to the server 120. For example, the account application 113 and/or the digital service 114 may output an indication to bring the contactless card 101 proximate to the client device 110. In one embodiment, once the contactless card 101 is brought near the client device 110, the contactless card 101 transmits the card data 103 to the client device 110. In another embodiment, once the contactless card 101 is brought near the client device 110, the account application 113 may instruct the contactless card 101 to transmit the card data 103 to the client device 110. In one example, the contactless card 101 transmits the card data 103 (including one or more of the account number, expiration date, CVV value, and the account holder's name) to the client device 110 in an NDEF file (e.g. via NFC, Bluetooth, and/or RFID). In another example, the contactless card 101 transmits the card data 103 using the EMV protocol. In examples where the EMV protocol is used, the card data 103 transmitted using the EMV protocol includes the account number, expiration date, and the account holder's name. The contactless card 101 may then transmit the card data 103 to the account application 113 using the EMV protocol. In examples where the EMV protocol is used, the account application 113 may receive the CVV value from the contactless card 101 (e.g., via the NFC read to receive the CVV in an NDEF file) and/or from the management application 123 of the server 120. However, in some embodiments, the EMV protocol may be used to transmit the CVV value directly from the contactless card 101. The account application 113 may then provide the card data 103 (e.g., the account number, expiration date, and/or CVV) to the API of the digital service 114.

[0041] Regardless of the technique used to provide card data 103 and/or the account number 108 to the digital service 114, the account application 113 and/or the OS 112 may manage the data provided to the digital service 114. For example, the card data 103 and/or the account number 108 may be maintained at the digital service 114 so long as the contactless card 101 is active, e.g., when positioned adjacent the client device 110. Access/authentication to the digital service 114 is therefore maintained. As another example, the card data 103 and/or the account

number 108 may be maintained at the digital service 114 after the card data 103 and/or the account number 108 has been used to make a purchase.

[0042] Furthermore, the account application 113 and/or the digital service 114 may copy an account number to the clipboard 116 of the OS. The clipboard 116 stores data that can be copied and/or pasted within the OS 112. For example, the clipboard 116 may store data locally for pasting into fields of the client device 110, and a user may input/paste the data stored in the clipboard 116 using a command and/or gesture available within the OS 112. For example, copying the account number to the clipboard 116 allows the user to paste the account number to the corresponding form field using a command and/or gesture available within the OS 112. Further still, the digital service 114 may output a notification which specifies the expiration date and the CVV while the account number is copied to the clipboard 116. Doing so allows the user to manually enter the expiration date and CVV to the corresponding form fields while the notification remains in view. In some embodiments, the account application 113 and/or the digital service 114 may also copy the expiration date, billing address, and/or the CVV to the clipboard 116, allowing the expiration date, billing address, and/or the CVV to be pasted to the corresponding form fields.

[0043] FIG. 2 is a schematic 200 depicting an example embodiment for providing continuous authentication to the digital service 214 based on proximity of the contactless card 201 to a client device, such as a mobile device 210. Although non-limiting, the mobile device 210 may be a smart phone or tablet computer. In other embodiments, the client device may be a laptop, desktop computer, or transaction kiosk. For example, the client device may be laptop computer with an internal or external reader for communicating with the contactless card 201. Embodiments herein are not limited in this context.

[0044] In this non-limiting example, the digital service 214 may be a banking application stored within memory of the mobile device 210. The user may bring the contactless card 201 in close physical proximity to the mobile device 210. One or more chips and/or chip modules (not depicted) of the contactless card 201 may then be activated with power obtained from an electromagnetic field 227 of the mobile device 210. More specifically, the contactless card 201 may be operable to receive the electromagnetic field 227 and convert it to a suitable electrical voltage to power the other circuit components of the contactless card 201. For example, the electromagnetic field 227 may be converted to power a RFID chip, which is configured to communicate with the mobile device 210 via, e.g., NFC, the EMV standard, or other short-range protocols in wireless communication.

[0045] When the user initially attempts to log in to his/her account, log-in credentials received by an API 221 of the digital service 214 are delivered to a server 220 as a first set of

encrypted data 216. The first set of encrypted data 216 may be associated with a user account 228, which in turn is associated with a data store of account data 224.

[0046] The server 220 may then compare, for example by the management application 123 (FIG. 1), the first set of encrypted data 216 to a customer identifier in the account data 224 for the user account 228, validating or invalidating the data accordingly. In the event of a positive match, a first authentication/verification 230 is then provided to the mobile device 210.

[0047] The digital service 214 may then request a second authentication 232 from the contactless card 201. In some embodiments, the contactless card 201 may have been previously activated based on the electromagnetic field 227 received from the client device 201. In other embodiments, the contactless card 201 may be inactive, in which case the contactless card 201 needs to be activated to complete the request for the second authentication 232. For example, the user may not have previously placed the contactless card 201 proximate the mobile device 210, or the position of the contactless card 201 relative to a card reader 218 of the mobile 210 results in an inadequate communication signal strength emanating from the contactless card 201. In either case, the mobile device 210 may display a prompt to the user via a graphical user interface (GUI). For example, a notification may instruct the user to place the contactless card 201 in physical contact with a back surface of the mobile device 210. In other embodiments, the notification may provide feedback regarding the strength of the electromagnetic field 227 and/or a signal strength of the contactless card 201.

[0048] Once the contactless card 201 is active, the card reader 218 of the mobile device 201 may receive a second set of encrypted data 234 from a communications interface 236 of the contactless card 201. In some embodiments, the second set of encrypted data 234 may be generated based on a cryptographic algorithm and a diversified key stored in memory of the contactless card 201. The second set of encrypted data 234 is associated with the user account 228.

