

**TECHNIQUES AND SYSTEMS TO PERFORM AUTHENTICATION AND PAYMENT
OPERATIONS WITH A CONTACTLESS CARD TO PROVIDE ITEMS AND
SERVICES**

BACKGROUND

[0001] More and more of today's activities are being automated, including performing tasks such as renting items like scooters, vehicles, and other equipment. For example, many cities have fleets of scooters deployed throughout that city. These scooters are available for rent without interacting with a person. However, the process is quite cumbersome and high friction, especially for the first rental. A user may be required to perform several tasks, including downloading a specific application associated with the scooter to a mobile device. The user may then be required to set up an account with the scooter company to use the application to rent scooters. During the actual rental process, the user may be further required to identify the scooter for rent, login/access their account, confirm payment, and go through several additional steps to rent the scooter. Embodiments discussed herein aim to simplify this process securely.

BRIEF SUMMARY

[0002] Embodiments discussed herein are generally directed to systems, devices, methods, and techniques to perform authentication and payment operations with a contactless card to provide items and services. For example, embodiments may include a system configured to perform authentication and payment operations based on data stored in contactless cards. The system can include one or more servers comprising one or more processors and memory, the memory coupled with the one or more processors and configured to store instructions. The instructions, that when executed by the one or more processors, cause the one or more processors to receive, from a rental system, encrypted data generated by a contactless card corresponding to a rental of an item, extract authentication information from the encrypted data, perform an authentication operation on the authentication information to authenticate the contactless card, send, to the rental system, a result of the authentication operation indicating that the contactless card is authentic, receive, from the rental system, a payment request to pay for the rental of the item in response to the contactless card being authentic, process the payment request based on information in the encrypted data, and send, to the rental system, a second result of the processing of the payment request indicating that payment is successful for the rental of the item.

[0003] In another example, embodiments may include a server configured to enable rental of items based on authentication operations performed with data stored in contactless cards. The server may include one or more processors, and memory coupled with the one or more processors, the memory to store instructions. The instructions, that when executed by the one or more processors, cause the one or more processors to receive and process, from a computing device, encrypted data stored on a contactless card and rental data corresponding to a rental of an item, send the encrypted data to one or more servers to perform an authentication operation with the encrypted data, receive, from the one or more servers, a result of the authentication operation indicating the contactless card is authentic, and in response to authentication of the contactless card, a user, or a combination thereof, perform one or more operations to enable the rental of the item.

[0004] In another example, embodiments may include computing device, comprising processing circuitry, and memory coupled with the processing circuitry, the memory to store instructions. The instructions that when executed by the processing circuitry, cause the processing circuitry to detect a contactless card within a near-field communication (NFC) range, receive, via one or more NFC exchanges, encrypted data from the contactless card, the encrypted data comprising authentication information to authenticate a user, send, to one or more servers, the encrypted data and rental data, the rental data corresponding to a rental of an item, receive, from the one or more servers, an indication to enable the rental of the item, and cause an action to permit the rental of the item based on the indication.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0005] To easily identify the discussion of any particular element or act, the most significant digit or digits in a reference number refer to the figure number in which that element is first introduced.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0006] FIG. 1 illustrates an example of a system 100 in accordance with embodiments discussed herein.

[0007] FIG. 2A illustrates an example display on a computing device in accordance with embodiments discussed herein.

[0008] FIG. 2B illustrates an example display on a computing device in accordance with embodiments discussed herein.

[0009] FIG. 3A illustrates a first example configuration of a system 300a in accordance with embodiments discussed herein.

[0010] FIG. 3B illustrates a second example configuration of a system 300a in accordance with embodiments discussed herein.

[0011] FIG. 4 illustrates a routine 400 in accordance with embodiments.

[0012] FIG. 5 illustrates a routine 500 in accordance with embodiments.

[0013] FIG. 6 illustrates a routine 600 in accordance with embodiments.

[0014] FIG. 7 illustrates an example of a system 700 in accordance with embodiments.

[0015] FIG. 8 illustrates an example of a system 800 in accordance with embodiments.

[0016] FIG. 9 illustrates a contactless card 102 in accordance with one embodiment.

[0017] FIG. 10 illustrates a transaction card component 1000 in accordance with one embodiment.

[0018] FIG. 11 illustrates a sequence flow 1100 in accordance with one embodiment.

[0019] FIG. 12 illustrates a data structure 1200 in accordance with one embodiment.

[0020] FIG. 13 is a diagram of a key system according to an example embodiment.

[0021] FIG. 14 is a flowchart of a method of generating a cryptogram according to an example embodiment.

[0022] FIG. 15 illustrates an aspect of the subject matter in accordance with one embodiment.

[0023] FIG. 16 illustrates an aspect of the subject matter in accordance with one embodiment.

DETAILED DESCRIPTION

[0024] Embodiments may be generally directed to systems configured to provide improved one-tap rental services for items using a token, such as a contactless card. For example, embodiments discussed may be configured to enable users to rent items, such as scooters, bikes, chairs, cars, kayaks, paddleboards, or any other type of equipment by tapping their contactless card on a computing device associated with the item. The computing device may be configured to process the information on the card and communicate with one or more servers to provide authentication and payment services for the rental of the item. In embodiments discussed herein may also enable users to purchase services, such as rental time on a computer, access to a streaming service or item, processing time on a cloud computing device and so forth. Embodiments are not limited in this manner.

[0025] The systems discussed herein include computing devices, such as mobile devices, computers, servers, networking equipment, etc., configured to enable verification of the token and the user and rent the item. The solutions discussed herein provide advantages over previous solutions to rent items. Previous systems generally required a user to go through a number of steps or operations to rent an item. A user may be required to download and/or configure an application on their mobile device, set up an account for the item, including providing payment information and interact with the application to rent an item. Embodiments discussed herein provide improvements over previous technology by enabling a user to perform a single operation to rent an item by presenting a contactless card to a computing device that can be used to verify the user and provide payment for the rental. As will be discussed in more detail, the contactless card and the computing device are configured to perform an exchange. The information may be further communicated to one or more servers to authenticate the card and user, and to provide payment for the rental. The operation may also be used as a signature for the user to sign or accept terms and conditions for the rental of the item. These operations can be performed without requiring the user to set up an account and provide secure information to the application and a third-party provider of the application.

[0026] In one example, the computing device associated with the rental item may be configured to provide the information to the servers in an encrypted format generated by the contactless card. The servers may be configured to receive and process encrypted data generated by the contactless card and rental data corresponding to a rental of an item. For example, the systems may be configured to extract authentication information from the encrypted data that may be used to authenticate or verify the contactless card and the user. Specifically, the systems may perform an authentication routine on the authentication information to authenticate the user. The authenticate routine may include ensuring that the encrypted data can be successfully decrypted with a correct key, and the encrypted data, e.g., a shared secret, matches an authentic shared secret stored on the system. In response to authentication of the card and the user, the system may also perform one or more operations to enable the rental of the item, such as providing payment for the item and accepting any terms or conditions.

[0027] In embodiments, the computing device configured to communicate with the contactless card and the servers may be affixed and/or associated with the rental item. The computing device may be configured to communicate wirelessly in accordance with one or more wireless

technologies. For example, the computing device may exchange the data with the contactless card when the card is within a wireless short-range communication range. Specifically, the computing device may be configured to periodically emit signals in accordance with a near-field communication (NFC) protocol to energize and detect the contactless card. The device may receive the encrypted data via one or more communication exchanges, which may include authentication information to authenticate a card and the user, and information to pay for the item. The device may be configured to send, to one or more servers, the encrypted data and data associated with the rental of the item to a system in accordance with different wireless technology, e.g., cellular or WiFi communication. The computing device may also be configured to receive an indication from one or more servers to enable the rental of the item and process the indication. For example, the device may receive the indication based on the user being authenticated and a successful payment for the item. In some instances, the computing device may receive an indication to decline the rental of the time, e.g., when the user is not authenticated and/or payment is not received. If the user is authenticated and payment is received, the device may also be configured to cause an action to permit the rental of the item based on the indication. Additional details are provided in the following description.

[0028] FIG. 1 illustrates an example of a system 100 in accordance with embodiments discussed herein. The system 100 may be configured to provide one-tap authentication and payment services to enable users to rent or purchase items. The illustrated system 100 includes a limited number of systems, devices, components, etc., for simplistic discussion purposes. In an implementation, the system 100 may include any number of systems, device, components, etc., to provide the functionality discussed herein.

