INTELLIGENT CARD UNLOCK

RELATED APPLICATIONS

[0001] This application claims priority to U.S. Non-Provisional Application No. 16/863,179, filed April 30, 2020, titled "INTELLIGENT CARD UNLOCK". The contents of the aforementioned application are incorporated herein by reference in their entirety.

TECHNICAL FIELD

[0002] Examples herein generally relate to computing platforms, and more specifically, to intelligently unlocking a payment card, including a contactless card for use in a transaction.

BACKGROUND

[0003] Payment card locking functions presently allow a user to lock their payment card from being used when the card is not in possession of the user, i.e., the card is lost, stolen or misplaced. Locking the card prevents any transactions from being used in any transaction. The card lock functionality enables a user to ascertain whether the card is simply misplaced instead of stolen without having to go through all of the actions required when reporting the card lost or stolen. The actions required when reporting the card lost or stolen may include placing the account associated with the card on hold, sending a new physical card to the user via a delivery service and other inconveniences. The payment card lock functionality was developed to allow a user to avoid taking the required actions for replacement and mitigate the inconveniences.

[0004] It would be beneficial and an advantage with regard to fraud prevention and user security if the payment card could be locked at all times and easily unlocked at a user's request or at convenient times or when it is determined that the user is at a location where there is a high probability the user may locations.

SUMMARY

[0005] Examples disclosed herein provide systems, methods, articles of manufacture, and computer-readable media for enabling the unlocking of a contactless card for use in card-present transactions. According to one example, an apparatus may include a display device, a processor circuit, a transceiver, a card reader circuit and a memory. The processor circuit may be operable to present a graphical user interface on the display device. The transceiver may be coupled to the processor circuit and operable to communicate with external devices. The card reader circuit may be coupled to the processor circuit and be operable to emit and receive

signals within a signal field. The memory may be coupled to the processor circuit and operable to store an unlock-lock application. The unlock-lock application may have instructions which when executed by the processor circuit, causes the processor circuit to receive, via the card reader circuit, encrypted data from a contactless card. The contactless card may be locked to prevent use in a card present transaction and the encrypted data is generated based on a cryptographic algorithm and a diversified key. The unlock-lock application executed by the processor circuit may cause the encrypted data to be forwarded to an authentication server to authenticate and unlock the contactless card. An unlock indication that the contactless card has been unlocked enabling the contactless card for use in a card present transaction may be received. The unlock indication indicates the contactless card has been authenticated. User preferences may be identified for uses of the contactless card in payment card transactions when unlocked and a representation of the identified user preferences of the contactless card may be presented in the graphical user interface presented on the display device.

[0006] Another example discloses, a system including a contactless card and a mobile device. The contactless card may include a processor, a memory, and a communications interface operable to support at least one of near field communication, Bluetooth, or Wi-Fi communication protocol. The mobile device may include a mobile device processor, a mobile device memory, a transceiver, a display device, and a card reader circuit. The card reader circuit is operable to communicate with the contactless card via the communications interface and the mobile device memory stores programming code including an instance of an unlock-lock application. The processor of the contactless card may be operable to generate encrypted data using a cryptographic algorithm and a diversified key; and emit via the communications interface, a signal containing encrypted data usable to authenticate the contactless card. The programming code when executed by the mobile device processor causes the mobile device processor to perform functions, including functions to receive from the card reader circuit the signal containing encrypted data emitted from contactless card. The encrypted data may be forwarded via the transceiver for authentication and unlocking of the contactless card. The mobile device processor may receive an unlock indication indicating the contactless card is unlocked. User preferences may be identified that allow limited uses of the contactless card when unlocked for use in card-present transactions. A representation of the identified user preferences of the contactless card, when unlocked, may be presented in a graphical user interface presented on the display device.

[0007] An example of a non-transitory computer-readable storage medium is provided. The non-transitory computer-readable storage medium may be embodied with having computer-readable program code. The computer-readable program code is executable by a processor circuit to cause the processor circuit to receive, via a card reader circuit, encrypted data from a communications interface of a contactless card. The contactless card may be locked from being used in a card present transaction and the encrypted data is generated based on a cryptographic algorithm and a diversified key. The encrypted data may be forwarded to an authentication server to enable the contactless card to be unlocked. An unlock indication that the contactless card has been unlocked for use in a card present transaction may be received. The unlock indication is verification of the encrypted data. A permitted contactless card use restriction of a capability of the contactless card to complete a payment card transaction may be identified. An unlocked-for-use status indication and a representation of the identified permitted contactless card use restriction may be presented in a graphical user interface presented on a display device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Figures 1A and 1B illustrate examples of a system for locking and unlocking card for use in a transaction.

[0009] Figures 2A and 2B illustrate examples of locking and unlocking card for use in a transaction.

[0010] Figures 3A-3C illustrate examples of locking and unlocking card for use in a transaction.

[0011] Figures 4A and 4B illustrate an example contactless card suitable for use in the examples of Figures 1-2B.

[0012] Figure 5 illustrates an example of a mobile device suitable for implementing the examples of Figures 1-4.

[0013] Figure 6 illustrates an example of a computing architecture suitable for implementing the examples of Figures 1-5.

DETAILED DESCRIPTION

[0014] Examples disclosed herein provide secure techniques for locking and unlocking a payment card for use in a card present transaction. Commonly, a payment card is unlocked

and operable to allow completion of card-present transactions with merchants. In cases of lost cards and despite being able to lock the card if it the user does not know the card is lost, there is still the opportunity for the lost card to be used in fraudulent activities. The foregoing examples advantageously provide an easy to use and implement solution that reduces the potential for credit fraud.

[0015] In the foregoing examples, the contactless card when unauthenticated is locked which makes the contactless card unusable in a card present transaction and authentication of the contactless card indicates the contactless card is valid (e.g., authenticated and assigned to an authorized user and payment account) and unlocked which makes that contactless card usable in a card present transaction.

[0016] 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.

[0017] 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 examples. Rather, these operations are machine operations. Useful machines for performing operations of various examples 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 examples 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.

[0018] 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 examples 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.

[0019] Figure 1A depicts a schematic of an exemplary system 100, consistent with disclosed examples.

[0020] In the example of Figure 1A, a mobile device 110 may include a processor circuit 147, a communication interface 146, a touchscreen display 149, and a memory 141. The memory 141 may be operable to store an account authentication application 143, an unlock-lock application 144 and other applications 145, such a messaging application, a banking application, a location application, telephone application, or the like. The respective applications 143-145 may include computer-readable programming code that is executable by a processor or processor circuit. The account authentication application 143 may provide functions and features in response to a request from the unlock-lock application 144. Examples of the functions and features provided in response to the request are described with reference to Figures 2A and 2B.

[0021] The touchscreen display 149, for example, may be coupled to the processor circuit 147 and be operable to present a graphical user interface (shown in another example) in response to signals from the processor circuit 147. The communication interface 146 may be operable to communicate with external devices, such as server 120, via a number of transceivers (not shown in this example). For example, the mobile device 110, which may be a smartphone equipped with a cellular transceiver and a Wi-Fi transceiver (e.g., 802.11 family of transceivers) (shown in another example). The card reader 148 may be equipped with a near-field communication (NFC) circuit that is operable to emit and receive signals within a signal field (e.g., an area within a short range, such as 2-10 centimeters) of the mobile device 110. As shown, a memory 141 of the mobile device 110 includes an instance of an operating system (OS) 142. Example operating systems 142 include the Android® OS, iOS®, Linux®, and Windows® operating systems. As shown, the OS 142 includes an account authentication

application 143, an unlock-lock application 144, and one or more other applications 145. The account authentication application 143 allows 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 authentication application 143. For example, the authentication credentials may include a username and password, biometric credentials, and the like.