[0049] The server 220 may then receive the second set of encrypted data 234 from the mobile device 210, comparing it to the customer identifier in the account data 224 for the user account 228, and validating or invalidating the data accordingly. In the event of a positive match, a second authentication/verification 238 is then provided to the mobile device 210. Access to the digital service 214 may then be provided, e.g., by an account application 213 in response to the first verification 230 and the second verification 238 of the user account 228.

[0050] Once the user has successfully logged in to the digital service 214, authorization to access the digital service 214 continues while the contactless card 201 is active. To accomplish this, the account application 213 may cause a series of periodic heartbeat or status messages 250 to be provided between the mobile device 210 and the contactless card 201 to verify whether the

contactless card 201 is still active. In some embodiments, the status messages 250 may be a series of requests or “pings” to the contactless card 201, which result in a communication response via an antenna 229 of the contactless card 201. For example, the status messages 250 may trigger the card reader 218 of the contactless card 201 via an application programming interface (API) call. However, the status messages 250 may trigger the card reader to engage in communications using any feasible method. In the event the contactless card 201 is determined to be inactive, e.g., in the case no communication response is received by the contactless card 201, authorization to access the digital service 214 may be terminated.

[0051] Although non-limiting, the status messages 250 can be sent unencrypted or encrypted, signed, or otherwise secured. In some embodiments, the status messages 250 may include one or more verification messages, which include, for example, reporting on the active/inactive status of the contactless card 201. Furthermore, the status messages 250 may be related to the first verification 230 and/or the second verification 238.

[0052] In some embodiments, the status messages 250 can include sending any kind of command or query, transmitted securely or transmitted in the open, receiving a response from the contactless card 201, and then evaluating the response to determine if the response is within a range of parameters expected. In yet other embodiments, the mobile device 210 may include a timer 252 set to periodically transmit the status messages 250. Access to the digital service 214 may continue until the account application 213 determines the signal strength of the contactless card 201 is below a predetermined threshold value, which may occur, for example, if the contactless card 201 is moved away from the mobile device 210 or the mobile device 210 enters a sleep mode. In some embodiments, the account application 213 may prevent the mobile device 210 from entering the sleep mode when the contactless card 201 is active.

[0053] FIG. 3 is a schematic 300 depicting an example embodiment for providing continuous authentication to a digital service 314 based on proximity of a contactless card 301 to a mobile device 310. The schematic 300 may be similar to the schematic 200 described above. As such, only certain aspects of the schematic 300 will hereinafter be described for the sake of brevity.

[0054] As shown, the schematic 300 may include a second client device 311, such as a personal computer. In this non-limiting example, the digital service 314 may be a banking website operating/displayed on the second client device 311. An account application 313 may be located on the second client device 311. In other embodiments, the account application 313 may be part of the mobile device 310. In yet other embodiments, the account application 313 may be split between the mobile device 310 and the second client device 311.

[0055] When the user initially attempts to log in to his/her account, log-in credentials received by the digital service 314 are delivered to a server 320 as a first set of encrypted data 316, which may be associated with a user account 328 of the user. The server 320 may then compare, for example by a management application, the first set of encrypted data 316 to a customer identifier in an account data 324 for the user account 328, validating or invalidating the data accordingly. In the event of a positive match, a first authentication/verification 330 is then provided from the server 320 to the second client device 311.

[0056] The digital service 314 may then request the second authentication 332 from the contactless card 301. In some embodiments, the second authentication 332 request may be delivered directly to the mobile device 310, or may be sent to the server 320 for subsequent delivery to the mobile device 310. The contactless card 301 may have been previously activated based on a magnetic field 327 received from the client device 301. In other embodiments, the contactless card 301 may be inactive, in which case the contactless card 301 needs to be activated to complete the request for the second authentication 332.

[0057] Once the contactless card 301 is active, the card reader 318 of the mobile device 301 may receive a second set of encrypted data 334 from the communications interface 336 of the contactless card 301. In some embodiments, the second set of encrypted data 334 may be generated based on a cryptographic algorithm and a diversified key stored in memory of the contactless card 301. The second set of encrypted data 334 is associated with the user account 328.

[0058] The server 320 may then receive the second set of encrypted data 334 from the mobile device 310, comparing it to the customer identifier in the account data 324 for the user account 328, and validating or invalidating the data accordingly. In the event of a positive match, the second authentication/verification 338 is then provided to the second client device 311. Access to the digital service 314 may then be provided, e.g., by the account application 313 in response to the first verification 330 and the second verification 338 of the user account 328.

[0059] Once the user has successfully logged in to the digital service 314, authorization to access the digital service 314 may continue while the contactless card 301 is active. To accomplish this, the account application 313 may cause a series of periodic heartbeat or status messages 350 to be provided between the mobile device 310 and the contactless card 301 to verify whether the contactless card 301 is still active. In some embodiments, the status messages 350, or an output of the status messages (e.g., contactless card active/inactive), may be delivered to the server 320 and then to the second client device 311. In some embodiments, the status messages 350 may be communicated directly to the second client device 311. In the event the

contactless card 301 is determined to be inactive, authorization to access the digital service 314 may be terminated.

