

ASSIGNMENT OF NEAR-FIELD COMMUNICATIONS APPLETS**CROSS-REFERENCE TO RELATED APPLICATIONS**

[0001] This application claims priority to U.S. Patent Application Serial No. 18/462,714, filed September 07, 2023, the disclosure of which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] This disclosure relates generally to data processing and, in particular, to contactless cards, and more particularly, to use of contactless cards and mobile applications for selection and use of methods of payment for transactions.

BACKGROUND

[0003] Tap-to-pay transactions have become some of the most popular ways of paying for goods and services. Tap-to-pay is based on radio-frequency identification (RFID) technology that may be embedded into credit cards, smartphones, and other mobile devices. This technology allows users to make credit card transactions by bringing their cards and/or smartphones within a specific distance of (or tapping on) specific areas of point-of-sale terminals, which enables transfer of certain data for the purposes of making a payment. However, existing systems do not allow for displaying and selection of methods of payment for a transaction.

SUMMARY

[0004] In some implementations, the current subject matter relates to a computer-implemented method for using contactless cards and mobile applications for selection and use of

methods of payment for transactions. The method may include receiving, using at least one processor, an identifier associated with a transaction. The transaction may be configured to be executed using at least one computing device communicatively coupled to at least one processor. The method may further include generating, using the received identifier, one or more virtual identifiers, selecting at least one virtual identifier in one or more virtual identifiers, assigning the selected at least one virtual identifier to the transaction, and triggering execution of the transaction by at least one computing device using the assigned at least one virtual identifier.

[0005] In some implementations, the current subject matter may include one or more of the following optional features. The receiving may include receiving the identifier from a contactless card communicatively coupled to at least one processor, the contactless card storing the identifier. The receiving may also include executing a near-field communication (NFC) exchange between the contactless card and at least one processor upon the contactless card being detected by at least one processor to be located within a predetermined distance of at least one processor.

[0006] In some implementations, executing the NFC exchange may include triggering at least one processor to generate at least one user interface, at least one user interface receiving an input triggering the selecting. The received identifier may include a contactless card number. The contactless card number may be associated with one or more financial accounts. The generated user interface may be configured to display each financial account in one or more financial accounts in response to the executing of the NFC exchange. The generated virtual identifiers may correspond to one or more financial accounts.

[0007] In some implementations, the contactless card may include at least one of the following: a credit card, a debit card, an electronic gift card, a pre-paid credit card, a pre-paid debit card, and any combination thereof.

[0008] In some implementations, the current subject matter relates to a system for using contactless cards and mobile applications for selection and use of methods of payment for transactions. The system may include a mobile device including at least one processor and at least one non-transitory storage media storing instructions, that when executed by at least one processor, may cause the processor to perform one or more of the following operations. The operations may include generating one or more virtual identifiers using one or more identifiers associated with a transaction. The transaction may be configured to be executed using at least one computing device communicatively coupled to the mobile device. One or more identifiers may be received from a contactless card communicatively coupled to the mobile device. The operations may further include triggering execution of the transaction by at least one computing device using at least one virtual identifier in one or more virtual identifiers.

[0009] In some implementations, the current subject matter may include one or more of the following optional features. At least one virtual identifier may be selected from one or more virtual identifiers and assigned to the transaction. The contactless card may be configured to store one or more identifiers. In some implementations, a near-field communication (NFC) exchange may be configured to be executed between the contactless card and the mobile device upon the contactless card being detected by the mobile device to be located within a predetermined distance of the mobile device. Execution of the NFC exchange may trigger the mobile device to generate at least one user interface. The user interface may be configured to receive an input triggering selection of at least one virtual identifier from one or more virtual identifiers. One or more

identifiers may include a contactless card number. The contactless card number may be associated with one or more financial accounts. At least one user interface may be configured to display each financial account in one or more financial accounts in response to execution of the NFC exchange. One or more virtual identifiers may correspond to one or more financial accounts. The contactless card may include at least one of the following: a credit card, a debit card, an electronic gift card, a pre-paid credit card, a pre-paid debit card, and any combination thereof.

[0010] In some implementations, the current subject matter relates to a computer program product including a non-transitory machine-readable medium storing instructions that, when executed by at least one programmable processor, cause at least one programmable processor to perform one or more of the following operations. The operations may include executing a near-field communication (NFC) exchange between a contactless card and a mobile device upon the contactless card being detected by the mobile device to be located within a predetermined distance of the mobile device, receiving, in response to the executing of the NFC exchange, from the contactless card, one or more identifiers associated with a transaction, where the transaction may be configured to be executed using at least one computing device communicatively coupled to the mobile device, generating one or more virtual identifiers using one or more identifiers associated with the transaction, where one or more virtual identifier being associated with one or more financial accounts, and displaying one or more financial accounts on a user interface of the mobile device, selecting at least one virtual identifier in one or more virtual identifiers, and assigning the selected at least one virtual identifier to the transaction, and triggering execution of the transaction by at least one computing device using the assigned at least one virtual identifier.

[0011] In some implementations, the current subject matter include one or more of the following optional features. One or more identifiers include a contactless card number. The

contactless card may include at least one of the following: a credit card, a debit card, an electronic gift card, a pre-paid credit card, a pre-paid debit card, and any combination thereof.

[0012] Non-transitory computer program products (i.e., physically embodied computer program products) are also described that store instructions, which when executed by one or more data processors of one or more computing systems, causes at least one data processor to perform operations herein. Similarly, computer systems are also described that may include one or more data processors and memory coupled to the one or more data processors. The memory may temporarily or permanently store instructions that cause at least one processor to perform one or more of the operations described herein. In addition, methods can be implemented by one or more data processors either within a single computing system or distributed among two or more computing systems. Such computing systems can be connected and can exchange data and/or commands or other instructions or the like via one or more connections, including but not limited to a connection over a network (e.g., the Internet, a wireless wide area network, a local area network, a wide area network, a wired network, or the like), via a direct connection between one or more of the multiple computing systems, etc.

[0013] The details of one or more variations of the subject matter described herein are set forth in the accompanying drawings and the description below. Other features and advantages of the subject matter described herein will be apparent from the description and drawings, and from the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The accompanying drawings, which are incorporated in and constitute a part of this specification, show certain aspects of the subject matter disclosed herein and, together with the

description, help explain some of the principles associated with the disclosed implementations. In the drawings,

[0015] FIG. 1 illustrates an example system for execution of a transaction, according to some implementations of the current subject matter;

[0016] FIG. 2 illustrates an example operation of an account selection engine of the mobile device shown in FIG. 1, according to some implementations of the current subject matter;

[0017] FIG. 3 illustrates a sequence diagram representing an example process for executing a transaction, according to some implementations of the current subject matter;

[0018] FIG. 4 illustrates an example of a graphical applet or graphical user interface that may be displayed on the mobile device shown in FIG. 1, according to some implementations of the current subject matter;

[0019] FIG. 5 illustrates an example process for execution of a transaction, according to some implementations of the current subject matter;

[0020] FIG. 6 illustrates another example process for execution of a transaction, according to some implementations of the current subject matter;

[0021] FIG. 7 illustrates yet another example process for execution of a transaction, according to some implementations of the current subject matter;

[0022] FIG. 8 illustrates an aspect of the subject matter in accordance with some implementations;

[0023] FIG. 9 illustrates an aspect of the subject matter in accordance with some implementations;

[0024] FIG. 10 illustrates a contactless card, according to some implementations of the current subject matter;

[0025] FIG. 11 illustrates a transaction card component, according to some implementations of the current subject matter;

[0026] FIG. 12 illustrates a sequence flow, according to some implementations of the current subject matter;

[0027] FIG. 13 illustrates a data structure, according to some implementations of the current subject matter;

[0028] FIG. 14 is a diagram of a key system, according to some implementations of the current subject matter;

[0029] FIG. 15 is a flowchart of a method of generating a cryptogram, according to some implementations of the current subject matter;

[0030] FIG. 16 illustrates an aspect of the subject matter in accordance with some implementations; and

[0031] FIG. 17 illustrates an aspect of the subject matter in accordance with some implementations.

DETAILED DESCRIPTION

[0032] To address these and potentially other deficiencies of currently available solutions, one or more implementations of the current subject matter relate to methods, systems, articles of manufacture, and the like that can, among other possible advantages, provide an ability to execute transactions through selection of specific financial accounts.

[0033] In some implementations, the current subject matter generally relates to an ability to use a contactless card and a mobile device to select a specific financial account to execute (e.g., pay for) a transaction (e.g., at a point-of-sale terminal). For example, a user of the contactless card and/or the mobile device may have and use a variety of financial accounts at different (or same) financial institutions (e.g., credit card companies, banks, etc.). The contactless card may be a credit card, a debit card, an electronic gift card, a pre-paid credit card, a pre-paid debit card, and/or any other card, and/or any combination thereof. The user may use user's financial accounts for transaction payments (e.g., purchasing, bill payments, etc.), transfer of funds, and/or any other executions of financial transactions, and/or for any other purpose. When executing financial transactions (e.g., a purchase at point-of-sale terminal at retailer 1), the user may select a particular account (e.g., credit card no. 1) from user's financial accounts for such transaction. Similarly, when executing another financial transaction (e.g., a payment of a bill at a utility company 1), the user may select another account (e.g., checking account) from user's financial accounts for completion of that transaction.

[0034] To perform selection of an account, the user of the contactless card and the mobile device (e.g., mobile telephone, smartphone, smart tablet, etc.) may tap the card on the mobile device. Such tapping may prompt the mobile device to obtain information from the contactless card. In some implementations, the current subject matter may be configured to execute a near field communication (NFC) exchange between the contactless card and the mobile device, upon the mobile device detecting that the contactless card is located within a predetermined distance, area, boundary, etc. from the mobile device. The mobile device may be configured to act as an "active" component and provide power to energize the contactless card, which may be considered as a "passive" component. The NFC exchange may be configured to trigger opening of a user

interface containing the applet on the mobile device and/or displaying one or more user's financial accounts for use in executing the transaction.

[0035] In some implementations, upon detecting the contactless card within a predetermined distance, area, boundary, etc. of the mobile device, the mobile device may request and/or be automatically provided with various identification data from the contactless card. The card's identification data may include various information identifying the card and/or the user of the card. It may include one or more identifiers that may be used to identify the card. The contactless card may also transmit various contactless card data. The contactless card data may include the contactless card data includes at least one of the following: an account number associated with the contactless card, an expiration date associated with the contactless card, a card verification value (CVV) associated with the contactless card, a billing address associated with the contactless card, a name of a user associated with the contactless card, and any combination thereof. In some implementations, the mobile device may be configured to store the received contactless card data and/or transmit it to one or more servers (e.g., servers that may be communicatively coupled to the mobile device and associated with the financial institution that issued the card).

[0036] The mobile device may then use the contactless card information to generate a user interface (e.g., an applet) that may display user's various financial accounts. For example, the mobile device may use the contactless card information to retrieve user's financial accounts information from various financial institutions and then display them in the generated user interface. The mobile device may also indicate which of the displayed accounts (some and/or all) may be used for transaction execution. For example, the mobile device may display available

balances for each account, which may assist the user with making a selection of a specific financial account for transaction execution.

[0037] Once the accounts are presented in the generated user interface, the mobile device may generate and assign one or more virtual account numbers/identifiers to each displayed financial account. The user may then select (e.g., by tapping on a specific financial account with user's finger, palm, etc.) a particular financial account on the user interface that the user desires to use in connection with execution of the transaction. The virtual account number associated with the selected financial account may be transmitted to a computing device (e.g., point-of-sale terminal) executing the transaction (e.g., payment for a purchase).