[0029] In embodiments, the system 100 is configured to enable users to rent or purchase items, such as item 104. In the illustrated example, the item 104 is a scooter; however, embodiments are not limited in this manner. The item 104 may be any type of item or service that a user may rent or purchase. For example, the item 104 may be any type of vehicle including a scooter, a bicycle, a car, etc. The item may a beach chair, an umbrella, outdoor equipment such as a kayak, a tent, a paddleboard, etc. In some instances, the item 104 may be a service, such as renting time of a computer, processing time, cloud-based storage, etc. Embodiments are not limited to these examples.

[0030] In embodiments, the item 104 may include or have a computing device 106 that may be utilized by a user to rent the item 104. In some instances, the computing device 106 may be

a special-purpose computer configured only to provide rental services for the user. The computing device 106 may include one or more processing components, such as central processing units, processors, graphic processing units, controllers, etc. The computing device also includes volatile memory, non-volatile memory, input/output (I/O) devices, wired and wireless communication interfaces, displays (touchscreen), and so forth that enable a user to interact with the computing device 106. In one example, the computing device 106 may be a single-board computer, including a circuit board having the processor(s), memory, I/O devices, and other features configured to provide the functionality discussed herein. In embodiments, the item 104 and/or computing device 106 may include one or more location determining devices, such as a global positioning system (GPS) device, a location positioning system (LPS) using cellular or WiFi stations and signals, systems using triangulation, and so forth. The location determining device may be utilized to determine the location of the computing device 106 and the item 104. In some instances, the computing device 106 may determine a time based on the signals received from a location determining device, e.g., based on a clock or time signal.

[0031] In embodiments, the computing device 106 is in a housing that is affixed or integrated into the body of the item 104. The computing device 106 may be attached to the item 104 utilizing any type of attaching mechanism or fastener. In some instances, the computing device 106 may be integrated into the item 104, e.g., located in a molded portion of the handle bars or stem of the scooter, such that it cannot be detached from the item 104. In other examples, the computing device 106 may be integrated or affixed to a locking mechanism for the item 104. For example, the computing device 106 may be for a locked storage system (lockers) that enables access to the item 104 once the user is authenticated. As will be discussed in more detail, the computing device 106 may be configured to control (lock/unlock) the locking mechanism based on the card and user being authenticated.

[0032] In embodiments, the computing device 106 includes one or more wireless interfaces configured to communicate with other devices of the system 100. For example, the computing device 106 may include a short-range wireless communication interface configured to communication in accordance with a short-range communication protocol, such as NFC, Bluetooth, any other short range RF protocol, or infrared (IF) protocol. In embodiments, the computing device 106 may utilize the short-range wireless communication interface to communicate with devices, including the contactless card 102.

[0033] In embodiments, the contactless card 102 and the computing device 106 are configured to communicate when they are brought within a short-range wireless communication range of each other, e.g., 10 centimeters for NFC. For example, the computing device 106, including the short-range wireless communication interface, periodically energizes to cause one or more signals to be emitted that further energize circuitry on the contactless card 102 to communicate. The contactless card 102 and computing device 106 may be configured to initiate a communication exchange, such as an NFC communication exchange, to establish a connection between each other and communicate data, for example. In some instances, the user may tap or touch the contactless card 102 to the computing device 106 to ensure that the contactless card 102 is within communication range with the computing device 106 to exchange the data. The data may include a shared secret that may be used to authenticate the card and/or the user, a customer identifier, one or more account numbers, one or more counter values, and so forth. FIG. 9 and FIG. 10 illustrate and discuss more detail with respect to the contactless card 102. In some instances, the contactless card 102 may be configured to encrypt the data to communicate computing device 106. FIG. 11 illustrates one possible sequence 1100 that may be performed between the contactless card 102 and the computing device 106 to exchange data for the authentication operations and FIG. 12 through FIG. 16 illustrate and discuss additional detail for communicating the data in a secure manner utilizing diversified keys.

[0034] In embodiments, the contactless card 102 may generate encrypted data and communicate the data to the computing device 106. The computing device 106, in turn, may communicate the encrypted data to one or more other systems, devices, servers, etc., to authenticate the user and provide payment information. For example, the computing device 106 may utilize one or more wired and wireless networks, such as network 108, to communicate with the system(s) 110.

[0035] Network 108 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 computing device 106 to system(s) 110. For example, network 108 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 802.11 family of standards, IEEE 902.15.x (wireless PAN family), Bluetooth, NFC, Radio Frequency Identification (RFID), Wi-Fi, and/or the like. In addition, network 108 may include hardware and infrastructure, 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 108 may support an Internet Protocol (IP) network, a wireless communication network, a cellular network, or the like, or any combination thereof. Although network 108 is depicted as a single network, it should be appreciated that according to one or more examples, network 108 may include a plurality of interconnected networks.

[0036] In embodiments, the computing device 106 may communicate data to the system(s) 110 via the network 108 to authenticate the user, provide payment information, and enable the user to rent the item 104. In embodiments, the system(s) 110 may be operated by an owner or provider of the item 104 and/or a bank to provide authentication and payment services. For example, the system(s) 110 may be incorporated into a scooter rental system to provide rental scooters in a market, such as in a city. The system(s) 110 may include physical servers in a location operated and maintained by the item provider or may be cloud-based computing servers system(s) 110 that provide services to the item provider on demand.

[0037] In some instances, one or more of the system(s) 110 may include servers maintained and operated by a banking system to provide the authentication services and payments services to rent the item 104. Additionally, the system(s) 110 controlled by the banking system may be associated with the contactless card 102. As will be discussed in more detail in FIGs. 2A and 2B, the system(s) 110 may include a rental server, an authentication server, and a payment server. The rental server may be controlled and operated by the rental company and the authentication server and payment server may be controlled and operated the bank. The rental server may provide rental services and the authentication server and payment server may provide authentication and payment services for the rental of the item 104.

[0038] FIG. 2A illustrates an example display that may be displayed by the computing device 106, including instructions for the user to perform a single-tap operation with a token, such as a contactless card 102, to rent an item.

[0039] In embodiments, the computing device 106 may include a display device, such as a touchscreen display, capable of display text and images. In the illustrated example of FIG. 2A the computing device 106 is configured to display an indication, such as “Tap Card Here to

Rent Item” and image of a contactless card, on the display device. The indication and the image presented on the display device ensures that a user brings the contactless card 102 close enough to the computing device 106 to perform a communication exchange, as described herein.

[0040] In some embodiments, the computing device 106 be configured with a display device of any type including a liquid crystal display (LCD), light-emitting diode (LED) display, a plasma display, or any other type of flat panel system. In some instances, to preserve battery power, the display device may be an electronic ink (e-ink) display configured to display the indications. The e-ink display may hold state and display the indications even when power is not being applied to the display device, saving power and battery usage, for example. In some instances, the computing device 106 may maintain the display device in an off or standby state and may be configured to detect an object, such as a person, near the computing device 106, e.g., via one or more sensors. For example, the computing device 106 may include a proximity sensor configured to detect the person and the computing device 106 may be configured to light the display device and display the indications based upon a detection.

[0041] In embodiments, the computing device 106 may detect the contactless card 102 when it is brought within a communication range of an interface and the computing device 106 and exchange information with the card, as discussed herein.

[0042] FIG. 2B illustrates another example display that may be presented to the user on a display device to rent an item. In the illustrated example, the display may present an indication to review terms and conditions to rent the item, e.g., such as the text “Click Here for Terms & Conditions” and a button. The computing device 106, including the display device may be configured to detect a user selection of the button on the display device and display the terms and conditions for the user to review. The terms and conditions may be stored in memory or retrieved by the computing device 106 via an Internet server.

[0043] In embodiments, the computing device 106 may include an indication for the user to accept the terms and conditions and to initiate rental of the item with a single tap of the contactless card 102. For example, the display device in FIG. 2B may also be configured to present text, such as “Tap Card Here to Rent Item and Accept Terms and Conditions” and an image of the contactless card. As similarly discussed in FIG. 2A, the computing device 106 may detect the contactless card 102 and perform an exchange of data with the contactless card, as discussed herein.

[0044] FIG. 3A illustrates a first example configuration of a system 300a to perform the operations discussed herein, including enabling a user to rent an item 104 with one tap of a contactless card. In the illustrated example, the computing device 106 is coupled with the item 104 and is configured to communicate with a rental system 310, including a rental server 304. In the illustrated example, the rental server 304 is configured to provide a number of services, including authenticating the card, confirming payment, and providing rental management services, e.g., monitoring and tracking one or more items, communicating with items, processing payment for rental of the items, and so forth.