[0060] FIG. 4A illustrates an exemplary contactless card 401, which may be a payment card, such as a credit card, debit card, and/or a gift card. As shown, the contactless card 401 may be issued by a service provider 405 displayed on the front or back of the card 401. In some examples, the contactless card 401 is not related to a payment card, and may comprise, without limitation, an identification card. In some examples, the payment card may comprise a dual interface contactless payment card. The contactless card 401 may comprise a substrate 410, which may include a single layer or one or more laminated layers composed of plastics, metals, and other materials. Exemplary substrate materials include polyvinyl chloride, polyvinyl chloride acetate, acrylonitrile butadiene styrene, polycarbonate, polyesters, anodized titanium, palladium, gold, carbon, paper, and biodegradable materials. In some examples, the contactless card 401 may have physical characteristics compliant with the ID-1 format of the ISO/IEC 7810 standard, and the contactless card may otherwise be compliant with the ISO IEC 14443 standard. However, it is understood that the contactless card 401 according to the present disclosure may have different characteristics, and the present disclosure does not require a contactless card to be implemented in a payment card.

[0061] The contactless card 401 may also include identification information 415 displayed on the front and/or back of the card, and a contact pad 420. The contact pad 420 may be configured to establish contact with another communication device, such as the client device(s) 110 (FIG. 1), a user device, smart phone, laptop, desktop, or tablet computer. The contactless card 401 may also include processing circuitry, antenna and other components not shown in FIG. 4A. These components may be located behind the contact pad 420 or elsewhere on the substrate 410. The contactless card 401 may also include a magnetic strip or tape, which may be located on the back of the card (not shown in FIG. 4A).

[0062] As illustrated in FIG. 4B, the contact pad 420 of the contactless card 401 may include processing circuitry 425 for storing and processing information, including a microprocessor 430 and the memory 102. It is understood that the processing circuitry 425 may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamperproofing hardware, as necessary to perform the functions described herein.

[0063] The memory 102 may be a read-only memory, write-once read-multiple memory or read/write memory, e.g., RAM, ROM, and EEPROM, and the contactless card 401 may include one or more of these memories. A read-only memory may be factory programmable as read-only or one-time programmable. One-time programmability provides the opportunity to write once

then read many times. A write once/read-multiple memory may be programmed at a point in time after the memory chip has left the factory. Once the memory 102 is programmed, it may not be rewritten, but it may be read many times. A read/write memory may be programmed and re-programmed many times after leaving the factory. A read/write memory may also be read many times after leaving the factory.

[0064] The memory 102 may be configured to store one or more applets 440, one or more counters 104, a customer identifier 107, and virtual account numbers 108. The one or more applets 440 may include one or more software applications configured to execute on one or more contactless cards, such as a Java® Card applet. However, it is understood that applets 440 are not limited to Java Card applets, and instead may be any software application operable on contactless cards or other devices having limited memory. The one or more counters 104 may comprise a numeric counter sufficient to store an integer. The customer identifier 107 may comprise a unique alphanumeric identifier assigned to a user of the contactless card 401, and the identifier may distinguish the user of the contactless card from other contactless card users. In some examples, the customer identifier 107 may identify both a customer and an account assigned to that customer and may further identify the contactless card 401, which is associated with the customer's account. In some embodiments, the account numbers 108 may include thousands of one-time use virtual account numbers associated with the contactless card 401.

[0065] The processor and memory elements of the foregoing exemplary embodiments are described with reference to the contact pad, but the present disclosure is not limited thereto. It is understood that these elements may be implemented outside of the pad 420 or entirely separate from it, or as further elements in addition to processor 430 and memory 402 elements located within the contact pad 420.

[0066] In some examples, the contactless card 401 may include one or more antennas (not shown). Generally, using the antennas, processing circuitry 425, and/or the memory 102, the contactless card 401 may provide a communications interface to communicate via NFC, Bluetooth, and/or Wi-Fi communications. In some embodiments, the antennas may be placed within the contactless card 401 and around the processing circuitry 425 of the contact pad 420. For example, the antennas may be integral with the processing circuitry 425 and the one or more antennas may be used with an external booster coil. As another example, antennas may be external to the contact pad 420 and the processing circuitry 425. As stated above, the antennas may communicate responses to the status messages to indicate whether the contactless card 401 is active. In the case no communication response is received from the antennas, authorization to access one or more digital services may be terminated.

[0067] As explained above, contactless cards 401 may be built on a software platform operable on smart cards or other devices having limited memory, such as JavaCard, and one or more applications or applets may be securely executed. Applets 440 may be added to contactless cards to provide a one-time password (OTP) for multifactor authentication (MFA) in various mobile application-based use cases. Applets 440 may be configured to respond to one or more requests, such as near field data exchange requests, from a reader, such as a mobile NFC reader (e.g., of the client device 110), and produce an NDEF message that comprises a cryptographically secure OTP encoded as an NDEF text tag.

[0068] One example of an NDEF OTP is an NDEF short -record layout (SR=1). In such an example, one or more applets 440 may be configured to encode the OTP as an NDEF type 4 well known type text tag. In some examples, NDEF messages may include one or more records. The applets 440 may be configured to add one or more static tag records in addition to the OTP record.

[0069] In some examples, the one or more applets 440 may be configured to emulate an RFID tag. The RFID tag may include one or more polymorphic tags. In some examples, each time the tag is read, different cryptographic data is presented that may indicate the authenticity of the contactless card. Based on the one or more applications, an NFC read of the tag may be processed, the data may be transmitted to a server, such as the server 120 (FIG. 1), and the data may be validated at the server.