[0038] In some implementations, the contactless card may be automatically detected by the mobile device upon coming within a predetermined area, distance, and/or boundary around the mobile device. Such area/distance/boundary may be determined by the NFC protocols. Once the contactless card has been detected by the mobile device, the mobile device may generate the above applet and display financial accounts.

[0039] FIG. 1 illustrates an example system 100 for execution of a transaction, according to some implementations of the current subject matter. The system 100 may include a contactless card 102, a mobile device 104 having a near-field communications boundary 114, a computing device 108 that may execute a transaction, one or more servers 110 (a, b...c) associated with financial institutions holding user's financial accounts, and one or more servers 112 associated with the computing device 108.

[0040] One or more components of the system 100 may be communicatively coupled using one or more communications networks. The communications networks may include one or more of the following: a wired network, a wireless network, a metropolitan area network ("MAN"), a

local area network ("LAN"), a wide area network ("WAN"), a virtual local area network ("VLAN"), an internet, an extranet, an intranet, and/or any other type of network and/or any combination thereof.

[0041] Further, one or more components of the system 100 may include any combination of hardware and/or software. In some implementations, one or more components of the system 100 may be disposed on one or more computing devices, such as, server(s), database(s), personal computer(s), laptop(s), cellular telephone(s), smartphone(s), tablet computer(s), virtual reality devices, and/or any other computing devices and/or any combination thereof. In some example implementations, one or more components of the system 100 may be disposed on a single computing device and/or may be part of a single communications network. Alternatively, or in addition to, such services may be separately located from one another. A service may be a computing processor, a memory, a software functionality, a routine, a procedure, a call, and/or any combination thereof that may be configured to execute a particular function associated with the current subject matter lifecycle orchestration service(s).

[0042] In some implementations, the system 100's one or more components may include network-enabled computers. As referred to herein, a network-enabled computer may include, but is not limited to a computer device, or communications device including, e.g., a server, a network appliance, a personal computer, a workstation, a phone, a smartphone, a handheld PC, a personal digital assistant, a thin client, a fat client, an Internet browser, or other device. One or more components of the system 100 also may be mobile computing devices, for example, an iPhone, iPod, iPad from Apple® and/or any other suitable device running Apple's iOS® operating system, any device running Microsoft's Windows®. Mobile operating system, any device running Google's

Android® operating system, and/or any other suitable mobile computing device, such as a smartphone, a tablet, or like wearable mobile device.

[0043] One or more components of the system 100 may include a processor and a memory, and it is understood that the processing circuitry 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. One or more components of the environment 100 may further include one or more displays and/or one or more input devices. The displays may be any type of devices for presenting visual information such as a computer monitor, a flat panel display, and a mobile device screen, including liquid crystal displays, light-emitting diode displays, plasma panels, and cathode ray tube displays. The input devices may include any device for entering information into the user's device that is available and supported by the user's device, such as a touch-screen, keyboard, mouse, cursor-control device, touch-screen, microphone, digital camera, video recorder or camcorder. These devices may be used to enter information and interact with the software and other devices described herein.

[0044] In some example implementations, one or more components of the environment 100 may execute one or more applications, such as software applications, that enable, for example, network communications with one or more components of environment 100 and transmit and/or receive data.

[0045] One or more components of the environment 100 may include and/or be in communication with one or more servers via one or more networks and may operate as a respective front-end to back-end pair with one or more servers. One or more components of the environment 100 may transmit, for example from a mobile device application (e.g., executing on one or more

user devices, components, etc.), one or more requests to one or more servers (e.g., server(s) 106). The requests may be associated with retrieving data from servers. The servers may receive the requests from the components of the system 100. Based on the requests, servers may be configured to retrieve the requested data from one or more databases (e.g., database 110, as shown in FIG. 1). Based on receipt of the requested data from the databases, the servers may be configured to transmit the received data to one or more components of the system 100, where the received data may be responsive to one or more requests.

[0046] The system 100 may include one or more networks, such as, for example, networks that may be communicatively coupling the mobile device 104, the computing device 108 and/or one or more servers 110 and/or 112. In some implementations, networks may be one or more of a wireless network, a wired network or any combination of wireless network and wired network and may be configured to connect the components of the system 100 and/or the components of the system 100 to one or more servers. For example, the networks may include one or more of a fiber optics network, a passive optical network, a cable network, an Internet network, a satellite network, a wireless local area network (LAN), a metropolitan area network (MAN), a wide area network (WAN), a virtual local area network (VLAN), an extranet, an intranet, a Global System for Mobile Communication, a Personal Communication Service, a Personal Area Network, Wireless Application Protocol, Multimedia Messaging Service, Enhanced Messaging Service, Short Message Service, Time Division Multiplexing based systems, Code Division Multiple Access based systems, D-AMPS, Wi-Fi, Fixed Wireless Data, IEEE 802.11b, 802.15.1, 802.11n and 802.11g, Bluetooth, NFC, Radio Frequency Identification (RFID), Wi-Fi, and/or any other type of network and/or any combination thereof.

[0047] In addition, the networks may include, without limitation, telephone lines, fiber optics, IEEE Ethernet 802.3, a wide area network, a wireless personal area network, a LAN, or a global network such as the Internet. Further, the networks may support an Internet network, a wireless communication network, a cellular network, or the like, or any combination thereof. The networks may further include one network, or any number of the exemplary types of networks mentioned above, operating as a stand-alone network or in cooperation with each other. The networks may utilize one or more protocols of one or more network elements to which they are communicatively coupled. The networks may translate to or from other protocols to one or more protocols of network devices. The networks may include a plurality of interconnected networks, such as, for example, the Internet, a service provider's network, a cable television network, corporate networks, such as credit card association networks, and home networks.

[0048] The system 100 may include one or more servers, which may include one or more processors that maybe coupled to memory. Servers may be configured as a central system, server or platform to control and call various data at different times to execute a plurality of workflow actions. Servers may be configured to connect to the one or more databases. Servers may be incorporated into and/or communicatively coupled to at least one of the components of the system 100.

[0049] One or more components of the system 100 may be configured to execute one or more transactions using one or more containers. In some implementations, each transaction may be executed using its own container. A container may refer to a standard unit of software that may be configured to include the code that may be needed to execute the action along with all its dependencies. This may allow execution of actions to run quickly and reliably.

[0050] In some implementations, as discussed above, the system 100 may be used for execution of a transaction using a financial account that may be selected from an applet generated by the mobile device 104. In particular, the account selection process and subsequent execution of the transaction may be initiated using near-field communications (NFC) exchange link between the contactless card 102 and the mobile device 104. To enable use of the NFC technology, a user (not shown in FIG. 1) may bring the contactless card 102 within the area 114 of the mobile device 104 (e.g., tap the card 102 on the mobile device 104 or hold the card 102 near the mobile device 104 without tapping), whereby the mobile device 104 may be configured to detect presence of the contactless card 102 within the area 114 and execute one or more operations discussed herein.

[0051] In the NFC exchange link, the mobile device 104 may be configured to act as an active component and provide power to energize the contactless card 102 (as discussed herein), which may be a passive component. Using the NFC exchange link, the mobile device 104 and the contactless card 102 may be configured to exchange various data, such as, for instance, for the purposes of identification of financial accounts and selections thereof for the purposes of transaction execution.

[0052] In some implementations, as discussed herein, the mobile device 104 may be securely linked to user's financial accounts at various financial institutions. Each financial institution may include one or more servers 110 (a, b, ...c), as shown in FIG. 1, with which the mobile device 104 may communicate to exchange various data associated with one or more of user's financial accounts. The contactless card 102 may likewise be securely linked to one of user's financial accounts. The linking of the mobile device 104 and the financial accounts may be configured to allow the mobile device 104 to display in an applet available financial accounts for user's selection to use in transaction execution. Access to the financial accounts from the mobile

device 104 may be secured/protected using various authentication/authorization mechanisms (e.g., a facial recognition data, a fingerprint data, a biometric data, a username and a password, a multi-factor authentication token, and any combination thereof, etc.).

[0053] Once the mobile device 104 detected the contactless card 102 within the area 114, the mobile device 104, using the NFC exchange link, may be configured to request and/or be automatically provided with various identification data from the contactless card 102. The identification data may include various information identifying the card and/or the user of the card (e.g., one or more identifiers, etc.).

[0054] In some implementations, to access a specific financial account (e.g., upon user selecting such account), the user may also be prompted to provide user authentication information. Such information may include, but is not limited to, one or more authentication keys, and/or data and/or information, such as, for example, a facial recognition data, a fingerprint data, a biometric data, a username and a password, a multi-factor authentication token, and any combination thereof. The mobile device 104 may be configured to generate an appropriate prompt requesting the user to provide authentication information. Once the information is provided, the mobile device 104 may transmit this information to one or more servers 110 (a, b, ...c) for verification. Once verified, the servers 110 (a, b, ...c) may transmit an indication that verification was successful and the account may be available for use in the transaction. Otherwise, the servers may transmit an indication the verification was not successful and access to the account may be blocked at this time, thereby preventing use of the account in the transaction.

[0055] To execute a transaction with the computing device 108 (e.g., a purchasing transaction at a point-of-sale terminal), the mobile device 104 may be configured to communicate with the computing device 108 and receive details of the transaction. The details may include

transaction identification information, computing device 108 identification information, amount(s) involved, terms of the transaction, and/or any other information that may be needed to execute such transaction. The computing device 108 may transmit this information to the mobile device 104 upon receiving an appropriate request from the mobile device 104. The computing device 108 and the mobile device 104 may be located proximate to one another and/or at any desired distance away (e.g., the mobile device 104 may be used to execute a transaction with the computing device 108 over the internet).

[0056] Upon receiving the transaction details from the computing device 108, the mobile device 104, using its account selection engine 106, may generate a prompt to the user to tap the contactless card 102 so that selection of one or more financial accounts for execution of the transaction may take place. Alternatively, the financial accounts may already be displayed in a graphical applet and/or any other graphical user interface (e.g., as shown in FIG. 4) of the mobile device 104 prior to receiving transaction details from the computing device 108. The applet may be generated by the account selection engine 106.

[0057] In some implementations, bringing the contactless card 102 within the area 114 of the mobile device 104 may cause the account selection engine 106 to automatically generate such graphical applet and/or any other graphical user interface populated with available user's financial accounts, as for example, is shown in FIG. 4. The mobile device 104, using the engine 106, may request the identification information from the contactless card 102 and, upon receiving it, may send it to one or more servers 110 (a, b, ..., c). In response, one or more of the servers 110 may respond with information relating to available user's financial account (e.g., name of the account, account number, balance information, credit limit, authorization requirements, etc.). The engine 106 of the mobile device 104 may then process the received financial accounts information and

display it in the generated applet. The mobile device 104 may also prompt the user to select one or more of the accounts for execution of the transaction with the computing device 108. In some example implementations, the mobile device 104, upon receiving user's selection of a particular financial account, may request the user to provide authentication information (e.g., a passcode, a fingerprint and/or any other biometric identification information, etc.) in order to verify user's right to use the accounts.

[0058] Once financial account(s) are selected, and, optionally, their use has been authenticated, the engine 106 of the mobile device 104 may request the user to confirm that the user wishes to execute the transaction. Upon receiving confirmation, the engine 106 of the mobile device 104 may generate a virtual account number and/or identifier (hereinafter, "virtual account number") representative of the selected financial account. The virtual account number may be any random sequence of alpha-numeric characters and may be generated in any desired way. The virtual account number may be configured to hide the actual account information (e.g., account number, name of the user, etc.) associated with the selected financial account.