[0022] The account authentication application when executed causes the processor circuit 147 to perform functions related to authenticating a contactless card, such as 101. For example, when the locked contactless card 101 is placed within the signal field of the card reader 148 of the mobile device 110, the contactless card 101 establish a communication path with the mobile device 110 and provide the encrypted data 190 to the account authentication application 143 of the mobile device 110. The account authentication application 143 may cause the transfer the encrypted data 190 via the network 130 to the server 120, which authenticates the contactless card 101 and unlocks the contactless card 101 for use in card-present transactions. The server 120 may provide an indication that the authentication and unlocking of the contactless card 101 was successful to the account authentication application 143 via a message through the network 130. The account authentication application 143 may provide the indication to, or otherwise notify, the unlock-lock application 144 which when executed causes the processor circuit 147 to perform functions related to limiting operation of the unlocked contactless card. The processor circuit 147 when the account authentication application 143 is executed causes the processor circuit to perform functions. In instances in which the account authentication application 143 and the unlock-lock application 144 are operating, the content of the graphical user interface may be generated or provided by the account authentication application 143 and the unlock-lock application 144 executed by the processor circuit 147.

[0023] With the foregoing operational example providing context for capabilities of the disclosed examples, it may be beneficial to describe the components of the system 100 in more detail with reference to the functions performed by the respective components.

[0024] As shown, the system 100 includes one or more contactless cards 101, one or more mobile devices 110, and a server 120. The contactless card 101 is representative of any type of payment card, such as a credit card, debit card, ATM card, gift card, and the like. The contactless cards 101 may include one or more chips (not depicted), such as a radio frequency identification (RFID) chip, operable to communicate with the mobile devices 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 mobile devices 110 are 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 equipped with one or more processors 121 may be any type of computing device, such as a server, workstation, computer cluster, cloud computing platform, virtualized computing system, or the like.

[0025] The contactless card 101 may include a processor 115 and a communication interface 116. As described with reference to the examples of Figures 4A and 4B, the processor 115 may be circuitry operable to perform logical functions and the communication interface 116 may be circuitry operable to exchange signals with other devices, such as mobile device 110 and the like.

[0026] As shown, a memory 102 of the contactless card includes 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 include an account number, an expiration date, a billing address, or 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. The account numbers 108 store one-time-use virtual account numbers with associated expiration dates and CVV values. For example, the account numbers 108 may include a number of single-use virtual account numbers, expiration dates, and CVV values.

[0027] As shown, the server 120 includes a data store of account data 124 and a memory 122. The account data 124 includes account-related data for a number of 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 virtual card numbers, and biographical information for each account. The memory 122 may include a management application 123 and an instance of the card data 103, an instance of the counter 104, an instance of the master key 105, and an instance of the diversified key 106 for one or more accounts from the account data 124.

[0028] The system 100 is operable 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 may be kept secret from all parties other than the contactless card 101 and server 120, thereby enhancing security of the system 100.

[0029] The master key 105 may be used in conjunction with the counters 104 to enhance security using key diversification. The counters 104 include values that are synchronized between the contactless card 101 and server 120. The value of counter 104 may include 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 mobile device 110). To enable NFC data transfer between the contactless card 101 and the mobile device 110, the account authentication application 143 may communicate with the contactless card 101 when the contactless card 101 is sufficiently close to a card reader 148 of the mobile device 110. Card reader 148 may be operable to read from and/or communicate with contactless card 101 (e.g., via NFC, Bluetooth, RFID, Wi-Fi, etc.). Therefore, example card readers 148 include NFC communication modules, Bluetooth® communication modules, and/or RFID communication modules.

[0030] After the account authentication application 143 and/or the unlock-lock application 144 are launched or opened, the opened application may prompt a user to tap the contactless card 101 to the mobile device 110. For example, a user may tap the contactless card 101 to the mobile device 110, thereby bringing the contactless card 101 sufficiently close to the card reader 148 of the mobile device 110 to enable NFC data transfer between the contactless card 101 and the card reader 148 of the mobile device 110. In some examples, the mobile device 110 may trigger the card reader 148 via an API call or the like. In addition, and/or alternatively, the mobile device 110 may trigger the card reader 148 by periodically polling the card reader 148. More generally, the mobile device 110 may trigger the card reader 148 to engage in communications using any feasible method. Once the contactless card 101 is tapped (e.g., brought within NFC communications range of the card reader 148) to the mobile device 110,

the account authentication application 143 either on its own initiative or in response to a signal from the unlock-lock application 144 may generate and transmit an indication to the contactless card 101 to generate an encrypted data 190 as depicted in Figure 1A.

[0031] In response, the contactless card 101 increments the value of counter 104 and provides the master key 105 and value of counter 104 as input to a cryptographic algorithm, which produces a diversified key 106 as output. The contactless card 101 may then encrypt the customer identifier 107 using the diversified key 106 to generate the encrypted data 190. The contactless card 101 may then transmit the encrypted data 190 to the account authentication application 143 of the mobile device 110 (e.g., via an NFC connection, Bluetooth connection, etc.). The account authentication application 143 of the mobile device 110 may then transmit the encrypted data 190 to the server 120 via the network 130. In at least one example, the contactless card 101 transmits the value of counter 104 along with the encrypted data 190.

[0032] After communication has been established between mobile device 110 and contactless card 101, the contactless card 101 may generate a message authentication code (MAC) cryptogram. 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 authentication application 143 and/or the card reader 148, may transmit a message, such as an applet select message, with the applet ID of an NDEF producing applet. At this point, the value of counter 104 maintained by the contactless card 101 may be updated or incremented. 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 (e.g., responsive to another 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 transmit the MAC cryptogram to the mobile device 110, which may then forward the MAC cryptogram to the server 120 for verification as explained below. However, in some examples, the mobile device 110 may verify the MAC cryptogram.

[0033] More generally, when preparing to send data (e.g., to the server 120 and/or the mobile device 110), the contactless card 101 may increment the value of counter 104. The contactless card 101 may then provide the master key 105 and value of counter 104 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 (HMAC) 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 HMAC algorithm, such as HMAC-SHA-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 data 190) to the account authentication application 143 of the mobile device 110 (e.g., via an NFC connection, Bluetooth connection, etc.). For example, the contactless card 101 may be operable to emit encrypted data via a tap 174 as well as receive signals when the contactless card is within a signal field of the card reader 148. Similarly, the card reader 148 may be operable to also emit signals and receive signals. In more detail, the card reader 148 may receive the encrypted data 190 via tap 174 while the contactless card 101 is locked. The account authentication application 143 of the mobile device 110 may then transmit the encrypted data to the server 120 via the network 130. In at least one example, the contactless card 101 transmits the value of counter 104 with the encrypted data. In such examples, the contactless card 101 may transmit a value of counter 104 that is either an encrypted or an unencrypted value of the counter 104.