[0070] In some examples, the contactless card 401 and server 120 may include certain data such that the contactless card 401 may be properly identified. The contactless card 401 may include one or more unique identifiers, wherein each time a read operation takes place, the counter 104 may be configured to increment based upon recognition of the one or more unique identifiers. In some examples, each time data from the contactless card 401 is read (e.g., by a client device 110), the counter 104 is transmitted to the server for validation and determines whether the counter values 104 are equal (e.g., as part of the validation).

[0071] In some embodiments, during the creation process of the contactless card 401, two cryptographic keys may be assigned uniquely per card. The cryptographic keys may comprise symmetric keys which may be used in both encryption and decryption of data. Triple DES (3DES) algorithm may be used by EMV and it is implemented by hardware in the contactless card 101. By using the key diversification process, one or more keys may be derived from a master key based upon uniquely identifiable information for each entity that requires a key.

[0072] In some examples, to overcome deficiencies of 3DES algorithms, which may be susceptible to vulnerabilities, a session key may be derived (such as a unique key per session) but rather than using the master key, the unique card-derived keys and the counter may be used as

diversification data. For example, each time the contactless card 401 is used in operation, a different key may be used for creating the message authentication code (MAC) and for performing the encryption. This results in a triple layer of cryptography. The session keys may be generated by the one or more applets and derived by using the application transaction counter with one or more algorithms (as defined in EMV 4.3 Book 2 A1.3.1 Common Session Key Derivation).

[0073] Further, the increment for the contactless card 401 may be unique, and assigned either by personalization, or algorithmically assigned by some identifying information. For example, odd numbered cards may increment by 2 and even numbered cards may increment by 5. In some examples, the increment may also vary in sequential reads, such that one card may increment in sequence by 1, 3, 5, 2, 2, ... repeating. The specific sequence or algorithmic sequence may be defined at personalization time, or from one or more processes derived from unique identifiers. This can make it harder for a replay attacker to generalize from a small number of card instances.

[0074] The authentication message may be delivered as the content of a text NDEF record in hexadecimal ASCII format. In another example, the NDEF record may be encoded in hexadecimal format.

[0075] FIGs. 5A-5B illustrate a non-limiting embodiment of a covering 560 over the client device 510, such as a mobile device. The covering 560 may be a mobile device case that wraps around the client device 510. In some embodiments, the covering 560 may include an opening to permit user interaction with a screen 562 of the client device 510. As shown, the covering 560 may include a slot or receptacle 566 through an end wall 568 of the covering 560, wherein the receptacle 566 is operable to receive the contactless card 501 therein. Once retained within the receptacle 566, the contactless card 501 may be pre-positioned to enable communication with the card reader (not shown) of the client device 510. It will be appreciated that the covering 560, including the size and position of the receptacle 566, may be altered depending on one or more characteristics of the client device 501 and/or the contactless card 501. As further shown, the receptacle 566 and the contactless card 501 may be disposed along a back side 570 of the client device 510. In some embodiments, the covering 560 may be transparent or opaque. Embodiments herein are not limited in this context.

[0076] FIG. 6 illustrates an embodiment of a logic flow 600 for providing continuous authentication to a digital service. At block 601, the logic flow 600 may include receiving, by an application executing on the processor circuit, a request to access a digital service. In some embodiments, the digital service may include one or more services including, but not limited to, a client device application (e.g., banking, social media, music streaming, gaming, etc.), a website,

or a messaging service (e.g., e-mail, text, etc.). At block 603, the logic flow 600 may include receiving, by the application, a first authentication based on verification of a first set of encrypted data associated with a user account. In some embodiments, the first set of encrypted data is generated based on log-in credentials supplied by the user to the digital service. At block 605, the logic flow 600 may include requesting, by the application, a second authentication from a contactless card.

[0077] At block 607, the logic flow 600 may include receiving, by a card reader of a client device, a second set of encrypted data from a communications interface of the contactless card in response to the contactless card being activated, the second set of encrypted data generated based on a cryptographic algorithm and a diversified key, the diversified key stored in a memory of the contactless card, wherein the contactless card is activated by the client device when the contactless card is positioned proximate the client device, and wherein the second set of encrypted data is associated with the user account.

[0078] At block 609, the logic flow 600 may include receiving, by the application from a server, a second verification of the user account based on the second set of encrypted data. At block 611, the logic flow may include authorizing, by the application, access to the digital service in response to the first and second verification of the user account. At block 613, the logic flow may include continuously providing, by the application, a series of periodic status messages between the client device and the contactless card to verify whether the contactless card remains active, wherein authorization to access the digital service continues while the contactless card is active, and wherein authorization to access the digital service terminates when the contactless card is inactive.

[0079] In some examples, the contactless cards described herein may be placed atop a device, such as one or more computer kiosks or terminals, to verify identity so as to receive a transactional item responsive to a purchase, such as a coffee. By using the contactless cards, a secure method of proving identity in a loyalty program may be established. Securely proving the identity, for example, to obtain a reward, coupon, offer, or the like or receipt of a benefit is established in a manner that is different than merely scanning a bar card. For example, an encrypted transaction may occur between the contactless cards and the device, which may configure to process one or more tap gestures. As explained above, the one or more applications may be configured to validate identity of the user. In some examples, data for example, bonus points, loyalty points, reward points, healthcare information, etc., may be written back to the contactless card.