[0059] The engine 106 of the mobile device 104 may then transmit the generated virtual account number to the computing device 108 for processing of the transaction. The computing device 108 may transmit the received virtual account number to the server 112. The server 112 may be associated with a financial institution that may be servicing one or more financial accounts that may be linked to the computing device 108 (e.g., in a retail purchase transaction, the computing device 108 may represent retailer's point of sale terminal and the server 112 may be associated with banking or financial institution holding one or more financial accounts used by the retailer). The server 112 may be communicatively coupled with one or more servers 110 (a, b, ... c) and may transmit the received virtual account number to one or some or all of the servers 110 (a,

b, ...c) and request verification. In the request, the server 112 may also transmit information about the transaction, such as, for example, transaction description, transaction amount(s), mobile device 104 information, etc.

[0060] In some implementations, the server 112 may use the received virtual account number to determine which sever 110 (a, b, ...c) should be receiving its request. In this case, the virtual account number may be configured to include an identifier of the financial institution corresponding to the selected financial account. Using this identifier, the server 112 may only transmit its request to the specific financial institution identified in the virtual account number.

[0061] Alternatively, or in addition, upon receiving a selection of specific financial account(s), the engine 106 of the mobile device 104 may transmit a request to the specific server(s) 110 (a, b, ...c) that is associated with the financial institution(s) holding the selected financial account(s). The request may include a request to authorize the transaction with the computing device 108. The request may also include a virtual account number corresponding to the selected financial account. Once the request to authorize transaction is received by the specific server(s) 110 (a, b, ...c), the server(s) may transmit an appropriate authorization to the server 112, which may then pass it along to the computing device 108 for completion of the transaction. Alternatively, or in addition, upon receiving the request to authorize transaction, the specific server 110 (a, b, ...c) may generate a virtual account number and transmit it to the server 112, and thus, to the computing device 108.

[0062] In some implementations, the virtual account number (regardless of whether it is generated by the engine 106 of the mobile device 104 and/or the servers 110 (a, b, ...c)) may only be used in connection with the specific transaction with the specific computing device 108. Its use with any other transaction and/or any other computing device may be prohibited. The virtual

account number may also be assigned a predetermined period of time within which it must be used. In this case, if the transaction is not completed within the predetermined period of time, use of such virtual account number may be prevented. This may provide further security to the use of user's financial accounts in connection with transactions. Alternatively, or in addition, virtual account numbers may be reusable and may be used in connection with any other transactions and/or any other computing devices and/or not be limited by a predetermined time of use.

[0063] Upon receiving of the virtual account number, the computing device 108 may complete execution of the transaction. For example, in the retail scenario, completion of execution of the transaction, may involve completion of the purchase transaction. In some implementations, the computing device 108 may transmit a request to the mobile device 104 to confirm use of the virtual account in connection with the transaction. The engine 106 of the mobile device 104 may respond to the computing device 108 with confirmation, after which transaction may be completed. Alternatively, the engine 106 of the mobile device 104 may respond with denial causing transaction to be aborted.

[0064] FIG. 2 illustrates an example operation of the account selection engine 106 of the mobile device 104, according to some implementations of the current subject matter. The engine 106 may include an account identification engine 204 that may be configured to receive details of the transaction 202 and/or information from the contactless card 102. The account identification engine 204 may transmit the received transaction details and/or contactless card information to servers 1, ..., 3 110 (a, b, ...c).

[0065] The servers 110 may respond to the engine 204 with information relating to available user's financial accounts, e.g., account 1 206a, account 2 206b, ..., account 3 206c. The engine 204 may then process the received financial accounts information and display information

related to accounts 206 in a graphical applet or any other graphical user interface 214 of the mobile device 204. For example, account 206a may be a checking account at Capital One Bank, account 206b may be a credit card, and account 206c may be an investment account. Each account may, for example, be identified by the logo associated with the financial institution holding the account, and its listing in the applet may include account number (or partial account number), available balance details, credit line (if any), and/or any other information.

[0066] The engine 204 may then prompt the user to select one of the account 206. This may be accomplished using any desired way (e.g., tapping a finger on the screen of the mobile device, clicking, sliding, etc.). The selected account information 208 may then be transmitted to the virtual account number assignment engine 210. The engine 210 may generate a virtual account number for the selected account. As stated above, the virtual account number may be any combination of alpha-numeric and/or any other characters that may be designed to conceal the actual account number information. The virtual account number may also include one or more identifiers identifying the financial institution associated with the selected account information 208.

[0067] The engine 210 may then transmit the virtual account number information 212 to the computing device 108 for processing of the transaction. Alternatively, or in addition, the engine 210 may also transmit this information to one or more of the servers 110 (as shown in FIG. 1) for verification and/or transmission to the computing device 108, via server 112.

[0068] FIG. 3 illustrates a sequence diagram representing an example process for executing a transaction, according to some implementations of the current subject matter. The process shown in FIG. 3 may be executed using the system 100 shown in FIGS. 1 and 2.

[0069] The contactless card 102 may be configured to transmit a message 302 to the mobile device 104, which may include the account identification engine 204 and the virtual account number assignment engine 210. The contactless card 102 may transmit such message using a near-field communication exchange link that may be established between the mobile device 104 and the contactless card 102 upon contactless card 102 being detected by the mobile device 104 to be within the predetermined area 114 of the mobile device 104.

[0070] The message 302 may include various contactless card 102 information, including but not limited to, an account number associated with the contactless card, an expiration date associated with the contactless card, a card verification value (CVV) associated with the contactless card, a billing address associated with the contactless card, a name of a user associated with the contactless card, and any combination thereof. The message 302 may be transmitted to the mobile device 104 either prior to initiation of a transaction with the computing device 108 and/or after commencement of the transaction.

[0071] The account identification engine 204 of the mobile device 104 may receive the message 302. This may trigger the engine 204 to identify one or more financial accounts that the user of the mobile device 104 and/or contactless card 102 may have with one or more financial institutions. As discussed above in connection with FIG. 2, the engine 204 may contact one or more servers 110 to retrieve information about such accounts and display them in a graphical applet or graphical user interface (such as, for example, as shown in FIG. 4). The accounts may include, a checking account, a saving account, a credit card account, an investment account, and/or any other type of account from which funds may be withdrawn for the purposes of execution of the transaction by the computing device 108.

[0072] The account identification engine 204 may, optionally, also prompt the user to select one or more of the displayed identified financial accounts. Selection may be made through tapping, clicking, sliding, etc. on the screen of the mobile device 104 in the area of the graphical user interface of the mobile device 104 corresponding to where the desired financial account is displayed.

[0073] The selected account information 304 may then be sent by the engine 204 to the virtual account number assignment engine 210 to generate a virtual account number 306. As stated above, the virtual account number may be any random sequence of alpha-numeric and/or any other characters that conceals the actual account information of the selected account 304. In some implementations, the engine 210 may generate virtual account numbers for all financial accounts that may have been retrieved by the account identification engine 204.

[0074] The virtual account number 306 may then be sent to the computing device 108 for use in connection with execution of the transaction. In some implementations, prior to transmission of the virtual account number 306, the mobile device 104 may be configured to request user's authorization to do so. For example, the mobile device 104 may request the user to provide authentication information, such as, a passcode, a fingerprint, a faceprint, and/or any other biometric information, and/or any other type of authentication information. Once the user provides the authentication information, the mobile device 104 may determine that the user authorized it to transmit the virtual account number 306 to the computing device 108. The virtual account number 306 may be one-time use only (e.g., to be used with the specific transaction only) and/or may be valid for a predetermined period of time (e.g., upon expiration of which, it may no longer be used).

[0075] Upon receipt of the virtual account number 306, the computing device 108 may transmit message 308 to the server 112, which may be associated with the computing device 108.

The message 308 may include the virtual account information 306 along with information associated with the transaction. The server 112 may transmit a request for authorization 310 to the server 110, which may be associated with the selected financial account 304. Alternatively, or in addition, the computing device 108 may transmit request for authorization 310 to the server 110 directly. The request 310 may seek server 110's authorization to use the financial account corresponding to the virtual account number 306 to proceed with execution of the transaction.

[0076] Assuming the request contains valid information (e.g., valid virtual account number 306, transaction information, authentication of the computing device 108, and/or any other information), the server 110 may transmit an authorization 312 to the server 112 and/or directly to the computing device 108. As can be understood, the servers 110, 112 and/or the computing device 108 may perform one or more exchanges prior to transmission of authorization 312. Once authorization 312 is received, the computing device 108 may be configured to proceed with execution 314 of the transaction.

[0077] The above process is advantageous in that it allows selection of specific financial accounts for execution of transactions. It also ensures and preserves security of any sensitive information that may be exchanged between various computing devices through use of virtual account numbers as well as various verification/authentication mechanisms.

[0078] FIG. 4 illustrates an example of a graphical applet or graphical user interface 214 that may be displayed on the mobile device 104. The applet/interface 214 may be generated by the mobile device 104, and in some implementations, its account identification engine 204 (as shown in FIG. 2). The applet/interface 214 may be generated as a result of the engine 204 receiving information from one or more servers 110 (not shown in FIG. 4) associated with one or more financial accounts that the user may have at various financial institutions. For example, the

applet/interface 214 may show the following accounts: “Capital One Checking”, “Capital One Credit Card”, and “Investment Account”. The applet/interface 214 may also display available balances for each account (e.g., “\$500.00” for the checking account; “\$2,000.00” for the credit card account; and “\$10,000.00 for the investment account). As can be understood, any other information may be displayed in the applet/interface 214. The displayed information is generated based on the information received from one or more servers 110.

[0079] As shown in FIG. 4, one of the accounts, account 206b, displayed in the applet/interface 214 has been selected as the account that the user wishes to use in connection with the transaction. The selection may be made by tapping, clicking, sliding, etc. on the screen of the mobile device 104. Once selected, the account may be highlighted to distinguish it from other accounts. As can be understood, more than one account may be selected. The selected account(s) may be transmitted to the virtual account number assignment engine 210 (not shown in FIG. 4) for generation of a corresponding virtual account number 306 (as shown in FIG. 3).

[0080] FIG. 5 illustrates an example process 500 for execution of a transaction, according to some implementations of the current subject matter. The process 500 may be executed using one or more components of the system 100 shown in FIG. 1. In particular, account selection engine 106 running on the mobile device 104 may be used for these purposes.

[0081] At 502, the account selection engine 106 may be configured to receive an identifier associated with a transaction to be executed by the computing device 108 communicatively coupled to the mobile device 104. Any other transaction information may be received. In some implementations, the contactless card 102 may also provide various information to the mobile device 104, which, as discussed above, may be used to retrieve information about one or more financial accounts that may be used in connection with the transaction execution. Alternatively, or

in addition, the contactless card 102 may also provide one or more identifiers (e.g., an account number associated with the contactless card, an expiration date associated with the contactless card, a card verification value (CVV) associated with the contactless card, a billing address associated with the contactless card, a name of a user associated with the contactless card, and any combination thereof), which may be stored in the memory of the contactless card 102.