[0045] In embodiments, a user may wish to rent item 104, which may be any type of rental item, as previously discussed. The item 104 may be coupled with a computing device 106, which may be physically affixed to the item 104, molded into the item 104, or located in another housing associated with the item 104. In some embodiments, the computing device 106 may be implemented in storage facility (e.g., a locker) associated with the item 104 and/or control a locking mechanism for the item 104.

[0046] In some embodiments, the computing device 106 is configured such that a user may rent the item 104 with a single tap of a token, such as contactless card 102. For example, the computing device 106 can be configured to periodically scan or attempt to detect a token or the contactless card 102, e.g., by energizing a short-range wireless communication interface, to probe for contactless cards and detect when contactless card 102 is within communication range of the computing device 106. The computing device 106 and/or item 104 may be affixed with a sticker or placard having instructions to the user to bring the contactless card 102 near the computing device 106 to ensure that the contactless card is within communication range. In some embodiments, the instructions may instruct the user to tap the contactless card 102 on the computing device 106. The computing device 106 may also include a display device, such as a flat panel display, a light-emitting diode (LED) display, a liquid crystal display (LCD), or the like configured to display the instructions. In one example, the display may display instructions to tap the card to the display and a graphical representation of the card indicating a location where to tap the card.

[0047] In other instances, the computing device 106 may include one or more interfaces, such as a touchscreen display, and the user may interface with the computing device 106 via the touchscreen display to initiate the rental of the item 104. For example, the computing device 106 may present one or more GUI(s) for the user to make selections, such as an indication to

rent the item 104, an amount of time to rent the item 104, a payment method to rent the item 104, accept terms and conditions for the rental, and so forth. In these instances, the computing device 106 may receive and process user selections corresponding to the parameters of the rental of the item 104 and instruct the user to bring the contactless card 102 near or on the computing device 106 to initiate an exchange with the contactless card 102. In some instances, the computing device 106 may not include a display. In these instances, the user may accept the terms and conditions via universal terms and conditions agreed to upon activation of the contactless card 102 or have previously activated a tap-to-rent feature for the card through a banking system.

[0048] The computing device 106 is configured to initiate a communication exchange with the contactless card 102 when the contactless card 102 is within wireless communication of the computing device 106 based on the communication protocol being used to communicate. For example, the computing device 106 may be configured to communicate in accordance with the NFC protocol and may initiate an NFC exchange with the contactless card 102 when the contactless card 102 is within the NFC communication range, e.g., ~ 10 centimeters (cms). In embodiments, the computing device 106 initiates an exchange with the contactless card 102, and the contactless card 102 sends data to the computing device 106. The data may include authentication information, such as a shared secret, a customer identifier or other unique identifiers. The data may also include information to enable payment for the rental, such as an account number or information associated with the customer's account that may be used to identify the account. In some instances, the contactless card 102 may send the data encrypted.

[0049] For example, the contactless card 102, to send the data to the computing device 106, may generate a message authentication code (MAC) cryptogram. In some examples, this may occur when the contactless card 102 is read by the computing device 106. 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, the computing device 106 may include a reader application configured to perform a read operation to read data from the contactless card 102. The contactless card 102 may generate the message including the cryptogram, which may include a header and the shared secret, a customer identifier or other identifying information, account information, or a combination thereof. The contactless card 102 may generate a MAC cryptogram (encrypted data) from the message, and the MAC cryptogram may be further encrypted, as further discussed in FIG. 11, e.g., with

random data utilizing a diversified or session key. The contactless card 102 may communicate the MAC cryptogram in an NDEF message format responsive to a “Read NDEF file” message received from the computing device 106.

[0050] In some instances, the computing device 106 and the contactless card 102 may exchange data in accordance with the different protocols. For example, communication may occur via Bluetooth, Wi-Fi, or other means of wireless data communication. Embodiments are not limited in this manner.

[0051] In embodiments, the computing device 106 may receive the data from the contactless card 102 and store the data in a memory. In some instances, the computing device 106 may provide an indication to the user that the data is successfully received or not received from the contactless card 102. For example, the computing device 106 may present the indication on a display in a GUI. In other instances, the computing device 106 may provide the indication by lighting one or more light emitting diodes (LEDs) corresponding to whether the data is received or not received.

[0052] The computing device 106 may further initiate a communication with one or more systems to process the rental of the item 104. In the illustrated example, the computing device 106 may send one or more messages to a rental system 310, including a rental server 304. The computing device 106 may send the one or more messages via a network, such as network 108. In embodiments, computing device 106 is configured to communicate in accordance with one or more cellular communication protocols including, but not limited to, Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), cdmaOne, CDMA2000, Evolution-Data Optimized (EV-DO), Enhanced Data Rates for GSM Evolution (EDGE), Universal Mobile Telecommunications System (UMTS), Digital Enhanced Cordless Telecommunications (DECT), Digital AMPS (IS-136/TDMA), Long Term Evolution (LTE), 5th Generation (5G), and Integrated Digital Enhanced Network (iDEN).

[0053] In some instances, the computing device 106 may be configured operate a battery. In embodiments, the battery may be dedicated to the computing device 106 or may be a battery also configured to supply power to the item 104. The computing device 106 may be configured to reduce power consumption to extend the battery life. As one example, the computing device 106 may be configured to communicate with network 108 utilizing a lower-powered cellular technology. For example, the computing device 106 may be configured to communicate utilizing low-power wide-area network (LPWAN) protocol, low-power wide-area (LPWA)

network protocol or low-power network (LPN) protocol, or any other type of wireless telecommunication wide area network designed to allow for long-range communication at a low bit rate.

[0054] In embodiments, the computing device 106 is configured to communicate the messages in accordance with a messaging communication protocol. For example, the computing device 106 may be configured to communicate with the rental server 304 in accordance with publish-subscribe protocol, such as the message queuing telemetry transport (MQTT) protocol configured to operate over transmission control protocol (TCP)/Internet Protocol (IP) or any other network protocol that provides ordered, lossless, bi-directional connections. MQTT may be utilized in implementations that require a small code footprint (reduced availability of memory) and/or low-bandwidth implementations. In one example, the computing device 106 may be configured to publish data, and the rental server 304 may subscribe to the data in accordance with the MQTT protocol. The data may include rental data or information. The rental data may include an item identifier, a date/time of rental, a location of rental, and other parameters of the rental. The data also may include the encrypted data from the contactless card 102. For example, the computing device 106 may publish the cryptogram to communicate the cryptogram to the rental server 304. In embodiments, the communications between the computing device 106 and the rental server 304 may be secured using one or more secure/encryption techniques.

[0055] In embodiments, the computing device 106 and rental server 304 may utilize other message protocols to communicate data. In some implementations, at least a portion of the data may be communicated in accordance with a representational state transfer (RESTful) JavaScript Object Notation (JSON) communication protocol. For example, the computing device 106 is configured to utilize a PUT command to send the data to a location or address of the rental server 304, e.g., <https://rentalserver.com/parameters>, where the parameters may include the rental data (item identifier), date/time, location, etc. In some instances, the computing device 106 may be configured to send the information from the contactless card 102 to the rental server 304 as one or more parameters, e.g., the cryptogram, a token, an account number, a customer name, a CVV, etc. In some implementations, the rental server 304 may be configured to retrieve the data from the computing device 106. For example, the rental server 304 may be configured to execute a GET command to retrieve at least a portion of the data from the computing device 106. Embodiments are not limited to these examples. In some

implementations, the computing device 106 and rental server 304 may communicate data between each utilizing a combination of the MQTT and RESTful JSON messaging protocols and/or additional/different protocols, e.g., extensible markup language (XML) and/or hypertext transfer protocol (HTTP) or secure HTTP (HTTPS).

[0056] The rental server 304 is configured to receive and process the data to enable rental of the item 104. For example, the rental server 304 may store the rental data in a database or data store to track a rent of an item 104. Specifically, the rental server 304 may store an identifier of the item with a start date/time of the rental for the item. For time based rentals, the rental server 304 may also receive an end date/time from the computing device 106 and calculate a cost for the rental to charge the account associated with the contactless card 102. Specifically, the rental server 304 may use the start date/time and the end date/time to calculate a rental time and determine a cost for the rental of the item 104.