[0080] In some embodiments, an example authentication communication protocol may mimic an offline dynamic data authentication protocol of the EMV standard that is commonly

performed between a transaction card and a point-of-sale device, with some modifications. For example, because the example authentication protocol is not used to complete a payment transaction with a card issuer/payment processor per se, some data values are not needed, and authentication may be performed without involving real-time online connectivity to the card issuer/payment processor. As is known in the art, point of sale (POS) systems submit transactions including a transaction value to a card issuer. Whether the issuer approves or denies the transaction may be based on if the card issuer recognizes the transaction value. Meanwhile, in certain embodiments of the present disclosure, transactions originating from a client device lack the transaction value associated with the POS systems. Therefore, in some embodiments, a dummy transaction value (i.e., a value recognizable to the card issuer and sufficient to allow activation to occur) may be passed as part of the example authentication communication protocol. POS based transactions may also decline transactions based on the number of transaction attempts (e.g., transaction counter). A number of attempts beyond a buffer value may result in a soft decline; the soft decline requiring further verification before accepting the transaction. In some implementations, a buffer value for the transaction counter may be modified to avoid declining legitimate transactions.

[0081] In some examples, the contactless card contactless cards can selectively communicate information depending upon the recipient device. Once brought into proximity, the contactless cards can recognize the device to which the contactless card is directed, and based on this recognition, the contactless card can provide appropriate data for that device. This advantageously allows the contactless card to transmit only the information required to complete the instant action or transaction, such as a payment or card authentication. By limiting the transmission of data and avoiding the transmission of unnecessary data, both efficiency and data security can be improved. The recognition and selective communication of information can be applied to various scenarios, including card activation, balance transfers, account access attempts, commercial transactions, and step-up fraud reduction.

[0082] As another example, continuous authentication can be directed to a POS device, including without limitation a kiosk, a checkout register, a payment station, or other terminal. The contactless cards can recognize the POS device and transmit only the information necessary for the action or transaction. For example, upon recognition of a POS device used to complete a commercial transaction, the contactless cards can communicate payment information necessary to complete the transaction under the EMV standard.

[0083] In some examples, the POS devices participating in the transaction can require or specify additional information, e.g., device-specific information, location-specific information, and transaction-specific information, that is to be provided by the contactless card. For example,

once the POS device receives a data communication from the contactless card, the POS device can recognize the contactless card and request the additional information necessary to complete an action or transaction.

[0084] In some examples the POS device can be affiliated with an authorized merchant or other entity familiar with certain contactless cards or accustomed to performing certain contactless card transactions. However, it is understood such an affiliation is not required for the performance of the described methods.

[0085] In some examples, such as a shopping store, grocery store, convenience store, or the like, the contactless cards may be placed against or near a client device without having to open an application, to indicate a desire or intent to utilize one or more of reward points, loyalty points, coupons, offers, or the like to cover one or more purchases. Thus, an intention behind the purchase is provided.

[0086] FIG. 7 illustrates an embodiment of an exemplary computing architecture 800 comprising a computing system 802 that may be suitable for implementing various embodiments as previously described. In various embodiments, the computing architecture 800 may include or be implemented as part of an electronic device. In some embodiments, the computing architecture 800 may be representative, for example, of a system 100 (FIG. 1) that implements one or more components of the system. In some embodiments, computing system 802 may be representative, for example, of the client devices 110 and server 120 of the system 100. Embodiments herein are not limited in this context. More generally, the computing architecture 800 is configured to implement all logic, applications, systems, methods, apparatuses, and functionality described herein with reference to FIGs. 1-6.

[0087] As used in this application, the terms “system” and “component” and “module” are intended to refer to a computer-related entity, either hardware, a combination of hardware and software, software, or software in execution, examples of which are provided by the exemplary computing architecture 800. For example, a component can be, but is not limited to being, a process running on a computer processor, a computer processor, a hard disk drive, multiple storage drives (of optical and/or magnetic storage medium), an object, an executable, a thread of execution, a program, and/or a computer. By way of illustration, both an application running on a server and the server can be a component. One or more components can reside within a process and/or thread of execution, and a component can be localized on one computer and/or distributed between two or more computers. Further, components may be communicatively coupled to each other by various types of communications media to coordinate operations. The coordination may involve the uni-directional or bi-directional exchange of information. For instance, the components may communicate information in the form of signals communicated over the

communications media. The information can be implemented as signals allocated to various signal lines. In such allocations, each message is a signal. Further embodiments, however, may alternatively employ data messages. Such data messages may be sent across various connections. Exemplary connections include parallel interfaces, serial interfaces, and bus interfaces.

[0088] The computing system 802 includes various common computing elements, such as one or more processors, multi-core processors, co-processors, memory units, chipsets, controllers, peripherals, interfaces, oscillators, timing devices, video cards, audio cards, multimedia input/output (I/O) components, power supplies, and so forth. The embodiments, however, are not limited to implementation by the computing system 802.

[0089] As shown in FIG. 7, the computing system 802 comprises a processor 804, a system memory 806 and a system bus 808. The processor 804 can be any of various commercially available computer processors, including without limitation an AMD® Athlon®, Duron® and Opteron® processors; ARM® application, embedded and secure processors; IBM® and Motorola® DragonBall® and PowerPC® processors; IBM and Sony® Cell processors; Intel® Celeron®, Core®, Core (2) Duo®, Itanium®, Pentium®, Xeon®, and XScale® processors; and similar processors. Dual microprocessors, multi-core processors, and other multi processor architectures may also be employed as the processor 804.