[0082] In some implementations, a near-field communication (NFC) exchange may be executed between the contactless card 102 and the mobile device 104 upon the contactless card 102 being detected by the mobile device 104 to be located within a predetermined area/distance 114, as shown FIG. 1. Further, once the NFC exchange between the contactless card 102 and the mobile device 104 is established, the mobile device 104 may be configured to generate one or more graphical applets and/or graphical user interfaces (e.g., user interface 214, as shown in FIG. 4). The generated applet may be configured to list the financial accounts and receive input that may trigger selections of the accounts and subsequent generation of virtual identifiers/account numbers for the selected account.

[0083] In some implementations, the contactless card 102 (including all of its information) may be linked to and/or associated with one or more user's financial accounts, which may be displayed in the generated applet, as discussed above. Moreover, virtual identifiers/account numbers may be generated for only the financial account that has been selected in the applet, or for some and/or all financial accounts being displayed in the applet.

[0084] Further, the contactless card 102 may be any type of card. For example, the contactless card 102 may be a credit card, a debit card, an electronic gift card, a pre-paid credit card, a pre-paid debit card, and any combination thereof.

[0085] Referring back to FIG. 5, the account selection engine 106 of the mobile device 104 may, at 504, generate one or more virtual identifiers or virtual account numbers based on the received information (e.g., information about the transaction, information about the financial accounts, etc.). For example, as shown in FIG. 3, the virtual account number assignment engine 210 may generate such virtual identifier or virtual account number 306. The virtual identifier may then be used in connection transaction execution. As can be understood, such virtual identifiers/account numbers may be generated for more than one financial account.

[0086] At 506, the virtual identifier may be selected and assigned for use with the transaction. For example, selection/assignment may be triggered as a result of a selection of an account from a listing of accounts made on the screen of the mobile device 104 (as shown in FIG. 4). Once selection is made, the engine 106 may trigger execution of the transaction by the computing device 108 using the assigned at least one virtual identifier, at 508.

[0087] FIG. 6 illustrates another example process 600 for execution of a transaction, according to some implementations of the current subject matter. The process 600 may likewise be executed using one or more components of the system 100 shown in FIG. 1.

[0088] At 602, the mobile device 104 may be configured to generate one or more virtual identifiers using one or more identifiers associated with a transaction (e.g., transaction 202, as shown in FIG. 2). The transaction may be executed using at least one computing device (e.g., computing device 108, as shown in FIG. 1) communicatively coupled to the mobile device. The identifiers may be received from a contactless card (e.g., contactless card 102 as shown in FIG. 1) communicatively coupled to the mobile device. More than one virtual identifier may be generated and one such virtual identifier may be selected for further processing of the transaction. As stated above the contactless card and the mobile device may be communicatively coupled using NFC

exchange communication link. Activation of such NFC exchange link may trigger generation of one or more graphical applets and/or graphical user interfaces to be displayed by the mobile device. The applets may display information about one or more financial accounts associated with the user, which the user may use to select for triggering execution of the transaction by the computing device, at 604. Selection of a financial account causes transmission of a virtual identifier to the computing device for execution of the transaction.

[0089] FIG. 6 illustrates yet another example process 700 for execution of a transaction that may be performed by one or more components of the system 100 shown in FIG. 1, according to some implementations of the current subject matter. At 702, a near-field communication (NFC) exchange may be executed between a contactless card (e.g., contactless card 102) and a mobile device (e.g., mobile device 104) upon the contactless card being detected by the mobile device to be located within a predetermined distance (e.g., distance/area 114) of the mobile device. At 704, in response to the execution of the NFC exchange, one or more identifiers associated with a transaction may be received from the contactless card (e.g., contactless card information, account number, expiration date, etc., as discussed above). The transaction may be configured to be executed using at least one computing device (e.g., computing device 108) communicatively coupled to the mobile device.

[0090] At 706, one or more virtual identifiers may be generated by the mobile device 104 using one or more identifiers associated with the transaction. The virtual identifier(s) may be associated with one or more financial accounts, e.g., user's financial accounts. The accounts information (e.g., name of the account, available balance, etc., as shown in FIG. 4) may be displayed on a user interface of the mobile device. At 708, at least one virtual identifier may be

selected and assigned to the transaction. At 710, execution of the transaction may be performed by the computing device using the assigned virtual identifier.

[0091] FIG. 8 illustrates a data transmission system 800 according to an example embodiment. As further discussed below, system 800 may include contactless card 802, client device 804, network 806, and server 808. Although FIG. 8 illustrates single instances of the components, system 800 may include any number of components.

[0092] System 800 may include one or more contactless cards 802, which are further explained below. In some embodiments, contactless card 802 may be in wireless communication, utilizing NFC in an example, with client device 804.

[0093] System 800 may include client device 804, which may be a network-enabled computer. As referred to herein, a network-enabled computer may include, but is not limited to a computer device, or communications device including, e.g., a server, a network appliance, a personal computer, a workstation, a phone, a handheld PC, a personal digital assistant, a thin client, a fat client, an Internet browser, or other device. client device 104 also may be a mobile device; for example, a mobile device may include an iPhone, iPod, iPad from Apple® or any other mobile device running Apple's iOS® operating system, any device running Microsoft's Windows® Mobile operating system, any device running Google's Android® operating system, and/or any other smartphone, tablet, or like wearable mobile device.

[0094] The client device 804 device can include a processor and a memory, and it is understood that the processing circuitry may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamperproofing hardware, as necessary to perform the functions described herein. The client device 104 may further include a display and input

devices. The display may be any type of device for presenting visual information such as a computer monitor, a flat panel display, and a mobile device screen, including liquid crystal displays, light-emitting diode displays, plasma panels, and cathode ray tube displays. The input devices may include any device for entering information into the user's device that is available and supported by the user's device, such as a touch-screen, keyboard, mouse, cursor-control device, touch-screen, microphone, digital camera, video recorder or camcorder. These devices may be used to enter information and interact with the software and other devices described herein.

[0095] In some examples, client device 804 of system 800 may execute one or more applications, such as software applications, that enable, for example, network communications with one or more components of system 800 and transmit and/or receive data.

[0096] The client device 804 may be in communication with one or more server(s) 808 via one or more network(s) 806, and may operate as a respective front-end to back-end pair with server 808. The client device 804 may transmit, for example from a mobile device application executing on client device 804, one or more requests to server 808. The one or more requests may be associated with retrieving data from server 808. The server 808 may receive the one or more requests from client device 804. Based on the one or more requests from client device 804, server 808 may be configured to retrieve the requested data from one or more databases (not shown). Based on receipt of the requested data from the one or more databases, server 808 may be configured to transmit the received data to client device 804, the received data being responsive to one or more requests.

[0097] System 800 may include one or more networks 806. In some examples, network 806 may be one or more of a wireless network, a wired network or any combination of wireless network and wired network, and may be configured to connect client device 804 to server 808. For

example, network 806 may include one or more of a fiber optics network, a passive optical network, a cable network, an Internet network, a satellite network, a wireless local area network (LAN), a Global System for Mobile Communication, a Personal Communication Service, a Personal Area Network, Wireless Application Protocol, Multimedia Messaging Service, Enhanced Messaging Service, Short Message Service, Time Division Multiplexing based systems, Code Division Multiple Access based systems, D-AMPS, Wi-Fi, Fixed Wireless Data, IEEE 1502.11 family of networking, Bluetooth, NFC, Radio Frequency Identification (RFID), Wi-Fi, and/or the like.

[0098] In addition, network 806 may include, without limitation, telephone lines, fiber optics, IEEE Ethernet 802.3, a wide area network, a wireless personal area network, a LAN, or a global network such as the Internet. In addition, network 806 may support an Internet network, a wireless communication network, a cellular network, or the like, or any combination thereof. network 806 may further include one network, or any number of the exemplary types of networks mentioned above, operating as a stand-alone network or in cooperation with each other. network 806 may utilize one or more protocols of one or more network elements to which they are communicatively coupled. network 806 may translate to or from other protocols to one or more protocols of network devices. Although network 806 is depicted as a single network, it should be appreciated that according to one or more examples, network 806 may comprise a plurality of interconnected networks, such as, for example, the Internet, a service provider's network, a cable television network, corporate networks, such as credit card association networks, and home networks.

[0099] System 800 may include one or more servers 808. In some examples, server 808 may include one or more processors, which are coupled to memory. The server 808 may be

configured as a central system, server or platform to control and call various data at different times to execute a plurality of workflow actions. Server 120 may be configured to connect to the one or more databases. The server 808 may be connected to at least one client device 804.

[0100] FIG. 9 illustrates a data transmission system according to an example embodiment. System 900 may include a transmitting or transmitting device 904, a receiving or receiving device 908 in communication, for example via network 906, with one or more servers 902. Transmitting or transmitting device 904 may be the same as, or similar to, mobile device 104 and/or computing device 108 discussed above with reference to FIG. 1. Receiving or receiving device 908 may be the same as, or similar to, mobile device 104 and/or computing device 108 discussed above with reference to FIG. 1. Network 906 may be similar to any network communicatively coupling components of the system 100 discussed above with reference to FIG. 1. Server 902 may be similar to any server 110, 112 discussed above with reference to FIG. 1. Although FIG. 9 shows single instances of components of system 900, system 900 may include any number of the illustrated components.

[0101] When using symmetric cryptographic algorithms, such as encryption algorithms, hash-based message authentication code (HMAC) algorithms, and cipher-based message authentication code (CMAC) algorithms, it is important that the key remain secret between the party that originally processes the data that is protected using a symmetric algorithm and the key, and the party who receives and processes the data using the same cryptographic algorithm and the same key.

[0102] It is also important that the same key is not used too many times. If a key is used or reused too frequently, that key may be compromised. Each time the key is used, it provides an attacker an additional sample of data which was processed by the cryptographic algorithm using

the same key. The more data which the attacker has which was processed with the same key, the greater the likelihood that the attacker may discover the value of the key. A key used frequently may be comprised in a variety of different attacks.

[0103] Moreover, each time a symmetric cryptographic algorithm is executed, it may reveal information, such as side-channel data, about the key used during the symmetric cryptographic operation. Side-channel data may include minute power fluctuations which occur as the cryptographic algorithm executes while using the key. Sufficient measurements may be taken of the side-channel data to reveal enough information about the key to allow it to be recovered by the attacker. Using the same key for exchanging data would repeatedly reveal data processed by the same key.

[0104] However, by limiting the number of times a particular key will be used, the amount of side-channel data which the attacker is able to gather is limited and thereby reduce exposure to this and other types of attack. As further described herein, the parties involved in the exchange of cryptographic information (e.g., sender and recipient) can independently generate keys from an initial shared master symmetric key in combination with a counter value, and thereby periodically replace the shared symmetric key being used with needing to resort to any form of key exchange to keep the parties in sync. By periodically changing the shared secret symmetric key used by the sender and the recipient, the attacks described above are rendered impossible.

[0105] Referring back to FIG. 9, system 900 may be configured to implement key diversification. For example, a sender and recipient may desire to exchange data (e.g., original sensitive data) via respective devices 904 and 908. As explained above, although single instances of transmitting device 904 and receiving device 908 may be included, it is understood that one or more transmitting devices 904 and one or more receiving devices 908 may be involved so long as

each party shares the same shared secret symmetric key. In some examples, the transmitting device 904 and receiving device 908 may be provisioned with the same master symmetric key. Further, it is understood that any party or device holding the same secret symmetric key may perform the functions of the transmitting device 904 and similarly any party holding the same secret symmetric key may perform the functions of the receiving device 908. In some examples, the symmetric key may comprise the shared secret symmetric key which is kept secret from all parties other than the transmitting device 904 and the receiving device 908 involved in exchanging the secure data. It is further understood that both the transmitting device 904 and receiving device 908 may be provided with the same master symmetric key, and further that part of the data exchanged between the transmitting device 904 and receiving device 908 comprises at least a portion of data which may be referred to as the counter value. The counter value may comprise a number that changes each time data is exchanged between the transmitting device 904 and the receiving device 908.