[0057] The rental server 304 may also process the data from the contactless card 102 to verify the card and to process payment for the rental of the item 104. In some instances, the rental server 304 may utilize a bank system 308 including an authentication server 302 to authenticate the contactless card 102. For example, the rental server 304 may communicate the cryptogram from the contactless card 102 to the authentication server 302 to authenticate the contactless card. In some embodiments, the rental server 304 may be configured to communicate with the authentication server 302 using RESTful JSON messaging protocol API(s). For example, the rental server 304 may execute a command including calling an authentication method with the cryptogram as a parameter (or information from the cryptogram as parameter(s)) at the location or address of the authentication server 302, e.g., <https://authenticationserver.com/authenticatemethod/parameters>. The authentication server 302 may authenticate the card and/or the user and return a result. Embodiments are not limited to this example implementation and other message protocols/formats may be used to communicate the data from the contactless card 102 to the authentication server 302.

[0058] In embodiments, the authentication server 302 may be part of a bank system 308, e.g., owned and operated by a bank, and is configured to perform authentication operations to authenticate the card and the user. Specifically, the authentication server 302 ensures that the data from the contactless card 102 is valid and the user is authentic. In embodiments, the authentication server 302 may be configured to receive the data and perform one or more

authentication operations, e.g., ensuring that encrypted data is encrypted with a correct key and the data from the contactless card 102 matches stored/authenticated data.

[0059] For example and as discussed in more detail in FIG. 15, the authentication server 302 may confirm when a successful authentication is determined when the following conditions are met. First, the ability to verify the MAC shows that a derived session key was proper for the contactless card 102. The MAC may only be correct if the decryption was successful by the authentication server 302 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 contactless card 102) and the recipient (e.g., the authentication server 302), it may be trusted that the contactless card which originally created the MAC and encrypted the MAC is indeed authentic. Moreover, a 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. Similarly, the authentication server 302 may use other information in the data from the contactless card 102 to authenticate the contactless card 102, e.g., by comparing a shared secret, a customer identifier, or other information stored on the contactless card 102 with authenticated information stored on the authentication server 302. For example, the authentication server 302 may retrieve an authentic shared secret from memory or a database, compare the authentic shared secret with the shared secret from the contactless card 102 and confirm that they may to authenticate the contactless card 102.

[0060] In embodiments, the authentication server 302 authenticates the card and provides an indication to the rental server 304. Specifically, the authentication server 302 may communicate one or more messages to the rental server 304, including an indication as to whether the card is authentic or not authentic based on the data from the contactless card 102. If the card is not authentic, the computing device 106 and/or the rental server 304 prevents the item 104 from being rented, e.g., by maintaining a lock on the item 104, providing an indication to a user via an interface, etc. If the card is authentic, the system 300a, including the computing device 106 and the rental server 304 may continue to process data to enable the user to rent the item 104.

[0061] In some instances, the system 300a may require the user to perform two-factor or multifactor authentication, such that the user associated with contactless card 102 may also be authenticated. Any number of additional authentications may be performed by the

authentication server 302. For example, the system 300a may require the user to provide an additional piece of information, e.g., enter a PIN, a password, an address, a telephone number, etc., to the 106 one or more interfaces that may be provided to the authentication server 302. The authentication server 302 may confirm that the additional piece of information is authenticated and is associated with the contactless card 102. In another example, the authentication server 302 may require and/or determine that the user is in possession of another device, such as a mobile device, by sending a one-time passcode to the device and having the user respond to the code and/or enter the code into the computing device 106, enter the code into a bank app, respond to the message, etc. Additional authentication methods may be used, e.g., authentication applications, to authenticate the user.

[0062] In embodiments, the authentication server 302 may return a result of authentication operations performed to the rental server 304 as one or more messages in accordance with a message protocol. The rental server 304 is configured to process the result and determine whether to proceed with rental of the item 104 or not. For example, if the rental server 304 receives an indication that the card and/or the user is authenticated, the rental server 304 may send one or more messages to the computing device 106 to enable rental of the item 104. The message(s) may include an indication that the rental is permitted. If the card and/or the user cannot be authenticated, the rental server 304 may not permit rental of the item 104 by sending one or more messages indicating the rental is denied to the computing device 106.

[0063] In embodiments, the computing device 106 may receive an indication indicating whether the rental is permitted or not permitted and process the indication accordingly. For example, the computing device 106 may send one or more signals to a locking mechanism to cause a lock to unlock if the rental is permitted. Other examples may include sending one or more signals to a motor to enable the item 104. If the rental of the item 104 is denied, the computing device 106 prevents the item 104 from being rented and may provide an indication to the user, e.g., presenting an indication in a display. Examples may include sending a signal to maintain or release a brake for the item, enable or disable a motor for the item, maintain or release a locking mechanism for the item, and so forth.

[0064] In embodiments, the rental server 304 is configured to process payment for the rental of the item 104. For example, the rental server 304 may utilize the payment server 306 to collect payment for the rental based on the data collected from the contactless card 102 and the rental data. In embodiments, the rental server 304 may determine an amount for the rental,

either at the time of rental or upon completion of the rental (e.g., based on the start time/date and end time/date), and communicate with the payment server 306 to collect the payment from an account associated with contactless card 102 and the user. In one example, the rental server 304 is configured to interface with the payment server 306 via an API to collect payment, e.g., send a payment request. The API may also be a RESTful JSON API and include a payment method that may be called using a GET command by the rental server 304, for example. The rental server 304 may invoke the GET command with the address of the payment server 306 to invoke with the payment method and include one or more parameters to enable the payment server 306 to process the payment, e.g., <https://paymentserver.com/payment> method/parameters. The parameters may include data from the computing device 106, such as the cryptogram, including an account number. The payment server 306 may process the payment by transferring funds from the user's account to an account associated with the rental system 310 and provide an indication to the rental server 304. The indication may indicate that the payment was successful or not successful.

[0065] Although illustrated as two separate servers, the authentication server 302 and payment server 306 may be implemented in the same server or in a cloud-based computing system. Each of the servers may include components such as one or more processors, memory, interfaces, displays, I/O devices, etc., as previously discussed.

[0066] FIG. 3B illustrates a second example of a system 300b configured to perform operations discussed herein. In the illustrated example, the computing device 106 may be configured to communicate directly with the bank system 308 to enable users to rent an item 104.

[0067] In embodiments, the computing device 106 is configured to detect an attempt to rent item 104 and to process communications with the contactless card 102, as discussed above in FIG. 3A. For example, the computing device 106 may perform one or more NFC exchanges to receive encrypted data from the contactless card 102. The encrypted data may be a cryptogram or a MAC cryptogram and include data that may be used to authenticate the card, and in some instances, the user. The data may be received from the contactless card 102 and stored in a memory of the computing device 106 for communication to the bank system 308.

[0068] In embodiments, the computing device 106 is also configured to determine rental data in system 300b in the same manner as discussed in FIG. 3A. For example, the computing device 106 may determine rental data such as a time/date of a rental based on a location device,

such as GPS. The computing device 106 is also configured to determine the status of the item 104 based on one or more sensors of the item 104, e.g., a battery sensor. In some instances, the computing device 106 may determine the amount of time for the rental based on a user input entered via a touchscreen interface or another input device. Embodiments are not limited in this manner.

[0069] In embodiments, the computing device 106 is configured to communicate with the bank system 308 to enable rental of the item 104. For example, the computing device 106 may communicate over a network, such as network 108, to send the encrypted data, the rental data, the payment request, or a combination thereof to the bank system 308. In embodiments, the computing device 106 may be configured to directly communicate with bank system 308 using one or more APIs, such as the MQTT configured and/or the RESTful JSON API(s), in a similar or same manner as the rental system 310 communicates with the bank system 308, e.g., by issue one or more API commands based on a location or address of the bank system 308. For example, to authenticate the card/user, the computing device 106 may call the authentication server 302 at an address via a command, e.g., `https://authenticationserver.com/authenticatemethod/parameters`, wherein the parameters include the cryptogram. Similarly, to obtain payment for the rental, the computing device 106 may call the payment server 306 at an address via a command, such as `https://paymentserver.com/payment method/parameters`, where the parameters include rental data.

[0070] In embodiments, the bank system 308, including the authentication server 302 may perform the authentication operations to authenticate the card, e.g., based on whether the encrypted data can be correctly decrypted and the information on the card matches stored authentic information. In this configuration, the bank system 308 may also be configured to implement two or multi-factor authentication to authenticate user.

[0071] The bank system 308 is configured to return a result of the authentication operation(s) to the computing device 106, e.g., as a return to the API calls. The result may indicate whether the card and/or the user are authentic. If the card and/or the user is not authentic, the computing device 106 prevents the item 104 from being rented, e.g., maintain a lock for the 104. If the card, and in some instances, the user are authenticated, the computing device 106 enables the user to use the item 104, e.g., by sending one or more signals to a locking mechanism to unlock the item 104.