[0090] The system bus 808 provides an interface for system components including, but not limited to, the system memory 806 to the processor 804. The system bus 808 can be any of several types of bus structure that may further interconnect to a memory bus (with or without a memory controller), a peripheral bus, and a local bus using any of a variety of commercially available bus architectures. Interface adapters may connect to the system bus 808 via a slot architecture. Example slot architectures may include without limitation Accelerated Graphics Port (AGP), Card Bus, (Extended) Industry Standard Architecture ((E)ISA), Micro Channel Architecture (MCA), NuBus, Peripheral Component Interconnect (Extended) (PCI(X)), PCI Express, Personal Computer Memory Card International Association (PCMCIA), and the like.

[0091] The system memory 806 may include various types of computer-readable storage media in the form of one or more higher speed memory units, such as read-only memory (ROM), random-access memory (RAM), dynamic RAM (DRAM), Double-Data-Rate DRAM (DDRAM), synchronous DRAM (SDRAM), static RAM (SRAM), programmable ROM (PROM), erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM), flash memory (e.g., one or more flash arrays), polymer memory such as ferroelectric polymer memory, ovonic memory, phase change or ferroelectric memory, silicon-oxide-nitride-oxide-silicon (SONOS) memory, magnetic or optical cards, an array of devices such as Redundant Array of Independent Disks (RAID) drives, solid state memory devices (e.g., USB memory, solid state

drives (SSD) and any other type of storage media suitable for storing information. In the illustrated embodiment shown in FIG. 8, the system memory 806 can include non-volatile memory 810 and/or volatile memory 812. A basic input/output system (BIOS) can be stored in the non-volatile memory 810.

[0092] The computing system 802 may include various types of computer-readable storage media in the form of one or more lower speed memory units, including an internal (or external) hard disk drive (HDD) 814, a magnetic floppy disk drive (FDD) 816 to read from or write to a removable magnetic disk 818, and an optical disk drive 820 to read from or write to a removable optical disk 822 (e.g., a CD-ROM or DVD). The HDD 814, FDD 816 and optical disk drive 820 can be connected to the system bus 808 by a HDD interface 824, an FDD interface 826 and an optical drive interface 828, respectively. The HDD interface 824 for external drive implementations can include at least one or both of Universal Serial Bus (USB) and IEEE 1394 interface technologies. The computing system 802 is generally configured to implement all logic, systems, methods, apparatuses, and functionality described herein with reference to FIGs. 1-6.

[0093] The drives and associated computer-readable media provide volatile and/or nonvolatile storage of data, data structures, computer-executable instructions, and so forth. For example, a number of program modules can be stored in the drives and memory units 810, 812, including an operating system 830, one or more application programs 832, other program modules 834, and program data 836. In one embodiment, the one or more application programs 832, other program modules 834, and program data 836 can include, for example, the various applications and/or components of the system 100, e.g., the operating system 112, account application 113, digital service 114, other applications 115, clipboard 116, and the management application 123.

[0094] A user can enter commands and information into the computing system 802 through one or more wire/wireless input devices, for example, a keyboard 838 and a pointing device, such as a mouse 840. Other input devices may include microphones, infra-red (IR) remote controls, radio-frequency (RF) remote controls, game pads, stylus pens, card readers, dongles, finger print readers, gloves, graphics tablets, joysticks, keyboards, retina readers, touch screens (e.g., capacitive, resistive, etc.), trackballs, trackpads, sensors, styluses, and the like. These and other input devices are often connected to the processor 804 through an input device interface 842 that is coupled to the system bus 808, but can be connected by other interfaces such as a parallel port, IEEE 1394 serial port, a game port, a USB port, an IR interface, and so forth.

[0095] A monitor 844 or other type of display device is also connected to the system bus 808 via an interface, such as a video adaptor 846. The monitor 844 may be internal or external to

the computing system 802. In addition to the monitor 844, a computer typically includes other peripheral output devices, such as speakers, printers, and so forth.

[0096] The computing system 802 may operate in a networked environment using logical connections via wire and/or wireless communications to one or more remote computers, such as a remote computer 848. The remote computer 848 can be a workstation, a server computer, a router, a personal computer, portable computer, microprocessor-based entertainment appliance, a peer device or other common network node, and typically includes many or all of the elements described relative to the computing system 802, although, for purposes of brevity, only a memory/storage device 850 is illustrated. The logical connections depicted include wire/wireless connectivity to a local area network (LAN) 852 and/or larger networks, for example, a wide area network (WAN) 854. Such LAN and WAN networking environments are commonplace in offices and companies, and facilitate enterprise-wide computer networks, such as intranets, all of which may connect to a global communications network, for example, the Internet. In embodiments, the network 130 of FIG. 1 is one or more of the LAN 852 and the WAN 854.

[0097] When used in a LAN networking environment, the computing system 802 is connected to the LAN 852 through a wire and/or wireless communication network interface or adaptor 856. The adaptor 856 can facilitate wire and/or wireless communications to the LAN 852, which may also include a wireless access point disposed thereon for communicating with the wireless functionality of the adaptor 856.

[0098] When used in a WAN networking environment, the computing system 802 can include a modem 858, or is connected to a communications server on the WAN 854 or has other means for establishing communications over the WAN 854, such as by way of the Internet. The modem 858, which can be internal or external and a wire and/or wireless device, connects to the system bus 808 via the input device interface 842. In a networked environment, program modules depicted relative to the computing system 802, or portions thereof, can be stored in the remote memory/storage device 850. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers can be used.