[0106] System 900 may include one or more networks 906. In some examples, network 906 may be one or more of a wireless network, a wired network or any combination of wireless network and wired network, and may be configured to connect one or more transmitting devices 904 and one or more receiving devices 908 to server 902. For example, network 906 may include one or more of a fiber optics network, a passive optical network, a cable network, an Internet network, a satellite network, a wireless LAN, a Global System for Mobile Communication, a Personal Communication Service, a Personal Area Network, Wireless Application Protocol, Multimedia Messaging Service, Enhanced Messaging Service, Short Message Service, Time Division Multiplexing based systems, Code Division Multiple Access based systems, D-AMPS, Wi-Fi, Fixed Wireless Data, IEEE 1502.11 family network, Bluetooth, NFC, RFID, Wi-Fi, and/or the like.

[0107] In addition, network 906 may include, without limitation, telephone lines, fiber optics, IEEE Ethernet 1602.3, a wide area network, a wireless personal area network, a LAN, or a global network such as the Internet. In addition, network 906 may support an Internet network, a wireless communication network, a cellular network, or the like, or any combination thereof. Network 906 may further include one network, or any number of the exemplary types of networks mentioned above, operating as a stand-alone network or in cooperation with each other. Network 906 may utilize one or more protocols of one or more network elements to which they are communicatively coupled. Network 906 may translate to or from other protocols to one or more protocols of network devices. Although network 906 is depicted as a single network, it should be appreciated that according to one or more examples, network 906 may comprise a plurality of interconnected networks, such as, for example, the Internet, a service provider's network, a cable television network, corporate networks, such as credit card association networks, and home networks.

[0108] In some examples, one or more transmitting devices 904 and one or more receiving devices 908 may be configured to communicate and transmit and receive data between each other without passing through network 906. For example, communication between the one or more transmitting devices 904 and the one or more receiving devices 908 may occur via at least one of NFC, Bluetooth, RFID, Wi-Fi, and/or the like.

[0109] At 910, when the transmitting device 904 is preparing to process the sensitive data with symmetric cryptographic operation, the sender may update a counter. In addition, the transmitting device 904 may select an appropriate symmetric cryptographic algorithm, which may include at least one of a symmetric encryption algorithm, HMAC algorithm, and a CMAC algorithm. In some examples, the symmetric algorithm used to process the diversification value

may comprise any symmetric cryptographic algorithm used as needed to generate the desired length diversified symmetric key. Non-limiting examples of the symmetric 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. It is understood that if the output of the selected symmetric algorithm does not generate a sufficiently long key, techniques such as processing multiple iterations of the symmetric algorithm with different input data and the same master key may produce multiple outputs which may be combined as needed to produce sufficient length keys.

[0110] At 912, the transmitting device 904 may take the selected cryptographic algorithm, and using the master symmetric key, process the counter value. For example, the sender may select a symmetric encryption algorithm, and use a counter which updates with every conversation between the transmitting device 904 and the receiving device 908. The transmitting device 904 may then encrypt the counter value with the selected symmetric encryption algorithm using the master symmetric key, creating a diversified symmetric key.

[0111] In some examples, the counter value may not be encrypted. In these examples, the counter value may be transmitted between the transmitting device 904 and the receiving device 908 at 912 without encryption.

[0112] At 914, the diversified symmetric key may be used to process the sensitive data before transmitting the result to the receiving device 908. For example, the transmitting device 904 may encrypt the sensitive data using a symmetric encryption algorithm using the diversified symmetric key, with the output comprising the protected encrypted data. The transmitting device 904 may then transmit the protected encrypted data, along with the counter value, to the receiving device 908 for processing.

[0113] At 916, the receiving device 908 may first take the counter value and then perform the same symmetric encryption using the counter value as input to the encryption, and the master symmetric key as the key for the encryption. The output of the encryption may be the same diversified symmetric key value that was created by the sender.

[0114] At 918, the receiving device 908 may then take the protected encrypted data and using a symmetric decryption algorithm along with the diversified symmetric key, decrypt the protected encrypted data.

[0115] At 920, as a result of the decrypting the protected encrypted data, the original sensitive data may be revealed.

[0116] The next time sensitive data needs to be sent from the sender to the recipient via respective transmitting device 904 and receiving device 908, a different counter value may be selected producing a different diversified symmetric key. By processing the counter value with the master symmetric key and same symmetric cryptographic algorithm, both the transmitting device 904 and receiving device 908 may independently produce the same diversified symmetric key. This diversified symmetric key, not the master symmetric key, is used to protect the sensitive data.

[0117] As explained above, both the transmitting device 904 and receiving device 908 each initially possess the shared master symmetric key. The shared master symmetric key is not used to encrypt the original sensitive data. Because the diversified symmetric key is independently created by both the transmitting device 904 and receiving device 908, it is never transmitted between the two parties. Thus, an attacker cannot intercept the diversified symmetric key and the attacker never sees any data which was processed with the master symmetric key. Only the counter value is processed with the master symmetric key, not the sensitive data. As a result, reduced side-channel data about the master symmetric key is revealed. Moreover, the operation of the transmitting

device 904 and the receiving device 908 may be governed by symmetric requirements for how often to create a new diversification value, and therefore a new diversified symmetric key. In an embodiment, a new diversification value and therefore a new diversified symmetric key may be created for every exchange between the transmitting device 904 and receiving device 908.

[0118] In some examples, the key diversification value may comprise the counter value. Other non-limiting examples of the key diversification value include: a random nonce generated each time a new diversified key is needed, the random nonce sent from the transmitting device 904 to the receiving device 908; the full value of a counter value sent from the transmitting device 904 and the receiving device 908; a portion of a counter value sent from the transmitting device 904 and the receiving device 908; a counter independently maintained by the transmitting device 904 and the receiving device 908 but not sent between the two devices; a one-time-passcode exchanged between the transmitting device 904 and the receiving device 908; and a cryptographic hash of the sensitive data. In some examples, one or more portions of the key diversification value may be used by the parties to create multiple diversified keys. For example, a counter may be used as the key diversification value. Further, a combination of one or more of the exemplary key diversification values described above may be used.

[0119] In another example, a portion of the counter may be used as the key diversification value. If multiple master key values are shared between the parties, the multiple diversified key values may be obtained by the systems and processes described herein. A new diversification value, and therefore a new diversified symmetric key, may be created as often as needed. In the most secure case, a new diversification value may be created for each exchange of sensitive data between the transmitting device 904 and the receiving device 908. In effect, this may create a one-time use key, such as a single-use session key.

[0120] FIG. 10 illustrates an example configuration of a contactless card 802, which may include a contactless card, a payment card, such as a credit card, debit card, or gift card, issued by a service provider as displayed as service provider indicia 1002 on the front or back of the contactless card 802. In some examples, the contactless card 802 is not related to a payment card, and may include, without limitation, an identification card. In some examples, the transaction card may include a dual interface contactless payment card, a rewards card, and so forth. The contactless card 802 may include a substrate 1008, 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 802 may have physical characteristics compliant with the ID-1 format of the ISO/IEC 7816 standard, and the transaction card may otherwise be compliant with the ISO/IEC 14443 standard. However, it is understood that the contactless card 802 according to the present disclosure may have different characteristics, and the present disclosure does not require a transaction card to be implemented in a payment card.

[0121] The contactless card 802 may also include identification information 1006 displayed on the front and/or back of the card, and a contact pad 1004. The contact pad 1004 may include one or more pads and be configured to establish contact with another client device, such as an ATM, a user device, smartphone, laptop, desktop, or tablet computer via transaction cards. The contact pad may be designed in accordance with one or more standards, such as ISO/IEC 7816 standard, and enable communication in accordance with the EMV protocol. The contactless card 802 may also include processing circuitry, antenna and other components as will be further discussed in FIG. 11. These components may be located behind the contact pad 1004 or elsewhere

on the substrate 1008, e.g., within a different layer of the substrate 1008, and may electrically and physically coupled with the contact pad 1004. The contactless card 802 may also include a magnetic strip or tape, which may be located on the back of the card (not shown in FIG. 10). The contactless card 802 may also include a Near-Field Communication (NFC) device coupled with an antenna capable of communicating via the NFC protocol. Embodiments are not limited in this manner.

[0122] As illustrated in FIG. 2, the contact pad 1004 of contactless card 802 may include processing circuitry 1116 for storing, processing, and communicating information, including a processor 1102, a memory 1104, and one or more interface(s) 1106. It is understood that the processing circuitry 1116 may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamperproofing hardware, as necessary to perform the functions described herein.

[0123] The memory 1104 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 802 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-programmed many times after leaving the factory. A read/write memory may also be read many times after leaving the factory. In some instances, the memory 1104 may be encrypted memory utilizing an encryption algorithm executed by the processor 1102 to encrypted data.

[0124] The memory 1104 may be configured to store one or more applet(s) 1108, one or more counter(s) 1110, a customer identifier 1114, and the account number(s) 1112, which may be virtual account numbers. The one or more applet(s) 1108 may comprise one or more software applications configured to execute on one or more contactless cards, such as a Java® Card applet. However, it is understood that applet(s) 1108 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 counter(s) 1110 may comprise a numeric counter sufficient to store an integer. The customer identifier 1114 may comprise a unique alphanumeric identifier assigned to a user of the contactless card 802, and the identifier may distinguish the user of the contactless card from other contactless card users. In some examples, the customer identifier 1114 may identify both a customer and an account assigned to that customer and may further identify the contactless card 802 associated with the customer's account. As stated, the account number(s) 1112 may include thousands of one-time use virtual account numbers associated with the contactless card 802. An applet(s) 1108 of the contactless card 802 may be configured to manage the account number(s) 1112 (e.g., to select an account number(s) 1112, mark the selected account number(s) 1112 as used, and transmit the account number(s) 1112 to a mobile device for autofilling by an autofilling service).

[0125] The processor 1102 and memory elements of the foregoing exemplary embodiments are described with reference to the contact pad 1004, but the present disclosure is not limited thereto. It is understood that these elements may be implemented outside of the contact pad 1004 or entirely separate from it, or as further elements in addition to processor 1102 and memory 1104 elements located within the contact pad 1004.

[0126] In some examples, the contactless card 802 may comprise one or more antenna(s) 1118. The one or more antenna(s) 1118 may be placed within the contactless card 802 and around the processing circuitry 1116 of the contact pad 1004. For example, the one or more antenna(s) 1118 may be integral with the processing circuitry 1116 and the one or more antenna(s) 1118 may be used with an external booster coil. As another example, the one or more antenna(s) 1118 may be external to the contact pad 1004 and the processing circuitry 1116.

[0127] In an embodiment, the coil of contactless card 802 may act as the secondary of an air core transformer. The terminal may communicate with the contactless card 802 by cutting power or amplitude modulation. The contactless card 802 may infer the data transmitted from the terminal using the gaps in the contactless card's power connection, which may be functionally maintained through one or more capacitors. The contactless card 802 may communicate back by switching a load on the contactless card's coil or load modulation. Load modulation may be detected in the terminal's coil through interference. More generally, using the antenna(s) 1118, processor 1102, and/or the memory 1104, the contactless card 802 provides a communications interface to communicate via NFC, Bluetooth, and/or Wi-Fi communications.