[0072] In some instances, the computing device 106 may know or have determined an amount of time for the rental and calculate a price for the rental. The computing device 106 may communicate the payment request to the bank system 308, including a payment server 306 to process payment. The bank system 308 may return a result indicating was successful or not successful. If payment is not successful, the computing device 106 is configured to prevent the rental of the item 104. If the payment is successful, the computing device 106 is configured to enable rental of the item 104.

[0073] In some instances, the computing device 106 may determine an amount to charge the user based on the amount of time the user utilizes the item 104. For example, the computing device 106 including the location determination device may determine a start time for the rental and an end time for the rental, and the computing device 106 may calculate a total rent time and amount for the rental time. The computing device 106 may send a payment request to the bank system 308 to process the payment.

[0074] In these instances, the computing device 106 may determine the end time based on a time period expiration or an indication entered by a user. When the payment is not received until upon completion of the rental, the computing device 106 may send one or more test payments to bank system 308 to ensure that the payment of the rental will be processed successfully. The test payments may include an arbitrarily nominal amount that may be subjected to the total amount charged at the end of the rental. Embodiments are not limited in this manner.

[0075] FIG. 4 illustrates an example routine 400 that may be performed by systems discussed herein to authenticate and process contactless cards. In embodiments, the routine 400 may be performed by one or more servers of a bank system, such as bank system 308 illustrated in FIG. 2A/2B.

[0076] In block 402, the routine 400 includes receiving encrypted data generated by a contactless card corresponding to a rental of an item. For example, a bank system may receive a cryptogram from a rental system or a computing device via one or more wired or wireless networks. The cryptogram may be encrypted by the contactless card with a diversified key generated with a master key, as described herein. The encrypted data may include a shared secret, a unique identifier, an account number, a CVV, and so forth. In one example, the bank system may be configured with one or more APIs for the rental system and/or computing

device to utilize to call the bank system including an authentication server to communicate the encrypted data.

[0077] In block 404, the routine 400 includes extracting authentication information from the encrypted data. For example, the bank system may generate a diversified key using a stored master key associated with a customer and/or the contactless card and stored in a data store. The bank system may verify that the authentication information is successfully extracted, indicating that the contactless card utilized a correct diversified key to generate the encrypted data. In some instances, the system may apply additional decryption algorithms to extract the data. For example, the encrypted data may be a MAC cryptogram, and the system may apply a message authentication code decryption operation.

[0078] In block 406, the routine 400 includes performing an authentication operation on the authentication information to authenticate the contactless card. In addition to determining the correct diversified key is used to encrypt the data, the system may also compare one or more portions of the data with stored verified data. For example, the system may determine that a shared secret, a unique identifier, an account number, or a combination thereof matches a stored and verified shared secret, unique identifier, and/or account number, etc.

[0079] In block 408, the routine 400 includes sending a result of the authentication operation indicating that the contactless card is authentic (or not authentic). In embodiments, the system may send the result to a rental system and/or a computing device associated with the item based on the requesting device. In some instances, when the authentication operation fails, the result indicates that the contactless card cannot be successfully authenticated.

[0080] In block 410, the routine 400 includes receiving a payment request to pay for the rental of the item. For example, the bank system, including a payment server may receive the payment request in response to the card being successfully authenticated from a rental system or a computing device associated with the item. The payment request may include an amount for payment. In some instances, the payment request may include or be communicated with the encrypted data from the contactless card for the bank system to use to identify an account to use to pay for the rental of the item. In some instances, the payment request may include an indication that the request corresponds with the encrypted data communicated at block 402. In some embodiments, the payment request may be communicated with the encrypted data at block 402, e.g., in one or more messages communicated prior to the card being authenticated. Embodiments are not limited in this manner. The request may include additional information to

process the payment including an identifier to identify an account to receive the payment, a bank name, routing number, account number, a date/time of the transaction, a location, a description, etc. In embodiments, the bank system including the payment server may be configured with one or more APIs that may be used by the rental system and/or the computing device to communicate the payment, as previously discussed.

[0081] In block 412, the routine 400 includes processing the payment request based on information in the encrypted data. In embodiments, the bank system initiates an electronic transfer of funds from the account of the user to the account associated with the item based on the information in the payment request. Embodiments are not limited in this manner.

[0082] In block 414, the routine 400 includes sending a second result of the processing of the payment request indicating that payment is successful for the rental of the item. For example, the bank system may return an indication to the rental system or the computing device indicating that the payment was processed successfully or unsuccessfully.

[0083] FIG. 5 illustrates an example of a routine 500 that may be performed by systems discussed herein. In some embodiments, the routine 500 may be performed by a rental system including a rental server, as illustrated in FIG. 3A.

[0084] In block 502, the routine 500 includes receiving encrypted data stored on a contactless card and rental data corresponding to a rental of an item from a computing device. For example, the rental system may receive the encrypted data and rental data from a computing device affixed and/or associated with the item for rent. In embodiments, the encrypted data may be a cryptogram/MAC cryptogram and the rental data may include data corresponding to rental of the item, as discussed herein.

[0085] In block 504, routine 500 includes sending the encrypted data to one or more servers to perform an authentication routine with the encrypted data. For example, the rental system may send the encrypted data to a bank system to perform one or more operations to authenticate the card and the user. In example embodiments, the rental system may utilize one or more APIs hosted by the bank system to call an authentication method(s)/operation(s) to perform on the encrypted data and pass the encrypted data to the bank system.

[0086] In block 506, the routine 500 includes receiving a result of the authentication routine indicating the contactless card is authentic (or not authentic). For example, the rental system may receive a result from the bank system. In some instances, the result may indicate that the authentication of the card and/or the user is not successful and one or both are not authentic.

[0087] In block 508, the routine 500 includes, in response to authentication of the user, performing one or more operations to enable the rental of the item. For example, the rental system may send an indication to the computing device associated with the item to permit the rental of the item. In some instances, the rental system may request payment for the rental of the item from the bank system. In some embodiments, when the card and/or the user is not authenticated, the rental system may prevent rental of the item, e.g., by sending an indication to the computing device. Embodiments are not limited in this manner.

[0088] FIG. 6 illustrates an example of a routine 600 that may be performed in accordance with embodiments discussed. In instances, the routine 600 may be performed by a computing device, such as computing device 106 that is affixed and/or coupled with an item for rent. The computing device may be configured to provide rental features for users; and as discussed herein, one-tap rental features so that a user may easily tap their contactless card on or near the computing device and proceed with using the item reducing the amount of time and steps needed to rent the item providing more convenience for the user.

[0089] In block 602, the routine 600 includes detecting a contactless card within a near-field communication (NFC) range. For example, a computing device configured to provide rental services for an item may periodically scan for radio-frequency identification tags or devices, such as contactless cards, on a periodic basis in accordance with the ISO/IEC 14443 standard. As discussed, the computing device may be configured with a display that may instruct that the desired user to present their contactless card to the computing device within a defined distances, e.g., 10cms. In some instances, the instructions may instruct the user to tap the card on the computing device, e.g., on the display or other portion of the body or housing of the device. In some instances, the instructions may instruct the user to tap a portion of the item itself, e.g., the body or housing of the item housing the computing device. Note that embodiments are not limited to providing the rental services utilizing NFC and other wireless technologies may be utilized, e.g., Bluetooth, 802.11 standards, ZigBee, etc.

[0090] In some instances, a single tap may be used to rent the item. In other instances, the computing device may present information and data to the user on a display device. For example, the computing device may be configured to present options for the user to select for the rental of the item in a GUI displayed on the display, e.g., an amount of time for the rental. The display may also present other legal obligations for the rental of the item. For example, the rental of the item may require the user to be presented with terms and conditions of the rental

and/or use instructions for the rental in a GUI on the display of the computing device. The computing device including the display, may enable the user to read through these terms and conditions and instructions on the display device. Once the user has read through them, the computing device may instruct the user to tap or bring the contactless card on or near the computing device and the one-tap operation may be used to accept the terms and conditions along with initiate the authentication and payment operations discussed herein.

[0091] In block 604, the routine 600 includes receiving encrypted data from the contactless card, the encrypted data comprising authentication information to authenticate a user. The computing device, in response to the contactless card being brought into communication range, is configured to initiate an exchange with the contactless card. The contactless card may be configured to communicate data to the computing device to be used to authenticate the card and to provide payment. As discussed herein, the contactless card is configured to generate a cryptogram or MAC cryptogram including data for authentication and/or payment. In embodiments, the data includes one or more a shared secret, a unique identifier, a customer identifier, a counter value, or a combination thereof. In some instances, the data may include an account number or other token that may be used for payment. The computing device may request the data as part of an NFC read operation and receive the cryptogram from the contactless card in one or more NFC messages.