[0034] Upon receipt of the encrypted data 190 from the mobile device 110, the management application 123 of the server 120 may be operable to verify the encrypted data 190 using key diversification. Key diversification performed by the management application 123 of the server 120 may include performing the same symmetric encryption using the value of counter 104 as input to the encryption (by the processor 115 of the contactless card), and the master key 105 as the key for the encryption. As stated, the value of counter 104 may be specified in data received with the encrypted data 190 from the mobile device 110, or a value of counter 104 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 data 190 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 mobile device 110, e.g., by comparing the decrypted customer ID 107 to a customer ID in the account data 124 for the account, where, for example, a match of the customer ID values verifies the encrypted data received from the contactless card 101.

[0035] Although the counter 104 is used as an example, other data may be used to secure communications between the contactless card 101, the mobile 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.

[0036] As shown, the server 120 may include one or more hardware security modules (HSM) 125. For example, one or more HSMs 125 may be operable to perform one or more cryptographic operations as disclosed herein. In some examples, one or more HSMs 125 may be configured as special purpose security devices that are operable to perform the one or more cryptographic operations. The HSMs 125 may be configured such that keys are never revealed outside the HSM 125, and instead are maintained within the HSM 125. For example, one or more HSMs 125 may be operable 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.

[0037] After authenticating the locked contactless card 101, and subsequently unlocking the contactless card for use in card present transactions, the components of system 100 may operate according to the system example shown in Figure 1B and the accompanying discussion.

[0038] As shown in the system example of Figure 1B, the system 184 in addition to the mobile device 110, network 130 and server 120, which perform the same functions, the system 184 further includes the unlock-lock server 129, a server 160 that hosts an payment account component 163, a point of sale device 170 at a merchant 180, and a network 191 that couples the point of sale device 170 to the payment account component 163 of server 160. The unlock-

lock server 129 may include a processor, and memory with programming code or instructions, and may be operable manage, via an instance of the unlock-lock application 144″, user preference settings that limit the use of the unlocked contactless card 101′ as well as a number of unlocked contactless cards belonging to other users.

[0039] Returning to the operational example, in response to sending the encrypted data 190 to the server 120, the processing circuit 147 executing the account authentication application 143 may receive from the server 120 an indication that the contactless card 101 has been unlocked based on an authentication of the encrypted data 190. The indication that the contactless card has been unlocked and authenticated may be output to the unlock-lock application 144 by the account authentication application 143.

[0040] In another example, the unlock-lock server 129 may be operable to receive, from the mobile device 110, user preference settings indicated as selected for permitted uses of the contactless card in card present transactions, when the contactless card is unlocked. The unlock-lock server 129 may be further operable to obtain the determined location of the mobile device from the mobile device 110 via a location application executing as one of the other applications 145. The location of the mobile device 110 may be used by the instance of the unlock-lock application 144″ to generate a list of merchants that satisfy the limited card uses of the user preferences.

[0041] The unlock-lock server 129 may be operable to manage user preferences of the unlock-lock application executing on the mobile device processor (i.e., processor circuit 147) of the mobile device 110. In a more detailed example, the unlock-lock server 129 may be operable to receive, from the mobile device, user preference settings indicated as selected, permitted uses of the unlocked contactless card in card-present transactions. The unlock-lock sever may be operable to derive a maximum transaction amount threshold from the user preference settings. For example, the user preference may be set at $50.00 for a transaction at a restaurant or the like. The unlock-lock server 129 may forward a maximum transaction amount threshold derived from the user preference settings to the payment account component 163 of server 160, via either the communication link 188 or the network 130. The communication link 188 may be a direct communication coupling between the unlock-lock server 129 and the server 160. The maximum transaction amount threshold may also be forwarded to the mobile device 110 for presentation in a graphical user interface presented on the touchscreen display 149.

[0042] As mentioned above with respect to Figure 1A above, once the management application 123 of server 120 verifies the encrypted data 190 using key diversification, the management application 123 may transmit an indication of authentication to the account authentication application 143 of the mobile device 110, which may, in one example, establish a connection to an application programming interface (API) of the unlock-lock application 144 and provide the indication of authentication to the unlock-lock application 144. Upon receipt of the indication of authentication which the unlock-lock application 144 interprets as an indication that contactless card 101′ is unlocked, the unlock-lock application 144 may send a request to unlock-lock server 129 regarding limiting use of the unlocked contactless card 101′. The limiting uses (which are described in more detail with reference to other examples) may include a list of merchants within an area that are whitelisted for card-present transactions using the unlocked contactless card 101′. Merchant 180 may be on the list of whitelisted merchants. The unlocked contactless card 101′ has the features as contactless card 101 with the only difference being that unlocked contactless card 101′ is now unlocked and enable to participate in some card-present transactions, subject to the limiting uses described herein. For example, the unlocked contactless card 101′ may be operable to communicate with card reader 148 via a wireless connection 175. Unlocked contactless card 101′ may be presented for a card-present transaction, and transaction data 166 may be transmitted via wireless connection 177 from the contactless card 101′ to the point of sale device 170 of the merchant 180. The transaction data 166 may be, for example, information used for completion of the transaction, such as a card number, account number or some other identifying information that may be used to verify whether the contactless card 101′ is coupled to an authorized payment account. Of course, if the contactless card 101′ is equipped with an identifying chip or a magnetic strip, the information required for the transaction may be transmitted by inserting the identifying chip into or swiping the magnetic strip through the point of sale device 170 to provide the transaction data 166. The point of sale device 170 at the merchant 180 may be operable to forward the transaction data 166 through the network 191 to the payment account component 163 for a verification process.

[0043] The server 160 may be operable to receive the transaction data 166 to determine whether the transaction may be completed based on a verification process performed by the payment account component 163. For example, the payment account component 163 may use the transaction data 166 to process the financial aspects of the transaction, such as, for example, verify that the transaction is a card-present transaction, the payment account of the user

associated with the unlocked contactless card 101′ is valid and has sufficient credit or funds, that the contactless card 101′ is unlocked for the card-present transaction, that the user preference settings provided by the unlock-lock application 144 are satisfied, and the like. The server 160 Transaction reaction data 167, which may be an indication of a result of the verification process performed by the payment account component 163, may be returned through the network 191 to the point of sale device 170.

[0044] The payment account component 163 may include additional capabilities beyond enabling completion of the card-present transaction. The payment account component may include query logic or machine learning that may be applied to past transactions to identify patterns or trends and whitelist those transactions that are considered low risk. For example, the patterns or trends may reveal frequent visits to certain merchants, dollar thresholds a user frequently does not exceed, and/or location patterns, such as consistently purchasing meals within 1 mile of the user's office or home, and/or during specific hours. These patterns and trends may be used to identify new user preferences or modify existing user preferences. For example, in situations, where a new restaurant or coffee shop opens within a set radius, a user preference may be modified to generate a list of any lunch place having a particular merchant category code being enabled to allow completion of a card-present transaction. For example, the modified user preference may also be to allow any restaurant purchase under $25 within 1 mile of the user's office, or the like.