[0099] The computing system 802 is operable to communicate with wired and wireless devices or entities using the IEEE 802 family of standards, such as wireless devices operatively disposed in wireless communication (e.g., IEEE 802.16 over-the-air modulation techniques). This includes at least Wi-Fi (or Wireless Fidelity), WiMax, and Bluetooth™ wireless technologies, among others. Thus, the communication can be a predefined structure as with a conventional network or simply an ad hoc communication between at least two devices. Wi-Fi networks use radio technologies called IEEE 802.11x (a, b, g, n, etc.) to provide secure, reliable, fast wireless

connectivity. A Wi-Fi network can be used to connect computers to each other, to the Internet, and to wire networks (which use IEEE 802.3-related media and functions).

[0100] Various embodiments may be implemented using hardware elements, software elements, or a combination of both. Examples of hardware elements may include processors, microprocessors, circuits, circuit elements (e.g., transistors, resistors, capacitors, inductors, and so forth), integrated circuits, application specific integrated circuits (ASIC), programmable logic devices (PLD), digital signal processors (DSP), field programmable gate array (FPGA), logic gates, registers, semiconductor device, chips, microchips, chip sets, and so forth. Examples of software may include software components, programs, applications, computer programs, application programs, system programs, machine programs, operating system software, middleware, firmware, software modules, routines, subroutines, functions, methods, procedures, software interfaces, APIs, instruction sets, computing code, computer code, code segments, computer code segments, words, values, symbols, or any combination thereof. Determining whether an embodiment is implemented using hardware elements and/or software elements may vary in accordance with any number of factors, such as desired computational rate, power levels, heat tolerances, processing cycle budget, input data rates, output data rates, memory resources, data bus speeds and other design or performance constraints.

[0101] One or more aspects of at least one embodiment may be implemented by representative instructions stored on a machine -readable medium which represents various logic within the processor, which when read by a machine causes the machine to fabricate logic to perform the techniques described herein. Such representations, known as “IP cores” may be stored on a tangible, machine readable medium and supplied to various customers or manufacturing facilities to load into the fabrication machines that make the logic or processor. Some embodiments may be implemented, for example, using a machine-readable medium or article which may store an instruction or a set of instructions that, if executed by a machine, may cause the machine to perform a method and/or operation in accordance with the embodiments. Such a machine may include, for example, any suitable processing platform, computing platform, computing device, processing device, computing system, processing system, computer, processor, or the like, and may be implemented using any suitable combination of hardware and/or software. The machine-readable medium or article may include, for example, any suitable type of memory unit, memory device, memory article, memory medium, storage device, storage article, storage medium and/or storage unit, for example, memory, removable or non removable media, erasable or non-erasable media, writeable or re-writeable media, digital or analog media, hard disk, floppy disk, Compact Disk Read Only Memory (CD-ROM), Compact Disk Recordable (CD-R), Compact Disk Rewriteable (CD-RW), optical disk, magnetic media, magneto-optical media,

removable memory cards or disks, various types of Digital Versatile Disk (DVD), a tape, a cassette, or the like. The instructions may include any suitable type of code, such as source code, compiled code, interpreted code, executable code, static code, dynamic code, encrypted code, and the like, implemented using any suitable high-level, low-level, object-oriented, visual, compiled and/or interpreted programming language.

[0102] The foregoing description of example embodiments has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the present disclosure to the precise forms disclosed. Many modifications and variations are possible in light of this disclosure. It is intended that the scope of the present disclosure be limited not by this detailed description, but rather by the claims appended hereto. Future filed applications claiming priority to this application may claim the disclosed subject matter in a different manner, and may generally include any set of one or more limitations as variously disclosed or otherwise demonstrated herein.

CLAIMS

1. A method, comprising:

receiving, by an application executing on a processor circuit of a client device, a request to access a digital service;

receiving, by the application, a first authentication based on verification of a first set of encrypted data associated with a user account;

requesting, by the application based on the first authentication, a second authentication from a contactless card, wherein the contactless card is activated by a magnetic field of the client device;

receiving, by a card reader of the client device, a second set of encrypted data from the contactless card in response to the contactless card being activated, wherein the second set of encrypted data is based on a cryptographic algorithm and a diversified key of the contactless card, wherein the second set of encrypted data is associated with the user account;

performing, by the application, the second authentication based on the second set of encrypted data;

authorizing, by the application, access to the digital service in response to the first authentication and the second authentication;

transmitting, by the application at each of a plurality of time periods, a respective status message of a plurality of status messages to the contactless card to verify that the contactless card is active;

receiving, by the application, a first response of a plurality of responses from the contactless card in response to a first status message of the plurality of status messages;

providing, by the application based on the first response, access to the digital service without requiring re-authentication;

determining, by the application, that a response to a second status message of the plurality of status messages is not received from the contactless card; and

terminating, by the application, access to the digital service based on the determination that the response to the second status message is not received from the contactless card.

2. The method of claim 1, wherein the second set of encrypted data is received from the contactless card in a near-field communication (NFC) data exchange format (NDEF) message in response to the contactless card coming into a communication range of the client device, wherein the second set of encrypted data includes at least one of: an encrypted

expiration date, an encrypted billing address, and an encrypted card verification value (CVV) associated with the user account.

3. The method of claim 2, wherein the plurality of status messages are transmitted by energizing an NFC interface and an antenna to perform one or more NFC read operations with the contactless card, wherein the plurality of responses are received via an antenna of the contactless card in response to the corresponding status message in a respective NDEF message.

4. The method of claim 1, wherein performing the second authentication comprises:
 sending, by the application, the second set of encrypted data to a server; and
 receiving, by the application from the server, the second authentication based on the second set of encrypted data.