[0092] In embodiments, the computing device may receive the data from the card and store the data in memory. In embodiments, the computing device is configured to store the data temporarily in memory ensure that confidential data is not stored permanently on the computing device. The memory may be volatile memory or non-volatile memory and configured to store the data until the data is communicated to one or other devices or systems and deleted by the computing device.

[0093] In block 606, the routine 600 includes sending the encrypted data and/or rental data to a system, the rental data corresponding to a rental of an item. In some embodiments, as discussed in FIG. 3A, the computing device is configured to send the encrypted data and the rental data to a rental system that may process the data to enable the user rent the item. The computing device may send the data over a network, such as network 108, in one or more secure messages, as discussed herein. The encrypted data may include an unaltered MAC cryptogram received from the contactless card, and the rental data may include data

corresponding to the rental, e.g., a date/time of rental, a location of rental, an identifier of the item, a status of the item, etc.

[0094] In some instances, the rental data may include a desired duration for the rental, e.g., two hours, and the rental system may calculate a cost to rent the item for the desired time and retrieve payment from a bank system upfront, as discussed herein. Once the duration is over, the computing device may disable rental of the item, or determine the item is still be used and bill the user additional charges. In other instances, the system including the computing device and the rental system may be configured to not bill the user until the user is done utilizing the item. In these instances, the computing device is configured to determine when the rental of the item has ended. For example, the computing device may receive a user selection via a GUI on a touchscreen display. In another example the computing device may detect a timeout or that the item has not been used for a particular or set amount of time. The computing device, up completion of the rental, is configured to send an end date/time to the rental system to determine the cost of the rental to request payment.

[0095] In some embodiments, as discussed in FIG. 3B, the computing device may be configured to communicate directly with the bank system to authenticate the contactless card, and in some instances, and the user. In these instances, the computing device may send the encrypted data and the rental data to the one or more servers of the bank system. In this configuration, the computing device may determine the amount for the rental of the item based on one or more calculations and may send a payment request to the bank system. In these instances, the computing device may not need to send the rental data to the bank system and may only send the encrypted data to the bank system to perform the authentication operations and the payment request.

[0096] In block 608, the routine 600 includes receiving an indication to enable the rental of the item. For example, the computing device may receive from the rental system that rental of the item is permitted. The computing device may receive the indication from the rental system in response to the successful authentication of the contactless card and, in some instances, payment for the rental. Note that in some instances, the computing device may receive an indication from the rental system to deny the rental of the item.

[0097] In some instances, the computing device may receive an indication from the bank system. The indication from the bank system may indicate that the card is successfully (or not) authenticated. The indicate whether the user is authenticated or not. When payment is collected

prior to rental of item, the computing device may also receive an indication from the bank system that payment for the rental was successful or not.

[0098] In block 610, the routine 600 includes causing an action to permit the rental of the item based on the indication. For example, the computing device may send a signal to a locking mechanism to unlock a lock for the item. Other examples may include sending one or more signals to apply power to the item, enable a motor of the item, provide an indication to the user on a display, etc. In embodiments, when the card and/or the user is not authenticated or payment is not able to be collected, the computing device may prevent the user from renting the item. For example, the computing device may maintain a lock for the item, prevent power from being applied, etc. Embodiments are not limited to these examples.

[0099] FIG. 7 illustrates a data transmission system 700 according to an example embodiment. As further discussed below, system 700 may include contactless card 102, computing device 106, network 702, and server 704. Although FIG. 7 illustrates single instances of the components, system 700 may include any number of components.

[0100] System 700 may include one or more contactless cards 102, which are further explained below. In some embodiments, contactless card 102 may be in wireless communication, utilizing NFC in an example, with computing device 106.

[0101] System 700 may include computing device 106, 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 106 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.

[0102] The computing device 106 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 tamper proofing 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.

[0103] In some examples, computing device 106 of system 700 may execute one or more applications, such as software applications, that enable, for example, network communications with one or more components of system 700 and transmit and/or receive data.

[0104] The computing device 106 may be in communication with one or more server(s) 704 via one or more network(s) 702, and may operate as a respective front-end to back-end pair with server 704. The computing device 106 may transmit, for example from a mobile device application executing on computing device 106, one or more requests to server 704. The one or more requests may be associated with retrieving data from server 704. The server 704 may receive the one or more requests from computing device 106. Based on the one or more requests from computing device 106, server 704 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 704 may be configured to transmit the received data to computing device 106, the received data being responsive to one or more requests.

[0105] System 700 may include one or more networks 702. In some examples, network 702 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 computing device 106 to server 704. For example, network 702 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 802.11 family, 802.15 family or other IEEE 802 communication protocols, Bluetooth, NFC, Radio Frequency Identification (RFID), Wi-Fi, and/or the like.

[0106] In addition, network 702 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 702 may support an Internet network, a wireless communication network, a cellular network, or the like, or any combination thereof. network 702 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 702 may utilize one or more protocols of one or more network elements to which they are communicatively coupled. network 702 may translate to or from other protocols to one or more protocols of network devices. Although network 702 is depicted as a single network, it should be appreciated that according to one or more examples, network 702 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.

[0107] System 700 may include one or more servers 704. In some examples, server 704 may include one or more processors, which are coupled to memory. The server 704 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 704 may be configured to connect to the one or more databases. The server 704 may be connected to at least one computing device 106.

[0108] FIG. 8 illustrates a data transmission system according to an example embodiment. System 800 may include a transmitting or transmitting device 804, a receiving or receiving device 808 in communication, for example via network 806, with one or more servers 802. Transmitting or transmitting device 804 may be the same as, or similar to, client device 106 discussed above with reference to FIG. 1A. Receiving or receiving device 808 may be the same as, or similar to, client device 110 discussed above with reference to FIG. 1A. Network 806 may be similar to network 115 discussed above with reference to FIG. 1A. Server 802 may be similar to server 120 discussed above with reference to FIG. 1A. Although FIG. 8 shows single instances of components of system 800, system 800 may include any number of the illustrated components.

[0109] 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.

[0110] 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.

[0111] 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.

[0112] 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.

[0113] Referring back to FIG. 8, system 800 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 804 and 808. As explained above, although single instances of transmitting device 804 and receiving device 808 may be included, it is understood that one or more transmitting devices 804 and one or more receiving devices 808 may be involved so long as each party shares the same shared secret symmetric key. In some examples, the transmitting device 804 and receiving device 808 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 804 and similarly any party holding the same secret symmetric key may perform the functions of the receiving device 808. 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 804 and the receiving device 808 involved in exchanging the secure data. It is further understood that both the transmitting device 804 and receiving device 808 may be provided with the same master symmetric key, and further that part of the data exchanged between the transmitting device 804 and receiving device 808 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 804 and the receiving device 808.

[0114] 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 one or more transmitting devices 804 and one or more receiving devices 808 to server 802. 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 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 802.11 family, 802.15 family, Bluetooth, NFC, RFID, Wi-Fi, and/or the like.

[0115] 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.

[0116] In some examples, one or more transmitting devices 804 and one or more receiving devices 808 may be configured to communicate and transmit and receive data between each other without passing through network 806. For example, communication between the one or more transmitting devices 804 and the one or more receiving devices 808 may occur via at least one of NFC, Bluetooth, RFID, Wi-Fi, and/or the like.

[0117] At block 810, when the transmitting device 804 is preparing to process the sensitive data with symmetric cryptographic operation, the sender may update a counter. In addition, the transmitting device 804 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.

[0118] At block 812, the transmitting device 804 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 804 and the receiving device 808. The transmitting device 804 may then encrypt the counter value with the selected symmetric encryption algorithm using the master symmetric key, creating a diversified symmetric key.

[0119] In some examples, the counter value may not be encrypted. In these examples, the counter value may be transmitted between the transmitting device 804 and the receiving device 808 at block 812 without encryption.

[0120] At block 814, the diversified symmetric key may be used to process the sensitive data before transmitting the result to the receiving device 808. For example, the transmitting device 804 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 804 may then transmit the protected encrypted data, along with the counter value, to the receiving device 808 for processing.

[0121] At block 816, the receiving device 808 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.

[0122] At block 818, the receiving device 808 may then take the protected encrypted data and using a symmetric decryption algorithm along with the diversified symmetric key, decrypt the protected encrypted data.

[0123] At block 820, as a result of the decrypting the protected encrypted data, the original sensitive data may be revealed.