[0045] The example of Figure 1B shows the management application 123 of the server 120 transmitting the card data 103 from the server 120 to the mobile device 110 after verifying the encrypted data 190 of Figure 1A. In at least one example, the management application 123 may encrypts the card data 103 before sending to the account authentication application 143. As stated, the card data 103 may include the account number, CVV, and/or expiration date of the contactless card 101. The card data 103 may further include the account holder's first name, last name, shipping address, and billing address. In one example, the account number of the card data 103 may be the virtual card number generated subsequent to the verification of the encrypted data 190 by the management application 123. In another example, the account number of the card data 103 is a record from the account numbers 108. In one example, the first and last names are stored in the account authentication application 143 (or another element of the OS). The account authentication application 143 may provide the card data 103 and/or the indication of the authentication of the encrypted data 190 to an API of the unlock-lock application 144. The unlock-lock application 144 may use interpret information provided by

the account authentication application 143 to determine whether the contactless card is unlocked for card-present transactions, and, if so, implement the user-preferences as discussed with reference to this example and the examples of FIGs. 2A-3C.

[0046] In one example, the card data 103 sent by the server 120 to the mobile device 110 includes all relevant information (e.g., the account number, expiration date, CVV, billing address, shipping address, first name, last name, etc.) required to make a purchase using the account associated with the contactless card 101.

[0047] In an example, the network 130 may couple to other servers in addition to server 120. For example, the mobile device processor circuit 147 may be operable to obtain a location preference setting from a number of user preference settings stored in memory 141. The mobile device processor circuit 147 may obtain location data from a location application of the location and other applications 145. The location data may include a position, a timestamp and a velocity. The obtained location preference setting and the obtained location data to may be sent to an unlock-lock server 129. In response, the mobile device processor circuit 147 may receive a list of merchants satisfying the obtained location preference setting based on the obtained location data. The processor circuit may present the list of merchants in the graphical user interface on a display device, such as the touchscreen display 149.

[0048] The mobile device processor circuit 147 may be further operable to determine, based on the location data provided by the location application, a card unlock action is required to meet an imminent a card present transaction. The processor circuit may generate instructions to produce a notification indicating the card unlock action is required. A notification actuation signal operable to actuate an output device or a display device according to the generated instructions may be output. An example of an output device and a display device are shown in the example of FIG. 6.

[0049] Figure 2A is a flowchart illustrating an example of a process that utilizes the system example of Figure 1. The process 200 may be executed by the mobile device 110 of Figure 1A or 1B. The execution of the unlock-lock application and an authentication application may make the processor circuit 147 of the mobile device 110 operable to, at 210, receive, via the card reader circuit, encrypted data from a contactless card. For example, the contactless card may be locked to prevent use in a card present transaction and the encrypted data is generated based on a cryptographic algorithm and a diversified key generated by the contactless card. At 220, the encrypted data may be forwarded to an authentication server to authenticate and unlock the contactless card. For example, the authentication server may be operable to decrypt the

encrypted data and verify the decrypted data to authenticate the contactless card. With a successful verification and resulting authentication, the contactless card may be unlocked for card-present transactions. The authentication server may be operable to generate, based on a verification of the decrypted data, the unlock indication that the contactless card is unlocked, and forward the unlock indication to the mobile device. The mobile device processor may receive the unlock indication that the contactless card has been unlocked enabling the card for use in a card present transaction (230). In addition, the unlock indication may indicate the contactless card has been authenticated and unlocked. The processor may be further operable to identify, at 240 user preferences for use of the contactless card when unlocked for use in payment card transactions. User preferences may include, for example, leaving the card unlocked for a set number of card present transactions (e.g., next 10 transactions or 20 transactions), allow relocking by manual tapping to phone, location (such as area between commuter drop off and office location, a particular business district, a shopping mall location, travel destination, or the like); amount of money spent (e.g., total of $100.00 for all transactions, $50.00 maximum for individual transactions, or the like), time increments (e.g., for next 6 hours, 1 hour, 45 minutes, length of commute or trip), or a re-lock setting in which the card is re-locked (or transition to a default state (e.g., a complete or a partial lock for some transactions) after an unlock duration, such as after one of the foregoing user preference time settings, after a default time setting, after the number of transaction or another setting). Alternatively, a server, such as 120 or 129 of FIG. 1 may, for example, according to a default setting or a user preference, automatically re-lock the card so that card present transactions are no longer possible without unlocking a subsequent time. At 250, the processor may present a representation of the identified user preferences of the contactless card in the graphical user interface presented on the display device, which may be a touchscreen display.

[0050] Figure 2B is another example of a process that may be implemented upon execution of an unlock-lock application 144 enable unlocking of a contactless card. The process 201 may be implemented as a mobile computing application that may provide permitted uses of an unlocked contactless card. The mobile computing application, such as the unlock-lock application 143 of Figure 1, may be stored as a non-transitory computer readable medium in a memory and may be implemented by a processor or processing circuitry. In the example process 201, the processor may receive, via the card reader circuit, encrypted data from a communications interface of a contactless card (211). For example, a contactless card may be locked from being used in a card present transaction and the encrypted data is generated based

on a cryptographic algorithm and a diversified key that are implemented and stored on the contactless card. The processor may cause the encrypted data to be forwarded to an authentication server to enable the contactless card to be unlocked (221). At 231, the processor executing the unlock-lock application on the mobile device may receive an unlock indication that the contactless card has been unlocked for use in a card present transaction. In addition, the indication may serve as verification by the server that the encrypted data was provided by an authorized user of the card or the like. The unlock-lock application executed by processor may identify a permitted contactless card use restriction of a capability of the contactless card to complete a payment card transaction (241). For example, a whitelist of merchants may be stored in a database maintained by the server, such as the unlock-lock application data 126 of FIG. 1A. In response to verifying that the encrypted data was provided by an authorized user of the card, the server may deliver a portion of or all of the whitelist of merchants to the unlock-lock application of the mobile device. The unlocked contactless card may only be usable (i.e., permitted for use) to conduct card-present transactions at the merchants included in the whitelist of merchants. For example, the server may receive user preference settings from the unlock-lock application of the mobile device. The user preference settings may indicate a time setting, a time and area setting that the user prefers, such as at 9 am allow card-present transactions to be made within 5 square blocks or half square mile of the user's location, the user's office or home location, an area setting, a merchant code setting (e.g., only coffee shops, restaurants and drug stores). Other settings may be based on a geographical location, a geo-fenced area, a merchant name, a price threshold, a time threshold, a day of the week, a time range within a day, a zip code, an area code; a merchant category, a product category, or the like. A time threshold may be a default timer, such as 30 minutes from the time of unlocking the contactless card. In an example, geo-fencing is a feature of a computer program that enables the developer or administrator to define geographical boundaries using a mobile device's location services such as global positioning system (GPS) or radio frequency identification tags (RFID) (if permitted by the mobile device's user) or using Wi-Fi or cellular data that is usable in determining location. A geo-fenced area may, for example, be an area enclosed by a radius or set by the zip code, or governmental boundary, such as a city or county designation or the like. In the example, the whitelist of merchants may be based on a user selecting a merchant code for limiting use of an unlocked contactless card at merchants assigned the merchant code.

[0051] At 251, the mobile device may present an unlocked-for-use status indication (e.g., unlocked, an icon of an opened lock, or the like) and a representation of the identified permitted

contactless card use restriction in the graphical user interface presented on the display device. For example, the representation may be the delivered portion of the whitelist of merchants or a map of the identified area setting or the like. In an example, the processor may present, via the graphical user interface, a number of limiting uses of the contactless card for a selection of a user preference that sets the limiting use of the contactless card. The limiting uses may include one or more of: a geographical location, a geo-fenced area, a merchant name, a price threshold, a time threshold, a day of the week, a time range within a day, a zip code, an area code; a merchant category, a product category, or the like.