[0128] As explained above, contactless card 802 may be built on a software platform operable on smart cards or other devices having limited memory, such as JavaCard, and one or more applications or applets may be securely executed. Applet(s) 1108 may be added to contactless cards to provide a one-time password (OTP) for multifactor authentication (MFA) in various mobile application-based use cases. Applet(s) 1108 may be configured to respond to one or more requests, such as near field data exchange requests, from a reader, such as a mobile NFC reader (e.g., of a mobile device or point-of-sale terminal), and produce an NDEF message that comprises a cryptographically secure OTP encoded as an NDEF text tag.

[0129] One example of an NDEF OTP is an NDEF short-record layout (SR=1). In such an example, one or more applet(s) 1108 may be configured to encode the OTP as an NDEF type 4 well known type text tag. In some examples, NDEF messages may comprise one or more records. The applet(s) 1108 may be configured to add one or more static tag records in addition to the OTP record.

[0130] In some examples, the one or more applet(s) 1108 may be configured to emulate an RFID tag. The RFID tag may include one or more polymorphic tags. In some examples, each time the tag is read, different cryptographic data is presented that may indicate the authenticity of the contactless card. Based on the one or more applet(s) 1108, an NFC read of the tag may be processed, the data may be transmitted to a server, such as a server of a banking system, and the data may be validated at the server.

[0131] In some examples, the contactless card 802 and server may include certain data such that the card may be properly identified. The contactless card 802 may include one or more unique identifiers (not pictured). Each time a read operation takes place, the counter(s) 1110 may be configured to increment. In some examples, each time data from the contactless card 802 is read (e.g., by a mobile device), the counter(s) 1110 is transmitted to the server for validation and determines whether the counter(s) 1110 are equal (as part of the validation) to a counter of the server.

[0132] The one or more counter(s) 1110 may be configured to prevent a replay attack. For example, if a cryptogram has been obtained and replayed, that cryptogram is immediately rejected if the counter(s) 1110 has been read or used or otherwise passed over. If the counter(s) 1110 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 is unable

to determine the application transaction counter(s) 1110 since there is no communication between applet(s) 1108 on the contactless card 802.

[0133] In some examples, the counter(s) 1110 may get out of sync. In some examples, to account for accidental reads that initiate transactions, such as reading at an angle, the counter(s) 1110 may increment but the application does not process the counter(s) 1110. In some examples, when the mobile device 104 is woken up, NFC may be enabled and the mobile device 104 may be configured to read available tags, but no action is taken responsive to the reads.

[0134] To keep the counter(s) 1110 in sync, an application, such as a background application, may be executed that would be configured to detect when the mobile device 104 wakes up and synchronize with the server of a banking system indicating that a read that occurred due to detection to then move the counter 1100 forward. 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(s) 1110 may be configured 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(s) 1110 increases in the appropriate sequence, then it possible to know that the user has done so.

[0135] The key diversification technique described herein with reference to the counter(s) 1110, master key, and diversified key, 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.

[0136] During the creation process of the contactless card 802, two cryptographic keys may be assigned uniquely per card. The cryptographic keys may comprise symmetric keys which may be used in both encryption and decryption of data. Triple DES (3DES) algorithm may be used by EMV and it is implemented by hardware in the contactless card 802. 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.

[0137] 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 802 is used in operation, a different key may be used for creating the message authentication code (MAC) and for performing the encryption. This results in a triple layer of cryptography. The session keys may be generated by the one or more applets and derived by using the application transaction counter with one or more algorithms (as defined in EMV 4.3 Book 2 A1.3.1 Common Session Key Derivation).

[0138] Further, the increment for each card may be unique, and assigned either by personalization, or algorithmically assigned by some identifying information. For example, odd numbered cards may increment by 2 and even numbered cards may increment by 5. In some examples, the increment may also vary in sequential reads, such that one card may increment in sequence by 1, 3, 5, 2, 2, ... repeating. The specific sequence or algorithmic sequence may be defined at personalization time, or from one or more processes derived from unique identifiers. This can make it harder for a replay attacker to generalize from a small number of card instances.

[0139] 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.

[0140] FIG. 12 is a timing diagram illustrating an example sequence for providing authenticated access according to one or more embodiments of the present disclosure. Sequence flow 1200 may include contactless card 802 and client device 804, which may include an application 1202 and processor 1204.

[0141] At line 1208, the application 1202 communicates with the contactless card 802 (e.g., after being brought near the contactless card 802). Communication between the application 1202 and the contactless card 802 may involve the contactless card 802 being sufficiently close to a card reader (not shown) of the client device 804 to enable NFC data transfer between the application 1202 and the contactless card 802.

[0142] At line 1206, after communication has been established between client device 804 and contactless card 802, contactless card 802 generates a message authentication code (MAC) cryptogram. In some examples, this may occur when the contactless card 802 is read by the application 1202. 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 application, such as application 1202, may transmit a message, such as an applet select message, with the applet ID of an NDEF producing applet. Upon confirmation of the selection, a sequence of select file messages followed by read file messages may be transmitted. For example, the sequence may include “Select Capabilities file”, “Read Capabilities file”, and “Select NDEF file”. At this point, a counter value maintained by the contactless card 802 may be updated or incremented, which may be followed by “Read NDEF file.” At this point,

the message may be generated which may include a header and a shared secret. Session keys may then be generated. The MAC cryptogram may be created from the message, which may include the header and the shared secret. The MAC cryptogram may then be concatenated with one or more blocks of random data, and the MAC cryptogram and a random number (RND) may be encrypted with the session key. Thereafter, the cryptogram and the header may be concatenated, and encoded as ASCII hex and returned in NDEF message format (responsive to the “Read NDEF file” message).

[0143] 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). In some examples, application 1202 may be configured to transmit a request to contactless card 802, the request comprising an instruction to generate a MAC cryptogram.

[0144] At line 1210, the contactless card 802 sends the MAC cryptogram to the application 1202. In some examples, the transmission of the MAC cryptogram occurs via NFC, however, the present disclosure is not limited thereto. In other examples, this communication may occur via Bluetooth, Wi-Fi, or other means of wireless data communication. At line 1212, the application 1202 communicates the MAC cryptogram to the processor 1204.

[0145] At line 1214, the processor 1204 verifies the MAC cryptogram pursuant to an instruction from the application 122. For example, the MAC cryptogram may be verified, as explained below. In some examples, verifying the MAC cryptogram may be performed by a device other than client device 804, such as a server of a banking system in data communication with the client device 804. For example, processor 1204 may output the MAC cryptogram for transmission to the server of the banking system, which may verify the MAC cryptogram. In some examples, the MAC cryptogram may function as a digital signature for purposes of verification. Other digital

signature algorithms, such as public key asymmetric algorithms, e.g., the Digital Signature Algorithm and the RSA algorithm, or zero knowledge protocols, may be used to perform this verification.

[0146] FIG. 13 illustrates an NDEF short-record layout (SR=1) data structure 1300 according to an example embodiment. One or more applets may be configured to encode the OTP as an NDEF type 4 well known type text tag. In some examples, NDEF messages may comprise one or more records. The applets may be configured to add one or more static tag records in addition to the OTP record. Exemplary tags include, without limitation, Tag type: well-known type, text, encoding English (en); Applet ID: D2760000850101; Capabilities: read-only access; Encoding: the authentication message may be encoded as ASCII hex; type-length-value (TLV) data may be provided as a personalization parameter that may be used to generate the NDEF message. In an embodiment, the authentication template may comprise the first record, with a well-known index for providing the actual dynamic authentication data.

[0147] FIG. 14 illustrates a diagram of a system 1400 configured to implement one or more embodiments of the present disclosure. As explained below, during the contactless card creation process, two cryptographic keys may be assigned uniquely for each card. The cryptographic keys may comprise symmetric keys which may be used in both encryption and decryption of data. Triple DES (3DES) algorithm may be used by EMV and it is implemented by hardware in the contactless card. By using a 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.

[0148] Regarding master key management, two issuer master keys 1402, 1426 may be required for each part of the portfolio on which the one or more applets is issued. For example, the first master key 1402 may comprise an Issuer Cryptogram Generation/Authentication Key (Iss-

Key-Auth) and the second master key 1426 may comprise an Issuer Data Encryption Key (Iss-Key-DEK). As further explained herein, two issuer master keys 1402, 1426 are diversified into card master keys 1408, 1420, which are unique for each card. In some examples, a network profile record ID (pNPR) 522 and derivation key index (pDKI) 1424, as back office data, may be used to identify which Issuer Master Keys 1402, 1426 to use in the cryptographic processes for authentication. The system performing the authentication may be configured to retrieve values of pNPR 1422 and pDKI 1424 for a contactless card at the time of authentication.

[0149] In some examples, to increase the security of the solution, 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, as explained above. For example, each time the card is used in operation, a different key may be used for creating the message authentication code (MAC) and for performing the encryption. Regarding session key generation, the keys used to generate the cryptogram and encipher the data in the one or more applets may comprise session keys based on the card unique keys (Card-Key-Auth 1408 and Card-Key-Dek 1420). The session keys (Aut-Session-Key 1432 and DEK-Session-Key 1410) may be generated by the one or more applets and derived by using the application transaction counter (pATC) 1404 with one or more algorithms. To fit data into the one or more algorithms, only the 2 low order bytes of the 4-byte pATC 1404 is used. In some examples, the four byte session key derivation method may comprise: $F1 := \text{PATC}(\text{lower 2 bytes}) \parallel 'F0' \parallel '00' \parallel \text{PATC (four bytes)}$ $F1 := \text{PATC}(\text{lower 2 bytes}) \parallel '0F' \parallel '00' \parallel \text{PATC (four bytes)}$ $SK := \{(\text{ALG}(\text{MK})[F1]) \parallel \text{ALG}(\text{MK})[F2]\}$, where ALG may include 3DES ECB and MK may include the card unique derived master key.

[0150] As described herein, one or more MAC session keys may be derived using the lower two bytes of pATC 1404 counter. At each tap of the contactless card, pATC 1404 is configured to

be updated, and the card master keys Card-Key-AUTH 508 and Card-Key-DEK 1420 are further diversified into the session keys Aut-Session-Key 1432 and DEK-Session-KEY 1410. pATC 1404 may be initialized to zero at personalization or applet initialization time. In some examples, the pATC counter 1404 may be initialized at or before personalization, and may be configured to increment by one at each NDEF read.

[0151] Further, the update for each card may be unique, and assigned either by personalization, or algorithmically assigned by pUID or other identifying information. For example, odd numbered cards may increment or decrement by 2 and even numbered cards may increment or decrement by 5. In some examples, the update may also vary in sequential reads, such that one card may increment in sequence by 1, 3, 5, 2, 2, ... repeating. The specific sequence or algorithmic sequence may be defined at personalization time, or from one or more processes derived from unique identifiers. This can make it harder for a replay attacker to generalize from a small number of card instances.

[0152] The authentication message may be delivered as the content of a text NDEF record in hexadecimal ASCII format. In some examples, only the authentication data and an 8-byte random number followed by MAC of the authentication data may be included. In some examples, the random number may precede cryptogram A and may be one block long. In other examples, there may be no restriction on the length of the random number. In further examples, the total data (i.e., the random number plus the cryptogram) may be a multiple of the block size. In these examples, an additional 8-byte block may be added to match the block produced by the MAC algorithm. As another example, if the algorithms employed used 16-byte blocks, even multiples of that size may be used, or the output may be automatically, or manually, padded to a multiple of that size.