[0124] The next time sensitive data needs to be sent from the sender to the recipient via respective transmitting device 804 and receiving device 808, 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 804 and receiving device 808 may independently produce the same diversified symmetric key. This diversified symmetric key, not the master symmetric key, is used to protect the sensitive data.

[0125] As explained above, both the transmitting device 804 and receiving device 808 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 804 and receiving device 808, 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 804 and the receiving device 808 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 804 and receiving device 808.

[0126] 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 804 to the receiving device 808; the full value of a counter value sent from the transmitting device 804 and the receiving device 808; a portion of a counter value sent from the transmitting device 804 and the receiving device 808; a counter independently maintained by the transmitting device 804 and the receiving device 808 but not sent between the two devices; a one-time-passcode exchanged between the transmitting device 804 and the receiving device 808; 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.

[0127] 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 804 and the receiving device 808. In effect, this may create a one-time use key, such as a single-use session key.

[0128] FIG. 9 illustrates an example configuration of a contactless card 102, 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 902 on the front or back of the contactless card 102. In some examples, the contactless card 102 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 102 may include a substrate 908, 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 102 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 102 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.

[0129] The contactless card 102 may also include identification information 906 displayed on the front and/or back of the card, and a contact pad 904. The contact pad 904 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 102 may also include processing circuitry, antenna and other components as will be further discussed in FIG. 10. These components may be located behind the contact pad 904 or elsewhere on the substrate 908, e.g. within a different layer of the substrate 908, and may electrically and physically coupled with the contact pad 904. The contactless card 102 may also include a magnetic strip or tape, which may be located on the back of the card (not shown in FIG. 9). The contactless card 102 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.

[0130] As illustrated in FIG. 2, the contact pad 904 of contactless card 102 may include processing circuitry 1016 for storing, processing, and communicating information, including a processor 1002, a memory 1004, and one or more interface(s) 1006. It is understood that the processing circuitry 1016 may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamper proofing hardware, as necessary to perform the functions described herein.

[0131] The memory 1004 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 102 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 1004 may be encrypted memory utilizing an encryption algorithm executed by the processor 1002 to encrypted data.

[0132] The memory 1004 may be configured to store one or more applet(s) 1008, one or more counter(s) 1010, a customer identifier 1014, and the account number(s) 1012, which may be virtual account numbers. The one or more applet(s) 1008 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) 1008 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) 1010 may comprise a numeric counter sufficient to store an integer. The customer identifier 1014 may comprise a unique alphanumeric identifier assigned to a user of the contactless card 102, and the identifier may distinguish the user of the contactless card from other contactless card users. In some examples, the customer identifier 1014 may identify both a customer and an account assigned to that customer and may further identify the contactless card 102 associated with the customer's account. As stated, the account number(s) 1012 may include thousands of one-time use virtual account numbers associated with the contactless card 102. An applet(s) 1008 of the contactless card 102 may be configured to manage the account number(s) 1012 (e.g., to select an account number(s) 1012, mark the selected account number(s) 1012 as used, and transmit the account number(s) 1012 to a mobile device for autofilling by an autofilling service.

[0133] The processor 1002 and memory elements of the foregoing exemplary embodiments are described with reference to the contact pad 904, but the present disclosure is not limited thereto. It is understood that these elements may be implemented outside of the contact pad 904 or entirely separate from it, or as further elements in addition to processor 1002 and memory 1004 elements located within the contact pad 904.

[0134] In some examples, the contactless card 102 may comprise one or more antenna(s) 1018. The one or more antenna(s) 1018 may be placed within the contactless card 102 and around the processing circuitry 1016 of the contact pad 904. For example, the one or more antenna(s) 1018 may be integral with the processing circuitry 1016 and the one or more antenna(s) 1018 may be used with an external booster coil. As another example, the one or more antenna(s) 1018 may be external to the contact pad 904 and the processing circuitry 1016.

[0135] In an embodiment, the coil of contactless card 102 may act as the secondary of an air core transformer. The terminal may communicate with the contactless card 102 by cutting

power or amplitude modulation. The contactless card 101 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 102 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) 1018, processor 1002, and/or the memory 1004, the contactless card 101 provides a communications interface to communicate via NFC, Bluetooth, and/or Wi-Fi communications.

[0136] As explained above, contactless card 102 may be built on a software platform operable on smart cards or other devices having limited memory, such as JavaCard, and one or more or more applications or applets may be securely executed. Applet(s) 1008 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) 1008 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.

[0137] One example of an NDEF OTP is an NDEF short-record layout (SR=1). In such an example, one or more applet(s) 1008 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) 1008 may be configured to add one or more static tag records in addition to the OTP record.

[0138] In some examples, the one or more applet(s) 1008 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) 1008, 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.

[0139] In some examples, the contactless card 102 and server may include certain data such that the card may be properly identified. The contactless card 102 may include one or more unique identifiers (not pictured). Each time a read operation takes place, the counter(s) 1010 may be configured to increment. In some examples, each time data from the contactless card 102 is read (e.g., by a mobile device), the counter(s) 1010 is transmitted to the server for

validation and determines whether the counter(s) 1010 are equal (as part of the validation) to a counter of the server.

[0140] The one or more counter(s) 1010 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) 1010 has been read or used or otherwise passed over. If the counter(s) 1010 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) 1010 since there is no communication between applet(s) 1008 on the contactless card 102.

[0141] In some examples, the counter(s) 1010 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) 1010 may increment but the application does not process the counter(s) 1010. In some examples, when the mobile device 10 is woken up, NFC may be enabled and the device 110 may be configured to read available tags, but no action is taken responsive to the reads.

[0142] To keep the counter(s) 1010 in sync, an application, such as a background application, may be executed that would be configured to detect when the mobile device 110 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 1010 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) 1010 may be configured to move forward. But if within a different threshold number, for example within 10 or 1400, 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) 1010 increases in the appropriate sequence, then it possible to know that the user has done so.

[0143] The key diversification technique described herein with reference to the counter(s) 1010, 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.

[0144] During the creation process of the contactless card 102, 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 102. 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.

[0145] 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 102 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).

[0146] 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.

[0147] 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.

[0148] FIG. 11 is a timing diagram illustrating an example sequence for providing authenticated access according to one or more embodiments of the present disclosure. Sequence flow 1100 may include contactless card 102 and computing device 106, which may include an application 1102 and processor 1104.

[0149] At line 1108, the application 1102 communicates with the contactless card 102 (e.g., after being brought near the contactless card 102). Communication between the application 1102 and the contactless card 102 may involve the contactless card 102 being sufficiently close

to a card reader (not shown) of the computing device 106 to enable NFC data transfer between the application 1102 and the contactless card 102.

[0150] At line 1106, after communication has been established between computing device 106 and contactless card 102, contactless card 102 generates a message authentication code (MAC) cryptogram. In some examples, this may occur when the contactless card 102 is read by the application 1102. 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 1102, 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 102 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).

[0151] 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 1102 may be configured to transmit a request to contactless card 102, the request comprising an instruction to generate a MAC cryptogram.

[0152] At line 1110, the contactless card 102 sends the MAC cryptogram to the application 1102. 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 1112, the application 1102 communicates the MAC cryptogram to the processor 1104.

[0153] At line 1114, the processor 1104 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 computing device 106, such as a server of a banking system in data communication with the computing device 106. For example, processor 1104 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.

[0154] FIG. 12 illustrates an NDEF short-record layout (SR=1) data structure 1200 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.

[0155] FIG. 13 illustrates a diagram of a system 1300 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.

[0156] Regarding master key management, two issuer master keys 1302, 1326 may be required for each part of the portfolio on which the one or more applets is issued. For example, the first master key 1302 may comprise an Issuer Cryptogram Generation/Authentication Key (Iss-Key-Auth) and the second master key 1326 may comprise an Issuer Data Encryption Key (Iss-Key-DEK). As further explained herein, two issuer master keys 1302, 1326 are diversified into card master keys 1308, 1320, which are unique for each card. In some examples, a network

profile record ID (pNPR) 522 and derivation key index (pDKI) 1324, as back office data, may be used to identify which Issuer Master Keys 1302, 1326 to use in the cryptographic processes for authentication. The system performing the authentication may be configured to retrieve values of pNPR 1322 and pDKI 1324 for a contactless card at the time of authentication.