[0052] The processor circuit may be further operable to receive, via a graphical user interface, a selection of a user preference that sets the limiting use of the contactless card. Location information may not be available until user opens an application, such as when the user requests (at 211 in the example of Figure 2B) to unlock the card may launch the unlock-lock application which may have permission to access or obtain location information from a location application or service, such as GPS, Wi-Fi location services or the like. For example, the location application may be operable to determine a location of the apparatus. In the example, the memory may be operable to store a number of user preference settings for an unlock-lock application and further instructions which when executed by the processor circuit. The processing circuit may be operable to determine, based on location provided by the location application, a card unlock action is required to meet an imminent a card present transaction. The processing circuit may be operable to generate instructions to produce a notification indicating the card unlock action is required and output a notification actuation signal operable to actuate an output device or a display device according to the generated instructions. For example, the processing circuit may present a prompt in a graphical user interface indicating a locked status of the contactless card.

[0053] In an operational example, in response to the indication of authentication, the unlock-lock application 144 may generate a list of card use restriction s in a graphical user interface based on user preferences maintained by the unlock-lock application 144 and present the generated list of card use restriction s in the graphical user interface (shown in another example).

[0054] The processing circuit may be operable to present on the graphical user interface a menu of user preference settings for selection by a user. The user preference settings may be permitted uses of an unlocked contactless card in card present transactions that by being selected allow a user to customize the use of their contactless card when it is unlocked. For

example, as shown in Figure 3A, the menu in the graphical user interface 313 may include a number of user preferences 301-305. The user may select one or more of the presented user preferences 301-305. As shown in Figure 3A, the user preference #1 301 and user preference #3 303 are shown in bold to indicate that these user preferences have been selected by the user.

[0055] The processing circuit may be operable to receive an indication of a selection of one or more of the user preference settings presented in the menu. Figure 3B illustrates an example of a graphical user interface showing a selection of user preference settings. For example, the mobile device 310 may present a graphical user interface 314 on a display device 320. The unlock-lock application may present selections which may be via a touch, when the display device is a touchscreen, to the graphical user interface 314. Examples of the selecting user preference setting may include a selection of a location such as location #1 317, a time range selection, such as time range #3 311, an area selection, such as radius #6 and a merchant category code, such as MCC #X 315. In the example, the time range selection may identify a time range during which the contactless card remains unlocked. An area selection may identify an area in which the contactless card may be used in card-present transactions when the card is unlocked. For example, the area may be defined by a radius from the location of the user, an area in square city blocks or square miles or feet, or some other way of indicating area, such as zip code or other postal code. For example, the radius selection may identify a distance from a user's location in which the contactless is permitted to be used in a card-present transaction. The merchant category code selection identifies a category of goods or services provided by merchants assigned a merchant category code for the goods or services provided by the respective merchant.

[0056] The processing circuit may obtain a location preference setting from the number of user preference settings stored in the memory (see, for example, the location #1 setting 317 of Figure 3B). The unlock-lock application executed by the processing circuit may be operable to obtain location data from the location application also executing on the processor circuit. The unlock-lock application may cause the processing circuit to be operable to send the obtained location preference setting and the obtained location data to an unlock-lock server. The unlock-lock server may be able to identify a number of merchants that satisfy the obtained location preference setting. For example, the unlock-lock server may be operable to access information about merchants that satisfy the respective location preference setting as well as other user preference settings. The unlock-lock application may receive a list of merchants

satisfying the obtained location preference setting or other settings based on the obtained location data.

[0057] Returning to the example of Figure 2A, the processing circuit may operable to communicate via the unlock-lock application with a server, such as 120 of FIG. 1, that is operable to manage user preferences of the unlock-lock application. In an example, the processing circuit may be operable provide the user preference settings indicated as selected for permitted use of the unlocked contactless card in card present transactions.

[0058] In the examples, the merchant name or merchant category code (e.g., grocery store, professional services or the like (Per IRS revised procedure 2004-43, a Merchant Category Code (MCC) is a classification code that is assigned by a payment card organization to a merchant/payee. The payment card organization assigns the merchant a particular code based on the predominant business activity of the merchant)). The merchant category code allows users to make card present purchases at establishments that are new to area. For example, the restaurant is so new to the area that the user has not made a card present purchase there or that has not been established in the mapping applications used for location services.

[0059] Figure 3A is an example of a graphical user interface (GUI) of the unlock-lock application 144 on the mobile device 110. For example, the processor may be operable to the processor may drive a display device, such as a touchscreen display of the mobile device to present a graphical user interface with a number of user preferences for setting the limiting use of the contactless card. The respective user preferences 301-305 may include settings based on a geographical location, a geo-fenced area, a merchant name, a price threshold, a time threshold, a day of the week, a time range within a day, a zip code, an area code; a merchant category, a product category, or the like.

[0060] Once the contactless card 101 is tapped to the mobile device 110, the account authentication application 143 transmits, via the card reader 148 (e.g., via NFC, Bluetooth, RFID, and/or the EMV protocol etc.), an indication to the contactless card 101. In one example, the indication may specify to perform encryption using key diversification as depicted in Figure 1A, in which case the account authentication application 143 receives card data 103 from the server 120. In another example, the indication may specify to transmit the card data 103 to the account authentication application 143 in an NDEF file (e.g., via NFC, Bluetooth, RFID, etc.), in which case the account authentication application 143 receives the card data 103 in an NDEF file directly from the contactless card 101 via the card reader 148. In another example, the indication may specify to transmit the card data 103 to the account authentication application

143 via the EMV protocol, in which case the account authentication application 143 receives the card data 103 directly from the contactless card 101 via the EMV protocol. However, as stated, in examples where the EMV protocol is used, the CVV value is received from the contactless card 101 in an NDEF file and/or from the management application 123. In another example, the indication may specify to perform encryption using key diversification as depicted in Figure 1A and transmit an account number 108 to the account authentication application 143, in which case the account authentication application 143 receives a record from the account numbers 108 from the contactless card 101 (which is used subject to verification of the encrypted data 190 by the server 120).

[0061] Figure 3B is an illustration of a mobile device 310 that is presenting a graphical user interface 314 containing a selection of user preferences settings 311-317. The mobile device may be operable to send the selected user preferences settings 311-317 to a server. For example, the server may receive user preference settings from the unlock-lock application of the mobile device. The user preference settings 311-317 may indicate, for example, a time setting, a time and area setting that the user prefers, such as at 9 am allow card-present transactions to be made within 5 square blocks or half square mile of the user's location, the user's office or home location, an area setting, a merchant code setting (e.g., only coffee shops, restaurants and drug stores).