[0153] The MAC may be performed by a function key (AUT-Session-Key) 1432. The data specified in cryptogram may be processed with javacard.signature method: ALG_DES_MAC8_ISO9797_1_M2_ALG3 to correlate to EMV ARQC verification methods. The key used for this computation may comprise a session key AUT-Session-Key 1432, as explained above. As explained above, the low order two bytes of the counter may be used to diversify for the one or more MAC session keys. As explained below, AUT-Session-Key 1432 may be used to MAC data 1406, and the resulting data or cryptogram A 1414 and random number RND may be encrypted using DEK-Session-Key 1410 to create cryptogram B or output 1418 sent in the message.

[0154] In some examples, one or more HSM commands may be processed for decrypting such that the final 16 (binary, 32 hex) bytes may comprise a 3DES symmetric encrypting using CBC mode with a zero IV of the random number followed by MAC authentication data. The key used for this encryption may comprise a session key DEK-Session-Key 1410 derived from the Card-Key-DEK 1420. In this case, the ATC value for the session key derivation is the least significant byte of the counter pATC 1404.

[0155] The format below represents a binary version example embodiment. Further, in some examples, the first byte may be set to ASCII ‘A’.

Message Format				
1	2	4	8	8
0x43 (Message Type ‘A’)	Version	pATC	RND	Cryptogram A (MAC)
Cryptogram A (MAC)	8 bytes			
MAC of				
2	8	4	4	18 bytes input data
Version	pUID	pATC	Shared Secret	

Message Format				
1	2	4	16	
0x43 (Message Type 'A')	Version	pATC	Cryptogram B	
Cryptogram A (MAC)	8 bytes			
MAC of				
2	8	4	4	18 bytes input data
Version	pUID	pATC	Shared Secret	
Cryptogram B	16			
Sym Encryption of				
8	8			
RND	Cryptogram A			

[0156] Another exemplary format is shown below. In this example, the tag may be encoded in hexadecimal format.

Message Format				
2	8	4	8	8
Version	pUID	pATC	RND	Cryptogram A (MAC)
8 bytes				
8	8	4	4	18 bytes input data
pUID	pUID	pATC	Shared Secret	

Message Format				
2	8	4	16	
Version	pUID	pATC	Cryptogram B	
8 bytes				
8		4	4	18 bytes input data
pUID	pUID	pATC	Shared Secret	
Cryptogram B	16			
Sym Encryption of				
8	8			
RND	Cryptogram A			

[0157] The UID field of the received message may be extracted to derive, from master keys Iss-Key-AUTH 502 and Iss-Key-DEK 1426, the card master keys (Card-Key-Auth 1408 and Card-Key-DEK 1420) for that particular card. Using the card master keys (Card-Key-Auth 508 and Card-Key-DEK 1420), the counter (pATC) field of the received message may be used to derive the session keys (Aut-Session-Key 1432 and DEK-Session-Key 1410) for that particular card. Cryptogram B 1418 may be decrypted using the DEK-Session-KEY, which yields cryptogram A 1414 and RND, and RND may be discarded. The UID field may be used to look up the shared secret of the contactless card which, along with the Ver, UID, and pATC fields of the message, may be processed through the cryptographic MAC using the re-created Aut-Session-Key to create a MAC output, such as MAC'. If MAC' is the same as cryptogram A 1414, then this indicates that the message decryption and MAC checking have all passed. Then the pATC may be read to determine if it is valid.

[0158] During an authentication session, one or more cryptograms may be generated by the one or more applications. For example, the one or more cryptograms may be generated as a 3DES MAC using ISO 9797-1 Algorithm 3 with Method 2 padding via one or more session keys, such as Aut-Session-Key 1432. The input data 1406 may take the following form: Version (2), pUID (8), pATC (4), Shared Secret (4). In some examples, the numbers in the brackets may comprise length in bytes. In some examples, the shared secret may be generated by one or more random number generators which may be configured to ensure, through one or more secure processes, that the random number is unpredictable. In some examples, the shared secret may comprise a random 4-byte binary number injected into the card at personalization time that is known by the authentication service. During an authentication session, the shared secret may not

be provided from the one or more applets to the mobile application. Method 2 padding may include adding a mandatory 0x'80' byte to the end of input data and 0x'00' bytes that may be added to the end of the resulting data up to the 8-byte boundary. The resulting cryptogram may comprise 8 bytes in length.

[0159] In some examples, one benefit of encrypting an unshared random number as the first block with the MAC cryptogram, is that it acts as an initialization vector while using CBC (Block chaining) mode of the symmetric encryption algorithm. This allows the “scrambling” from block to block without having to pre-establish either a fixed or dynamic IV.

[0160] By including the application transaction counter (pATC) as part of the data included in the MAC cryptogram, the authentication service may be configured to determine if the value conveyed in the clear data has been tampered with. Moreover, by including the version in the one or more cryptograms, it is difficult for an attacker to purposefully misrepresent the application version in an attempt to downgrade the strength of the cryptographic solution. In some examples, the pATC may start at zero and be updated by 1 each time the one or more applications generates authentication data. The authentication service may be configured to track the pATCs used during authentication sessions. In some examples, when the authentication data uses a pATC equal to or lower than the previous value received by the authentication service, this may be interpreted as an attempt to replay an old message, and the authenticated may be rejected. In some examples, where the pATC is greater than the previous value received, this may be evaluated to determine if it is within an acceptable range or threshold, and if it exceeds or is outside the range or threshold, verification may be deemed to have failed or be unreliable. In the MAC operation 1412, data 1406 is processed through the MAC using Aut-Session-Key 1432 to produce MAC output (cryptogram A) 1414, which is encrypted.

[0161] In order to provide additional protection against brute force attacks exposing the keys on the card, it is desirable that the MAC cryptogram 1414 be enciphered. In some examples, data or cryptogram A 1414 to be included in the ciphertext may comprise: Random number (8), cryptogram (8). In some examples, the numbers in the brackets may comprise length in bytes. In some examples, the random number may be generated by one or more random number generators which may be configured to ensure, through one or more secure processes, that the random number is unpredictable. The key used to encipher this data may comprise a session key. For example, the session key may comprise DEK-Session-Key 1410. In the encryption operation 1416, data or cryptogram A 1414 and RND are processed using DEK-Session-Key 510 to produce encrypted data, cryptogram B 1418. The data 1414 may be enciphered using 3DES in cipher block chaining mode to ensure that an attacker must run any attacks over all of the ciphertext. As a non-limiting example, other algorithms, such as Advanced Encryption Standard (AES), may be used. In some examples, an initialization vector of 0x'0000000000000000' may be used. Any attacker seeking to brute force the key used for enciphering this data will be unable to determine when the correct key has been used, as correctly decrypted data will be indistinguishable from incorrectly decrypted data due to its random appearance.

[0162] In order for the authentication service to validate the one or more cryptograms provided by the one or more applets, the following data must be conveyed from the one or more applets to the mobile device in the clear during an authentication session: version number to determine the cryptographic approach used and message format for validation of the cryptogram, which enables the approach to change in the future; pUID to retrieve cryptographic assets, and derive the card keys; and pATC to derive the session key used for the cryptogram.

[0163] FIG. 15 illustrates a method 1500 for generating a cryptogram. For example, At 1502, a network profile record ID (pNPR) and derivation key index (pDKI) may be used to identify which Issuer Master Keys to use in the cryptographic processes for authentication. In some examples, the method may include performing the authentication to retrieve values of pNPR and pDKI for a contactless card at the time of authentication.

[0164] At 1504, Issuer Master Keys may be diversified by combining them with the card's unique ID number (pUID) and the PAN sequence number (PSN) of one or more applets, for example, a payment applet.

[0165] At 1506, Card-Key-Auth and Card-Key-DEK (unique card keys) may be created by diversifying the Issuer Master Keys to generate session keys which may be used to generate a MAC cryptogram.

[0166] At 1508, the keys used to generate the cryptogram and encipher the data in the one or more applets may comprise the session keys of block 1030 based on the card unique keys (Card-Key-Auth and Card-Key-DEK). In some examples, these session keys may be generated by the one or more applets and derived by using pATC, resulting in session keys Aut-Session-Key and DEK-Session-Key.

[0167] FIG. 16 depicts an exemplary process 1600 illustrating key diversification according to one example. Initially, a sender and the recipient may be provisioned with two different master keys. For example, a first master key may comprise the data encryption master key, and a second master key may comprise the data integrity master key. The sender has a counter value, which may be updated at 1602, and other data, such as data to be protected, which it may secure share with the recipient.

[0168] At 1604, the counter value may be encrypted by the sender using the data encryption master key to produce the data encryption derived session key, and the counter value may also be encrypted by the sender using the data integrity master key to produce the data integrity derived session key. In some examples, a whole counter value or a portion of the counter value may be used during both encryptions.

[0169] In some examples, the counter value may not be encrypted. In these examples, the counter may be transmitted between the sender and the recipient in the clear, i.e., without encryption.

[0170] At 1606, the data to be protected is processed with a cryptographic MAC operation by the sender using the data integrity session key and a cryptographic MAC algorithm. The protected data, including plaintext and shared secret, may be used to produce a MAC using one of the session keys (AUT-Session-Key).

[0171] At 1608, the data to be protected may be encrypted by the sender using the data encryption derived session key in conjunction with a symmetric encryption algorithm. In some examples, the MAC is combined with an equal amount of random data, for example each 8 bytes long, and then encrypted using the second session key (DEK-Session-Key).

[0172] At 1610, the encrypted MAC is transmitted, from the sender to the recipient, with sufficient information to identify additional secret information (such as shared secret, master keys, etc.), for verification of the cryptogram.

[0173] At 1612, the recipient uses the received counter value to independently derive the two derived session keys from the two master keys as explained above.

[0174] At 1614, the data encryption derived session key is used in conjunction with the symmetric decryption operation to decrypt the protected data. Additional processing on the

exchanged data will then occur. In some examples, after the MAC is extracted, it is desirable to reproduce and match the MAC. For example, when verifying the cryptogram, it may be decrypted using appropriately generated session keys. The protected data may be reconstructed for verification. A MAC operation may be performed using an appropriately generated session key to determine if it matches the decrypted MAC. As the MAC operation is an irreversible process, the only way to verify is to attempt to recreate it from source data.

[0175] At 1616, the data integrity derived session key is used in conjunction with the cryptographic MAC operation to verify that the protected data has not been modified.

[0176] Some examples of the methods described herein may advantageously confirm when a successful authentication is determined when the following conditions are met. First, the ability to verify the MAC shows that the derived session key was proper. The MAC may only be correct if the decryption was successful and yielded the proper MAC value. The successful decryption may show that the correctly derived encryption key was used to decrypt the encrypted MAC. Since the derived session keys are created using the master keys known only to the sender (e.g., the transmitting device) and recipient (e.g., the receiving device), it may be trusted that the contactless card which originally created the MAC and encrypted the MAC is indeed authentic. Moreover, the counter value used to derive the first and second session keys may be shown to be valid and may be used to perform authentication operations.

[0177] Thereafter, the two derived session keys may be discarded, and the next iteration of data exchange will update the counter value (returning to block 1602) and a new set of session keys may be created (at 1610). In some examples, the combined random data may be discarded.

[0178] FIG. 17 illustrates a method 1700 for card activation according to an example embodiment. For example, card activation may be completed by a system including a card, a

device, and one or more servers. The contactless card, device, and one or more servers may reference same or similar components that were previously explained above, such as contactless card 802, client device 804, and a server.