5. The method of claim 1, wherein determining the response to the second status message is not received comprises:

 determining, by the application, that a signal strength of the contactless card is below a threshold value.

6. The method of claim 1, further comprising receiving the contactless card within a slot through an end wall of a physical covering, the slot defining a set of walls operable to house the contactless card, and the slot disposed along a backside of the client device when the client device is coupled with the physical covering.

7. The method of claim 1, wherein authorization to access the digital service continues while the contactless card is active, wherein authorization to access the digital service terminates when the contactless card is inactive, wherein a third response of the plurality of responses is received subsequent to the first response and prior to determining the response to the second status message is not received, wherein the application provides access to the digital service without requiring re-authentication based on the third response.

8. A computer-readable storage medium including instructions that when executed by a processor of a client device, cause the processor to:

 receive, by an application, a request to access a digital service;
 receive, by the application, a first authentication based on verification of a first set of encrypted data associated with a user account;

request, by the application based on the first authentication, a second authentication from a contactless card, wherein the contactless card is activated by a magnetic field of the client device;

receive, via a card reader of the client device, a second set of encrypted data from the contactless card in response to the contactless card being activated, wherein the second set of encrypted data is based on a cryptographic algorithm and a diversified key of the contactless card, wherein the second set of encrypted data is associated with the user account;

perform, by the application, the second authentication based on the second set of encrypted data;

authorize, by the application, access to the digital service in response to the first authentication and the second authentication;

transmit, by the application at each of a plurality of time periods, a respective status message of a plurality of status messages to the contactless card to verify that the contactless card is active;

receive, by the application, a first response of a plurality of responses from the contactless card in response to a first status message of the plurality of status messages;

provide, by the application based on the first response, access to the digital service without requiring re-authentication;

determine, by the application, that a response to a second status message of the plurality of status messages is not received from the contactless card; and

terminate, by the application, access to the digital service based on the determination that the response to the second status message is not received from the contactless card.

9. The computer-readable storage medium of claim 8, wherein the second set of encrypted data is received from the contactless card in a near-field communication (NFC) data exchange format (NDEF) message in response to the contactless card come into a communication range of the client device, wherein the second set of encrypted data includes at least one of: an encrypted expiration date, an encrypted billing address, and an encrypted card verification value (CVV) associated with the user account.

10. The computer-readable storage medium of claim 9, wherein the plurality of status messages are transmitted by energizing an NFC interface and an antenna to perform one or more NFC read operations with the contactless card.

11. The computer-readable storage medium of claim 10, wherein the plurality of responses are received via an antenna of the contactless card in response to the corresponding status message in a respective NDEF message.

12. The computer-readable storage medium of claim 8, wherein determining the response to the second status message is not received comprises:

determine, by the application, that a signal strength of the contactless card is below a threshold value.

13. The computer-readable storage medium of claim 12, wherein the instructions further configure the processor to:

display, by the application, the signal strength of the contactless card in a graphical user interface.

14. The computer-readable storage medium of claim 8, wherein authorization to access the digital service continues while the contactless card is active, wherein authorization to access the digital service terminates when the contactless card is inactive, wherein a third response of the plurality of responses is received subsequent to the first response and prior to determining the response to the second status message is not received, wherein the application provides access to the digital service without requiring re-authentication based on the third response.

15. A computing apparatus comprising:

a processor;

a card reader; and

a memory storing instructions that, when executed by the processor, cause the processor to:

receive, by an application, a request to access a digital service;

receive, by the application, a first authentication based on verification of a first set of encrypted data associated with a user account;

request, by the application based on the first authentication, a second authentication from a contactless card, wherein the contactless card is activated by a magnetic field of the apparatus;

receive, by the card reader, a second set of encrypted data from the contactless card in response to the contactless card being activated, wherein the second set of encrypted data is based on a cryptographic algorithm and a diversified key of the contactless card, wherein the second set of encrypted data is associated with the user account;

perform, by the application, the second authentication based on the second set of encrypted data;

authorize, by the application, access to the digital service in response to the first authentication and the second authentication;

transmit, by the application at each of a plurality of time periods, a respective status message of a plurality of status messages to the contactless card to verify that the contactless card is active;

receive, by the application, a first response of a plurality of responses from the contactless card in response to a first status message of the plurality of status messages;

provide, by the application based on the first response, access to the digital service without requiring re-authentication;

determine, by the application, that a response to a second status message of the plurality of status messages is not received from the contactless card; and

terminate, by the application, access to the digital service based on the determination that the response to the second status message is not received from the contactless card.

16. The computing apparatus of claim 15, wherein the second set of encrypted data is received from the contactless card in a near-field communication (NFC) data exchange format (NDEF) message in response to the contactless card come into a communication range of the apparatus, wherein the second set of encrypted data includes at least one of: an encrypted expiration date, an encrypted billing address, and an encrypted card verification value (CVV) associated with the user account.

17. The computing apparatus of claim 16, wherein the plurality of status messages are transmitted by energizing an NFC interface and an antenna to perform one or more NFC read operations with the contactless card.

18. The computing apparatus of claim 17, wherein the plurality of responses are received via an antenna of the contactless card in response to the corresponding status message in a respective NDEF message.

19. The computing apparatus of claim 15, wherein determining the response to the second status message is not received comprises:

determining, by the application, that a signal strength of the contactless card is below a threshold value.

20. The computing apparatus of claim 15, further comprising a slot configured to receive the contactless card through an end wall of a physical covering, the slot defining a set of walls operable to house the contactless card, and the slot disposed along a backside of the apparatus.