[0062] As shown in FIG. 3C, the unlock-lock application may be operable to present the list of merchants 321-327 in the graphical user interface 324 on the display device 320 (e.g., a touchscreen display) of the mobile device 310. For example, as mentioned above, the mobile device 110 may provide a location of the mobile device to the unlock-lock server 129. In more detail, the unlock-lock server 129 may retrieve a location setting from the user preference settings, provided via the graphical user interface 313 of FIG. 3A. In the example, the location setting may be a radius (such as radius #6 in graphical user interface 314 of Figure 3B) from a predetermined location. The predetermined location may be, for example, the location of the mobile device, the user's office, home, friend's home, favorite restaurant, gym or the like. The unlock-lock server 129 may access a merchant location service, such as 149, based on the user preference settings. From the merchant location service 149, the instance of the unlock-lock application 144″ may obtain a list of merchants, such as merchant #1 to #X based on the retrieved location setting and the determined location. The instance of the unlock-lock application 144″ may be operable to generate a list of merchants based on the retrieved location setting and the determined location of the mobile device. The generated list of merchants may

be forward to the mobile device 110 via network 130, for example. In the example of FIG. 3C, the mobile device 310 may be operable to present the list of merchants 321-327 in the graphical user interface 324 on the display device 320 of the mobile device 310.

[0063] Figure 4A illustrates a contactless card 101/101′, which may include a payment card, such as a credit card, debit card, and/or a gift card. As shown, the contactless card 101/101′ may be issued by a service provider 405 displayed on the front or back of the card 101/101′. In some examples, the contactless card 101/101′ is not related to a payment card, and may include, without limitation, an identification card. In some examples, the payment card may include a dual interface contactless card. The contactless card 101/101′ may include 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 101/101′ 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 101/101′ 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.

[0064] The contactless card 101/101′ 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 operable to establish contact with another communication device, such as the mobile devices 110, a user device, smart phone, laptop, desktop, or tablet computer. The contactless card 101 may also include processing circuitry, antenna and other components not shown in the example of FIG. 4A. These components may be located behind the contact pad 420 or elsewhere on the substrate 410. The contactless card 101/101′ may also include a magnetic strip or tape, which may be located on the back of the card (not shown in FIG. 4A).

[0065] As illustrated in FIG. 4B, the contact pad 420 of contactless card 101/101′ may include processing circuitry 425 for storing and processing information, including a microprocessor 430, communications interface 431, and the memory 402. It is understood that the processing circuitry 425 may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anti-collision algorithms, controllers, command decoders, security primitives and tamper-proofing hardware, as necessary to perform the functions described herein.

[0066] The memory 402 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 101/101′ 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 is programmed, it may not be rewritten, but it may be read many times. A read/write memory may be programmed and re-programed many times after leaving the factory. A read/write memory may also be read many times after leaving the factory.

[0067] The memory 402 may be operable to store one or more applets 440, one or more counters 404, a customer identifier 407, and virtual account numbers 408. The one or more applets 440 may include one or more software applications operable 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 404 may include a numeric counter sufficient to store an integer. The customer identifier 407 may include a unique alphanumeric identifier assigned to a user of the contactless card 101/101′, and the customer identifier 407 may distinguish the user of the contactless card 101/101′ from other contactless card users. In some examples, the customer identifier 407 may identify both a customer and an account assigned to that customer and may further identify the contactless card associated with the customer's account. As stated, the account numbers 408 may include thousands of one-time use virtual account numbers associated with the contactless card 101/101′.

[0068] The processor and memory elements of the foregoing exemplary examples are described with reference to the contact pad 420, but the present disclosure is not limited thereto. It is understood that these elements may be implemented outside of the contact pad 420 or entirely separate from it, or as further elements in addition to microprocessor 430 and memory 402 elements located within the contact pad 420.

[0069] In some examples, the contactless card 101/101′ may include one or more antennas 455. The one or more antennas 455 may be placed within the contactless card 101/101′ and around the processing circuitry 425 of the contact pad 420. For example, the one or more antennas 455 may be integral with the processing circuitry 425 and the one or more antennas 455 may be used with an external booster coil to provide a communications interface 431. As

another example, the one or more antennas 455 may be external to the contact pad 420 and the processing circuitry 425.

[0070] In an example, the coil of contactless card 101/101′ may act as the secondary of an air core transformer. A terminal, such as the card reader 148 on the mobile device 110 of Figure 1 may communicate with the contactless card 101/101′ by cutting power or amplitude modulation. The contactless card 101/101′ may gather the data transmitted from a point-of-sale terminal (not shown in this example) or the card reader 148 using gaps in the contactless card's power connection, which may be functionally maintained through one or more capacitors. The contactless card 101/101′ may communicate back by switching a load on the contactless card's coil via load modulation that is detectable by. Load modulation may be detected in the terminal's coil. More generally, using the antennas 455, processing circuitry 425, and/or information stored in the memory 402, the contactless card 101/101′ provides a communications interface 431 to communicate via, respective, NFC, Bluetooth, and/or Wi-Fi communication protocols. If the contactless card 101/101′ is so equipped to provide Bluetooth and Wi-Fi communications, the Bluetooth and Wi-Fi communications may be provided via transceivers 435. The communication pro

[0071] As explained above, contactless cards 101/101′ may be built on a software platform operable on smart cards or other devices having limited memory, such as JavaCard, and one or more 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 operable 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 mobile device 110), and produce an NDEF message that includes a cryptographically secure OTP encoded as an NDEF text tag.

[0072] 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 operable 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 operable to add one or more static tag records in addition to the OTP record.

[0073] In some examples, the one or more applets 440 may be operable to emulate a radio frequency identification (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 RFID tag may be processed, the data may be transmitted to a server, such as the server 120, and the data may be validated at the server.

[0074] In some examples, the contactless card 101/101′ and server 120 may include certain data such that the card may be properly identified. The contactless card 101/101′ may include one or more unique identifiers (not pictured). Each time a read operation takes place, the counters 404 may be operable to increment. In some examples, each time data from the contactless card 101/101′ is read (e.g., by a mobile device 110), the counter 404 is transmitted to the server for validation and determines whether the counter values 404 are equal (as part of the validation).

[0075] The one or more counters 404 may be operable to prevent a replay attack. For example, if a cryptogram has been obtained and replayed, that cryptogram is immediately rejected if the counter 404 has been read or used or otherwise passed over. If the counter 404 has not been used, it may be replayed. In some examples, the counter that is incremented on the card is different from the counter that is incremented for transactions. The contactless card 101/101′ is unable to determine the application transaction counter 404 since there is no communication between applets 440 on the contactless card 101/101′. In some examples, the contactless card 101/101′ may include a first applet, which may be a transaction applet, and a second applet. Each of the first applet and the second applet may include a respective counter 404.

[0076] In some examples, the counter 404 may become unsynchronized with the server, such as 120 of Figure 1. In some examples, to account for accidental reads that initiate transactions, such as reading at an angle, the counter 404 may increment but the application does not process the counter 404. In some examples, when the mobile device 110 is woken up, the card reader 148 (which in this example operates as an NFC device) may be enabled and the mobile device 110 may be operable to read available tags, but no action is taken responsive to the reads.

[0077] To keep the counter 404 in synchronization, an application, such as a background application, may be executed that would be operable to detect when the mobile device 110 wakes up and synchronize with the server 120 indicating that a read that occurred due to detection to then increment the counter 404. In other examples, Hashed One Time Password may be utilized such that a window of mis-synchronization may be accepted. For example, if within a threshold of 10, the counter 404 may be operable to move forward. But if within a different threshold number, for example within 10 or 1000, a request for performing re-

synchronization may be processed which requests via one or more applications that the user tap, gesture, or otherwise indicate one or more times via the user's device. If the counter 404 increases in the appropriate sequence, then it possible to know that the user has done so.