[0179] At 1702, the card may be configured to dynamically generate data. In some examples, this data may include information such as an account number, card identifier, card verification value, or phone number, which may be transmitted from the card to the device. In some examples, one or more portions of the data may be encrypted via the systems and methods disclosed herein.

[0180] At 1704, one or more portions of the dynamically generated data may be communicated to an application of the device via NFC or other wireless communication. For example, a tap of the card proximate to the device may allow the application of the device to read the one or more portions of the data associated with the contactless card. In some examples, if the device does not comprise an application to assist in activation of the card, the tap of the card may direct the device or prompt the customer to a software application store to download an associated application to activate the card. In some examples, the user may be prompted to sufficiently gesture, place, or orient the card towards a surface of the device, such as either at an angle or flatly placed on, near, or proximate the surface of the device. Responsive to a sufficient gesture, placement and/or orientation of the card, the device may proceed to transmit the one or more encrypted portions of data received from the card to the one or more servers.

[0181] At 1706, the one or more portions of the data may be communicated to one or more servers, such as a card issuer server. For example, one or more encrypted portions of the data may be transmitted from the device to the card issuer server for activation of the card.

[0182] At 1708, the one or more servers may decrypt the one or more encrypted portions of the data via the systems and methods disclosed herein. For example, the one or more servers may receive the encrypted data from the device and may decrypt it in order to compare the received data to record data accessible to the one or more servers. If a resulting comparison of the one or more decrypted portions of the data by the one or more servers yields a successful match, the card may be activated. If the resulting comparison of the one or more decrypted portions of the data by the one or more servers yields an unsuccessful match, one or more processes may take place. For example, responsive to the determination of the unsuccessful match, the user may be prompted to tap, swipe, or wave gesture the card again. In this case, there may be a predetermined threshold comprising a number of attempts that the user is permitted to activate the card. Alternatively, the user may receive a notification, such as a message on his or her device indicative of the unsuccessful attempt of card verification and to call, email or text an associated service for assistance to activate the card, or another notification, such as a phone call on his or her device indicative of the unsuccessful attempt of card verification and to call, email or text an associated service for assistance to activate the card, or another notification, such as an email indicative of the unsuccessful attempt of card verification and to call, email or text an associated service for assistance to activate the card.

[0183] At 1710, the one or more servers may transmit a return message based on the successful activation of the card. For example, the device may be configured to receive output from the one or more servers indicative of a successful activation of the card by the one or more servers. The device may be configured to display a message indicating successful activation of the card. Once the card has been activated, the card may be configured to discontinue dynamically

generating data so as to avoid fraudulent use. In this manner, the card may not be activated thereafter, and the one or more servers are notified that the card has already been activated.

[0184] The various elements of the devices as previously described with reference to FIGS. 1-17 may include various hardware elements, software elements, or a combination of both. Examples of hardware elements may include devices, logic devices, components, processors, microprocessors, circuits, processors, 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), memory units, logic gates, registers, semiconductor device, chips, microchips, chip sets, and so forth. Examples of software elements may include software components, programs, applications, computer programs, application programs, system programs, software development 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. However, determining whether an embodiment is implemented using hardware elements and/or software elements may vary in accordance with any number of factors, such as desired computational rate, power levels, heat tolerances, processing cycle budget, input data rates, output data rates, memory resources, data bus speeds and other design or performance constraints, as desired for a given implementation.

[0185] One or more aspects of at least one embodiment may be implemented by representative instructions stored on a machine-readable medium which represents various logic within the processor, which when read by a machine causes the machine to fabricate logic to

perform the techniques described herein. Such representations, known as “IP cores”, may be stored on a tangible, machine readable medium and supplied to various customers or manufacturing facilities to load into the fabrication machines that make the logic or processor. Some embodiments may be implemented, for example, using a machine-readable medium or article which may store an instruction or a set of instructions that, if executed by a machine, may cause the machine to perform a method and/or operations in accordance with the embodiments. Such a machine may include, for example, any suitable processing platform, computing platform, computing device, processing device, computing system, processing system, computer, processor, or the like, and may be implemented using any suitable combination of hardware and/or software. The machine-readable medium or article may include, for example, any suitable type of memory unit, memory device, memory article, memory medium, storage device, storage article, storage medium and/or storage unit, for example, memory, removable or non-removable media, erasable or non-erasable media, writable or rewritable media, digital or analog media, hard disk, floppy disk, Compact Disk Read Only Memory (CD-ROM), Compact Disk Recordable (CD-R), Compact Disk Rewritable (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.

[0186] The components and features of the devices described above may be implemented using any combination of discrete circuitry, application specific integrated circuits (ASICs), logic gates and/or single chip architectures. Further, the features of the devices may be implemented

using microcontrollers, programmable logic arrays and/or microprocessors or any combination of the foregoing where suitably appropriate. It is noted that hardware, firmware and/or software elements may be collectively or individually referred to herein as “logic” or “circuit.”

[0187] It will be appreciated that the exemplary devices shown in the block diagrams described above may represent one functionally descriptive example of many potential implementations. Accordingly, division, omission or inclusion of block functions depicted in the accompanying figures does not infer that the hardware components, circuits, software and/or elements for implementing these functions would necessarily be divided, omitted, or included in embodiments.

[0188] At least one computer-readable storage medium may include instructions that, when executed, cause a system to perform any of the computer-implemented methods described herein.

[0189] Some embodiments may be described using the expression “one embodiment” or “an embodiment” along with their derivatives. These terms mean that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment. The appearances of the phrase “in one embodiment” in various places in the specification are not necessarily all referring to the same embodiment. Moreover, unless otherwise noted the features described above are recognized to be usable together in any combination. Thus, any features discussed separately may be employed in combination with each other unless it is noted that the features are incompatible with each other.

[0190] It is emphasized that the Abstract of the Disclosure is provided to allow a reader to quickly ascertain the nature of the technical disclosure. It is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the

foregoing Detailed Description, it can be seen that various features are grouped together in a single embodiment for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter lies in less than all features of a single disclosed embodiment. Thus, the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separate embodiment. In the appended claims, the terms "including" and "in which" are used as the plain-English equivalents of the respective terms "comprising" and "wherein," respectively. Moreover, the terms "first," "second," "third," and so forth, are used merely as labels, and are not intended to impose numerical requirements on their objects.

[0191] What has been described above includes examples of the disclosed architecture. It is, of course, not possible to describe every conceivable combination of components and/or methodologies, but one of ordinary skill in the art may recognize that many further combinations and permutations are possible. Accordingly, the novel architecture is intended to embrace all such alterations, modifications and variations that fall within the spirit and scope of the appended claims. The foregoing description of example embodiments has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the present disclosure to the precise forms disclosed. Many modifications and variations are possible in light of this disclosure. It is intended that the scope of the present disclosure be limited not by this detailed description, but rather by the claims appended hereto. Future filed applications claiming priority to this application may claim the disclosed subject matter in a different manner and may generally include any set of one or more limitations as variously disclosed or otherwise demonstrated herein.

CLAIMS:

What is claimed:

1. A computer implemented method, comprising:
receiving, using at least one processor, an identifier associated with a transaction, the transaction is configured to be executed using at least one computing device communicatively coupled to the at least one processor;
generating, using the at least one processor, using the received identifier, one or more virtual identifiers;
selecting, using the at least one processor, at least one virtual identifier in the one or more virtual identifiers, and assigning the selected at least one virtual identifier to the transaction; and
triggering, using the at least one processor, execution of the transaction by the at least one computing device using the assigned at least one virtual identifier.
2. The method according to claim 1, wherein the receiving includes receiving, using the at least one processor, the identifier from a contactless card communicatively coupled to the at least one processor, the contactless card storing the identifier.
3. The method according to claim 2, wherein the receiving includes executing a near-field communication (NFC) exchange between the contactless card and the at least one processor upon the contactless card being detected by the at least one processor to be located within a predetermined distance of the at least one processor.

4. The method according to claim 3, wherein the executing the NFC exchange includes triggering the at least one processor to generate at least one user interface, the at least one user interface receiving an input triggering the selecting.

5. The method according to claim 4, wherein the received identifier includes a contactless card number.

6. The method according to claim 5, wherein the contactless card number is associated with one or more financial accounts, wherein the generated at least one user interface is configured to display each financial account in the one or more financial accounts in response to the executing of the NFC exchange.

7. The method according to claim 6, wherein the generated one or more virtual identifiers corresponding to the one or more financial accounts.

8. The method according to claim 2, wherein the contactless card includes at least one of the following: a credit card, a debit card, an electronic gift card, a pre-paid credit card, a pre-paid debit card, and any combination thereof.

9. A system, comprising:
a mobile device including
at least one processor; and

at least one non-transitory storage media storing instructions, that when executed by the at least one processor, cause the at least one processor to perform operations including

generating one or more virtual identifiers using one or more identifiers associated with a transaction, the transaction is configured to be executed using at least one computing device communicatively coupled to the mobile device, wherein the one or more identifiers are received from a contactless card communicatively coupled to the mobile device; and

triggering execution of the transaction by the at least one computing device using at least one virtual identifier in the one or more virtual identifiers.

10. The system according to claim 9, wherein the at least one virtual identifier is selected from the one or more virtual identifiers and assigned to the transaction.

11. The system according to claim 9, wherein the contactless card is configured to store the one or more identifiers.

12. The system according to claim 9, wherein a near-field communication (NFC) exchange is configured to be executed between the contactless card and the mobile device upon the contactless card being detected by the mobile device to be located within a predetermined distance of the mobile device.

13. The system according to claim 12, wherein execution of the NFC exchange triggers the mobile device to generate at least one user interface, the at least one user interface is configured to receive an input triggering selection of the at least one virtual identifier from the one or more virtual identifiers.

14. The system according to claim 13, wherein the one or more identifiers include a contactless card number.

15. The system according to claim 14, wherein the contactless card number is associated with one or more financial accounts, wherein the at least one user interface is configured to display each financial account in the one or more financial accounts in response to execution of the NFC exchange.

16. The system according to claim 15, wherein the one or more virtual identifiers correspond to the one or more financial accounts.

17. The system according to claim 9, wherein the contactless card includes at least one of the following: a credit card, a debit card, an electronic gift card, a pre-paid credit card, a pre-paid debit card, and any combination thereof.

18. A computer program product comprising a non-transitory machine-readable medium storing instructions that, when executed by at least one programmable processor, cause the at least one programmable processor to perform operations comprising:

executing a near-field communication (NFC) exchange between a contactless card and a mobile device upon the contactless card being detected by the mobile device to be located within a predetermined distance of the mobile device;

receiving, in response to the executing of the NFC exchange, from the contactless card, one or more identifiers associated with a transaction, the transaction is configured to be executed using at least one computing device communicatively coupled to the mobile device;

generating one or more virtual identifiers using the one or more identifiers associated with the transaction, the one or more virtual identifier being associated with one or more financial accounts, and displaying the one or more financial accounts on a user interface of the mobile device;

selecting at least one virtual identifier in the one or more virtual identifiers, and assigning the selected at least one virtual identifier to the transaction; and

triggering execution of the transaction by the at least one computing device using the assigned at least one virtual identifier.

19. The computer program product according to claim 18, wherein the one or more identifiers include a contactless card number.

20. The computer program product according to claim 18, wherein the contactless card includes at least one of the following: a credit card, a debit card, an electronic gift card, a pre-paid credit card, a pre-paid debit card, and any combination thereof.