[0157] 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 1308 and Card-Key-Dek 1320). The session keys (Aut-Session-Key 1332 and DEK-Session-Key 1310) may be generated by the one or more applets and derived by using the application transaction counter (pATC) 1304 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 1304 is used. In some examples, the four byte session key derivation method may comprise: $F1 := \text{PATC}(\text{lower 2 bytes}) \parallel 'F0' \parallel '00' \parallel \text{PATC}(\text{four bytes})$ $F1 := \text{PATC}(\text{lower 2 bytes}) \parallel '0F' \parallel '00' \parallel \text{PATC}(\text{four bytes})$ $SK := \{ (\text{ALG}(\text{MK})[F1]) \parallel \text{ALG}(\text{MK})[F2] \}$, where ALG may include 3DES ECB and MK may include the card unique derived master key.

[0158] As described herein, one or more MAC session keys may be derived using the lower two bytes of pATC 1304 counter. At each tap of the contactless card, pATC 1304 is configured to be updated, and the card master keys Card-Key-AUTH 908 and Card-Key-DEK 1320 are further diversified into the session keys Aut-Session-Key 1332 and DEK-Session-KEY 1310. pATC 1304 may be initialized to zero at personalization or applet initialization time. In some examples, the pATC counter 1304 may be initialized at or before personalization, and may be configured to increment by one at each NDEF read.

[0159] 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.

[0160] 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 block size may be used, or the output may be automatically, or manually, padded to a multiple of that block size.

[0161] The MAC may be performed by a function key (AUT-Session-Key) 1332. 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 1332, 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 1332 may be used to MAC data 1306, and the resulting data or cryptogram A 1314 and random number RND may be encrypted using DEK-Session-Key 1310 to create cryptogram B or output 1318 sent in the message.

[0162] 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 1310 derived from the Card-Key-DEK 1320. In this case, the ATC value for the session key derivation is the least significant byte of the counter pATC 1304.

[0163] 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			

[0164] 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			

[0165] The UID field of the received message may be extracted to derive, from master keys Iss-Key-AUTH 902 and Iss-Key-DEK 1326, the card master keys (Card-Key-Auth 1308 and Card-Key-DEK 1320) for that particular card. Using the card master keys (Card-Key-Auth 908 and Card-Key-DEK 1320), the counter (pATC) field of the received message may be used to derive the session keys (Aut-Session-Key 1332 and DEK-Session-Key 1310) for that particular

card. Cryptogram B 1318 may be decrypted using the DEK-Session-KEY, which yields cryptogram A 1314 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 1314, 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.

[0166] 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 1332. The input data 1306 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.

[0167] 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.

[0168] 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 1312, data 1306 is processed through the MAC using Aut-Session-Key 1332 to produce MAC output (cryptogram A) 1314, which is encrypted.

[0169] In order to provide additional protection against brute force attacks exposing the keys on the card, it is desirable that the MAC cryptogram 1314 be enciphered. In some examples, data or cryptogram A 1314 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 1310. In the encryption operation 1316, data or cryptogram A 1314 and RND are processed using DEK-Session-Key 610 to produce encrypted data, cryptogram B 1318. The data 1314 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.

[0170] 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.

[0171] FIG. 14 illustrates a method 1400 for generating a cryptogram. For example, at block 1402, 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.

[0172] At block 1404, 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.

[0173] At block 1406, 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.

[0174] At block 1408, 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.

[0175] FIG. 15 depicts an exemplary process 1500 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 block 1502, and other data, such as data to be protected, which it may secure share with the recipient.

[0176] At block 1504, 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.

[0177] 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.

[0178] At block 1506, 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).

[0179] At block 1508, 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).

[0180] At block 1510, 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.

[0181] At block 1512, the recipient uses the received counter value to independently derive the two derived session keys from the two master keys as explained above.

[0182] At block 1514, 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.

[0183] At block 1516, 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.

[0184] 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.

[0185] Thereafter, the two derived session keys may be discarded, and the next iteration of data exchange will update the counter value (returning to block 1502) and a new set of session keys may be created (at block 1510). In some examples, the combined random data may be discarded.

[0186] FIG. 16 illustrates a method 1600 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 a, such as contactless card 102, computing device 106, and a server.

[0187] In block 1602, 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.

[0188] In block 1604, 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.

[0189] In block 1606, 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.

[0190] In block 1608, 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.

[0191] In block 1610, 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.

WHAT IS CLAIMED

1. A system configured to perform authentication and payment operations based on data stored in contactless cards, comprising:

one or more servers comprising one or more processors and memory, the memory coupled with the one or more processors and configured to store instructions that when executed by the one or more processors, cause the one or more processors to:

receive, from a rental system, a payment request and encrypted data generated by a contactless card corresponding to a rental of an item;

perform one or more authentication operations on the encrypted data to authenticate the contactless card;

process the payment request based on information in the encrypted data; and

send, to the rental system, an indication that the contactless card is authenticated and that payment is successful for the rental of the item.

2. The system of claim 1, wherein the encrypted data comprises authentication information further comprising a unique identifier to identify the contactless card, and the authentication information encrypted with a diversified key and one or more cryptographic algorithms by the contactless card to generate the encrypted data.

3. The system of claim 2, wherein the authentication information further comprises a counter value the one or more processors, to perform the one or more authentication operations to verify the counter value based on a stored counter value.

4. The system of claim 2, wherein the authentication information comprises a shared secret, and the one or more processors, to perform the one or more authentication operations to verify the shared secret with a stored share secret.

5. The system of claim 1, wherein the encrypted data is encrypted with a diversified key generated from a master key by the contactless card, and the one or more processors to perform the authentication operation to:

generate a second diversified key using a stored master key;

decrypt the encrypted data with the second diversified key; and

verify the encrypted data is successfully decrypted with the second diversified key.

6. The system of claim 1, wherein sending the indication of the one or more authentication operations indicates acceptance of terms and conditions for the rental of the item.
7. The system of claim 1, wherein the one or more processors to receive the encrypted data based on a command of an application programming interface (API) invoked by a rental server of the rental system invoking an authentication method.
8. The system of claim 1, wherein the one or more processors to receive the payment request based on a command of an application programming interface (API) invoked by a rental server on the rental system invoking a payment method.
9. A server configured to enable rental of items based on authentication operations performed with data stored in contactless cards, comprising:
 - one or more processors;
 - memory coupled with the one or more processors, the memory to store instructions that when executed by the one or more processors, cause the one or more processors to:
 - receive, from a computing device, encrypted data stored on a contactless card and rental data corresponding to a rental of an item;
 - send the encrypted data to one or more servers to perform an authentication operation with the encrypted data;
 - receive, from the one or more servers, a result of the authentication operation indicating the contactless card is authentic;
 - in response to authentication of the contactless card, a user, or a combination thereof, perform one or more operations to enable the rental of the item.
10. The server of claim 9, wherein the encrypted data comprises a shared secret, a unique identifier, or a combination thereof, and the encrypted data encrypted with a diversified key and one or more cryptographic algorithms.
11. The server of claim 9, wherein the rental data comprises one or more of an identifier to identify the item, a price associated with the rental of the item, terms and conditions associated with the rental of the item, or a combination thereof.
12. The server of claim 9, the one or more processors to:

send at least a portion of the encrypted data, the rental data, or a combination thereof to the one or more servers; and

receive, in response to sending a portion of the rental data, payment for the rental of the item.

13. The server of claim 9, the one or more processors to:

send at least a portion of the encrypted data, rental data, or a combination thereof to the one or more servers; and

receive, in response to sending the portion of the rental data, an indication of acceptance of terms and conditions for the rental of the item.

14. The server of claim 9, the one or more processors to send, to a computing device associated with the item, an indication the rental of the item is approved.

15. The server of claim 9, the one or more processors to send, to the computing device, an indication the rental of the item is disapproved.

16. A computing device, comprising:

processing circuitry;

memory coupled with the processing circuitry, the memory to store instructions that when executed by the processing circuitry, cause the processing circuitry to:

detect a contactless card within a near-field communication (NFC) range;

receive, via one or more NFC exchanges, encrypted data from the contactless card, the encrypted data comprising authentication information to authenticate a user;

send, to one or more servers, the encrypted data and rental data, the rental data corresponding to a rental of an item;

receive, from the one or more servers, an indication to enable the rental of the item; and

cause an action to permit the rental of the item based on the indication.

17. The computing device of claim 16, wherein the computing device is affixed to the item.

18. The computing device of claim 16, wherein item is a vehicle, and the action is to send a signal to release a brake of the vehicle.

19. The computing device of claim 16, wherein the item is a vehicle, and the action is to send a signal to enable a motor of the vehicle.

20. The computing device of claim 16, wherein the item is a chair, and the action is to send a signal to release a lock associated with the chair.