[0078] The key diversification technique described herein with reference to elements of Figures 1A and 1B, such as the counter 104, master key 105, and diversified key 106 is one example of encryption and/or decryption a key diversification technique. This example key diversification technique should not be considered limiting of the disclosure, as the disclosure is equally applicable to other types of key diversification techniques.

[0079] During the creation process of the contactless card 101/101′, two cryptographic keys may be assigned uniquely per card. The cryptographic keys may include 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 101/101′. 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.

[0080] 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 101/101′ 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 404 with one or more algorithms (as defined in EMV 4.3 Book 2 A1.3.1 Common Session Key Derivation).

[0081] Further, the counter increment for each card 101/101′ may be unique, and assigned either by personalization, or algorithmically assigned by some identifying information. For example, contactless cards 101/101′ ending in odd number may be operable to increment counters by 2 and contactless cards 101/101′ ending in even numbered cards may increment counters by 5. In some examples, the increment may also vary in sequential reads, such that one card may increment counters in sequence by 1, 3, 5, 2, 2, … repeating. The specific sequence or algorithmic sequence may be defined at time of issuance or another personalization time, or from one or more processes derived from unique identifiers. The specific sequence or algorithmic sequence can make it harder for a replay attacker to generalize from a small number of card instances.

[0082] 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.

[0083] If the tap of the contactless card 101 is directed to a device running Apple's iOS® operating system, e.g., an iPhone, iPod, or iPad, the contactless card can recognize the iOS® operating system and transmit data appropriate data to communicate with this device. For example, the contactless card contactless cards 101/101′ ending in can provide the encrypted identity information necessary to authenticate the card using NDEF tags via, e.g., NFC. Similarly, if the contactless card tap is directed to a mobile device 110 running the Android® operating system, e.g., an Android® smartphone or tablet, the contactless card contactless cards 101/101′ ending in can recognize the Android® operating system and transmit appropriate and data to communicate with this device (such as the encrypted identity information necessary for authentication by the methods described herein).

[0084] Figure 5 illustrates an example of an exemplary computing architecture 500 comprising a computing system 502 that may be suitable for implementing various examples as previously described. In various examples, the computing architecture 500 may include or be implemented as part of an electronic device. In some examples, the computing architecture 500 may be representative, for example, of a system that implements one or more components of the system 100. In some examples, computing system 502 may be representative, for example, of the mobile devices 110 and server 120 of the system 100. The examples are not limited in this context. More generally, the computing architecture 500 is operable to implement all logic, applications, systems, methods, apparatuses, and functionality described herein with reference to Figures 1-6.

[0085] 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 500. 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 examples, 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.

[0086] The computing system 502 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 examples, however, are not limited to implementation by the computing system 502.

[0087] As shown in Figure 5, the computing system 502 includes a processor 504, a system memory 506 and a system bus 508. The processor 504 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 multiprocessor architectures may also be employed as the processor 504.

[0088] The system bus 508 provides an interface for system components including, but not limited to, the system memory 506 to the processor 504. The system bus 508 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 508 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.

[0089] The system memory 506 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 example shown in Figure 5, the system memory 506 can include non-volatile memory 510 and/or volatile memory 512. A basic input/output system (BIOS) can be stored in the non-volatile memory 510.

[0090] The computing system 502 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) 514, a magnetic floppy disk drive (FDD) 516 to read from or write to a removable magnetic disk 518, and an optical disk drive 520 to read from or write to a removable optical disk 522 (e.g., a CD-ROM or DVD). The HDD 514, FDD 516 and optical disk drive 520 can be connected to the system bus 508 by an HDD interface 524, an FDD interface 526 and an optical drive interface 528, respectively. The HDD interface 524 for external drive implementations can include at least one or both of Universal Serial Bus (USB) and IEEE 1394 interface technologies. The computing system 502 is generally is operable to implement all logic, systems, methods, apparatuses, and functionality described herein with reference to Figures 1-7.

[0091] 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 510, 512, including an operating system 530, one or more application programs 532, other program modules 534, and program data 536. In one example, the one or more application programs 532, other program modules 534, and program data 536 can include, for example, the various applications and/or components of the system 100, e.g., the operating system 142, account authentication application 143, unlock-lock application 144, other applications 145 and the management application 123.

[0092] A user can enter commands and information into the computing system 502 through one or more wire/wireless input devices, for example, a keyboard 538 and a pointing device, such as a mouse 540. 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 504 through an input device interface 542 that is coupled to the system bus 508 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.

[0093] A monitor 544 or other type of display device is also connected to the system bus 508 via an interface, such as a video adaptor 546. The monitor 544 may be internal or external to the computing system 502. In addition to the monitor 544, a computer typically includes other peripheral output devices, such as speakers, printers, and so forth.

[0094] The computing system 502 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 548. The remote computer 548 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 502, although, for purposes of brevity, only a memory/storage device 550 is illustrated. The logical connections depicted include wire/wireless connectivity to a local area network (LAN) 552 and/or larger networks, for example, a wide area network (WAN) 554. 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 examples, the network 130 of Figure 1 is one or more of the LAN 552 and the WAN 554.

[0095] When used in a LAN networking environment, the computing system 502 is connected to the LAN 552 through a wire and/or wireless communication network interface or adaptor 556. The adaptor 556 can facilitate wire and/or wireless communications to the LAN 552, which may also include a wireless access point disposed thereon for communicating with the wireless functionality of the adaptor 556.

[0096] When used in a WAN networking environment, the computing system 502 can include a modem 558, or is connected to a communications server on the WAN 554 or has other means for establishing communications over the WAN 554, such as by way of the Internet. The modem 558, which can be internal or external and a wire and/or wireless device,

connects to the system bus 508 via the input device interface 542. In a networked environment, program modules depicted relative to the computing system 502, or portions thereof, can be stored in the remote memory/storage device 550. 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.

[0097] The computing system 502 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).

[0098] FIG. 6 illustrates an example of a mobile device usable for implementing the techniques and processes discussed with reference to the examples of FIGs. 1-5.

[0099] The mobile device 611 may be a smart phone including a display device, such as a touch screen display 620. The touch screen display 620 may be coupled to the processor 612 and be operable to present screen content and receive inputs via touch sensors 622. Examples of touch screen type mobile devices, such as mobile device 611, may include (but are not limited to) a smart phone, personal digital assistant (PDA), tablet computer, smart watch, or another portable device. However, the structure and operation of mobile device 611 that utilizes a touch screen is provided by way of example; and the subject technology as described herein is not intended to be limited thereto. For purposes of this discussion, FIG. 6 provides a block diagram illustration of an example of the mobile device 611 having a touch screen display for displaying content and receiving user input as (or as part of) the user interface.

[00100] There are a variety of ways that a mobile device 611 may be operable to obtain information as to current location of the device. In our example, the mobile device 611 includes a global positioning satellite (GPS) receiver 632 and associated antenna 634. GPS is a space-based satellite navigation system that provides location and time information practically anywhere on Earth. A rechargeable battery 629 may provide electrical power sufficient to power the various components of the mobile device 611.

[00101] A mobile device supporting the sale notification application and techniques described herein may include a variety of different types of user interface elements. For discussion purposes, in the smart phone example of a mobile device shown in FIG. 6, the user interface elements of mobile device 611 include a touch screen display 620 (also referred to herein as "touch screen 620" or "display 620"). For output purposes, the touch screen 620 includes a display screen, such as a liquid crystal display (LCD) or the like. For input purposes, touch screen display 620 includes a plurality of touch sensors 622. Other interface elements may include a keypad including one or more keys 630. For example, the keypad may be implemented in hardware as a T9 or QWERTY keyboard of mobile device 611 and keys 630 may correspond to the physical keys of such a keyboard. Alternatively, keys 630 (and keyboard) of mobile device 611 may be implemented as "soft keys" of a virtual keyboard graphically represented in an appropriate arrangement via touch screen display 620. The soft keys presented on the touch screen display 620 may allow the user of mobile device 611 to invoke the same user interface functions as with the physical hardware keys. In some implementations, the microphone 602 and speaker 604 may be used as additional user interface elements, for audio input and output, including with respect to some functions related to the processing related to engaging with the sale notification application 647, as described herein. In a further example, the sale notification application 647 may in response to accessing contacts stored in the mobile device memory 614, present in the user interface, such as 425 of FIG. 4B, a prompt to send a request to one or more of the contacts to join an affinity reward group.

[00102] For output, touch screen display 620 is a display device used to present information (e.g., text, video, graphics or other visible content) to the user of mobile device 611. Processor 612 controls visible display output on the LCD or other display element of the touch screen display 620 via a display driver 624, to present the various visible outputs to the device user. In addition, an output device may include for example, a speaker 604, a vibration mechanism 631, the touchscreen display 620, or the like.

[00103] In general, touch screen display 620 and touch sensors 622 (and one or more keys 630, if included) are used to provide the textual and graphical user interface for the mobile device 611. In an example, touch screen display 620 provides viewable content to the user at mobile device 611. Touch screen display 620 also enables the user to interact directly with the viewable content provided in the content display area, typically by touching the surface of the screen with a finger or an implement such as a stylus.

[00104] As shown in FIG. 6, the mobile device 611 also includes a touch detect circuit 628 coupled to touch sensors 622 for detecting the occurrence and relative location/position of each touch with respect to a content display area of touch screen display 620. In this example, touch detect circuit 628 is operable to provide processor 612 with touch-position information based on user input received via touch sensors 622. In some implementations, processor 612 is operable to correlate the touch position information to specific content being displayed within the content display area on touch screen display 620. The touch-position information captured by touch detect circuit 628 and provided to processor 612 may include, but is not limited to, coordinates identifying the location of each detected touch with respect to the display area of touch screen display 620 and a timestamp corresponding to each detected touch position.

[00105] In the example shown in FIG. 6, the mobile device 611 includes a microphone 602 for audio signal input and a speaker 604 for audio signal output. The microphone 602 and speaker 604 are communicatively coupled to a voice or audio encoder/decoder (vocoder) 606. For a voice telephone call, for example, the vocoder 606 provides two-way conversion between analog audio signals representing speech or other audio and digital samples at a compressed bit rate compatible with the digital protocol of wireless telephone network communications or voice over packet (e.g., Internet Protocol) communications. The vocoder, speaker and microphone may also be used as elements of the user interface during other operations of the device, including some types of transaction communications.

[00106] Also, as shown in FIG. 6, the mobile device 611 includes at least one transceiver (XCVR) 608, which may be a digital transceiver for digital wireless communications via a wide area wireless mobile communication network, although the mobile device 611 may include additional digital or analog transceivers (not shown). The transceiver 608 conforms to one or more of the various digital wireless communication standards utilized by modern mobile networks. Examples of such transceivers include (but are not limited to) transceivers operable to operate in accordance with Code Division Multiple Access (CDMA) and 3rd Generation Partnership Project (3GPP) network technologies including, for example and without limitation, 3GPP type 2 (or 3GPP2) and 3GPP Long Term Evolution (LTE), at times referred to as "4G." For example, transceiver 608 provides two-way wireless communication of information including digitized audio signals, still image and/or video signals, web page information for display as well as web related inputs, and various types of mobile message communications to/from the mobile device 611. Transceiver 608 connects through radio frequency (RF) send-and-receive amplifiers (not separately shown) to an antenna 609.

Transceiver 608 may also support various types of mobile messaging services, such as short message service (SMS), enhanced messaging service (EMS), and/or multimedia messaging service (MMS).

[00107] In an example, the transceiver 608 may be coupled to the processor 612 and operable to exchange communications. The processor 612 of the mobile device 611 may be further operable to perform additional functions, including functions to establish, using the transceiver, a connection with a server, such as affinity exchange server 45 of FIG. 1, to exchange communications. Via the connection with the server, the mobile device 611 may be able to obtain various information, such as an affinity reward exchange rate, a neutral affinity reward value, affinity aggregation account-related information, and the like. The processor upon execution of the sale notification application 647 may implement the examples as discussed above with reference to FIGs. 1-5.

[00108] The mobile device 611 may also include a Wi-Fi transceiver 610 and associated antenna 633. Although Wi-Fi is used here as the example, the transceiver 610 may take the form of any available two-way wireless local area network transceiver of a type that is compatible with one or more standard protocols of communication implemented in wireless local area networks, such as one of the Wi-Fi standards under IEEE 802.11 and/or WiMAX.

[00109] The mobile device 611 further includes a processor 612, which serves as a programmable controller for mobile device 611 by configuring mobile device 611 to perform various operations, for example, in accordance with instructions or programming executable by processor 612. For example, such operations may include various general operations of the mobile device 611 as well as operations related to the screen brightness adjustment as described herein. A flash memory 614 may be used to store, for example, programming or instructions for execution by the processor 612. Depending on the type of device, the mobile device 611 stores and runs an operating system through which specific applications may be run on the device. Examples of operating systems include Android, Apple iOS, Microsoft Windows OS, Bada, Tizen, Symbian OS, Blackberry OS, or the like. Flash memory 614 may also be used to store mobile configuration settings for different mobile applications or services executable at mobile device 611 (using processor 612). Mobile device 611 may also include a non-volatile random-access memory (RAM) 616 for a working data processing memory. The RAM memory 616 or storage 637 may be coupled to the processor 612 and operable to store programming code executable by the 612 processor.

[00110] Alternatively, or in addition, applications may be stored in storage 637, which may be a solid-state memory storage or other memory device suitable for storing applications. In one example, the storage 637 may be a separate chip that includes tamperproof storage and execution memory and is operable to communicate with operating system. The storage 637 may, for example, store an instance of a sale notification application 647 for processing receipt data, communicating with one or more services or servers, and processes as described with reference to the examples of FIGs. 1-3. Other applications such as 642 and 644 may also be stored in storage 637.

[00111] The logic implemented by the processor 612 of the mobile device 611 configures the processor 612 to control various functions as implemented by the mobile device 611. The logic for a processor may be implemented in a variety of ways, but in the presented examples, the processor logic is implemented by programming for execution by the processor 612.

[00112] Various examples 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, application program interfaces (API), instruction sets, computing code, computer code, code segments, computer code segments, words, values, symbols, or any combination thereof. Determining whether an example 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.

[00113] One or more aspects of at least one example 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 examples 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 operations in accordance with the examples. 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.

[00114] The foregoing description of examples 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.