AUGMENTED REALITY CARD ACTIVATION EXPERIENCE

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Patent Application Serial No. 16/872,572, entitled "AUGMENTED REALITY CARD ACTIVATION EXPERIENCE" filed on May 12, 2020 (issued as U.S. Patent No. 10,963,865 on March 30, 2021). The contents of the aforementioned patent application are incorporated herein by reference in their entirety.

BACKGROUND

[0002] When a new card (e.g., debit card, credit card, etc.) arrives in the mail, an authorized user is required to activate the card in order to use it. There are various forms of activation. For example, the user can activate the card by calling a telephone number indicated on a sticker adhered to the card, performing various authentication steps, and speaking with a live or automated agent. In another example, the user can activate the card by opening up a web browser, logging in the user's online account, performing various authentication steps, and pressing an activation icon. In either example, the activation experience can be uninformative and dull.

SUMMARY

[0003] Various embodiments are generally directed to enhancing a card activation experience for an authorized card user when activating a new card by at least displaying various types of information related to the new card in augmented reality (AR) and allowing the user to perform the activation itself or experience other aspects of the activation process in AR. Information pertaining the successful activation of the card may also be provided to the user in AR.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] **FIG. 1A** illustrates an example data transmission system in accordance with one or more embodiments.

[0005] **FIG. 1B** illustrates an example sequence diagram for providing authenticated access in accordance with one or more embodiments.

[0006] **FIG. 2** illustrates an example system using a contactless card in accordance with one or more embodiments.

[0007] **FIG. 3A** illustrates an example contactless card in accordance with one or more embodiments.

[0008] **FIG. 3B** illustrates an example contact pad of a contactless card in accordance with one or more embodiments.

[0009] **FIG. 4** illustrate example URL readings in accordance with one or more embodiments.

[0010] **FIG. 5** illustrates an example interface flow for downloading a banking app, user registration, and card activation initiation in accordance with one or more embodiments.

[0011] **FIG. 6** illustrates a first example of card information displayed in augmented reality (AR) in accordance with one or more embodiments.

[0012] **FIG. 7** illustrates a second example of card information displayed in AR in accordance with one or more embodiments.

[0013] **FIG. 8** illustrate example card activation actions in accordance with one or more embodiments.

[0014] **FIG. 9** illustrates an example flow diagram in accordance with one or more embodiments.

DETAILED DESCRIPTION

[0015] Various embodiments are generally directed to enhancing the card activation experience for an authorized card user by at least displaying various types of information related to the new card in augmented reality (AR) and allowing the user to perform the activation or experience various aspects of the activation process in AR.

[0016] In embodiments, during the activation experience, various information and selectable options related to the card may be displayed in AR. For instance, if the card is a credit card, information such as the annual percentage rate (APR) of the card, credit limit, payment due date, or the like may be displayed around or adjacent to the card in AR. Other types of information may also be displayed in AR, such as information associated with one or more different types of components (e.g., hardware, software, etc.) contained in the card or various graphics (e.g., contactless graphic) depicted on the card. In another instance, selectable options related to the card such as adding or removing authorized users or setting up auto payment may also be displayed in AR. Moreover, instructions related to the activation process may be displayed and experienced in AR. It may be understood that, in AR, the information and selectable options may remain in predefined display positions relative to the card even if the physical position of the camera changes.

[0017] In embodiments, upon an authorized card user (e.g., banking customer) receiving a new card (e.g., credit card, debit card, business card), the user may tap the card to the user's mobile device (e.g., smartphone). When the card is tapped to the mobile device, the mobile device may read a uniform resource locator (URL) from the card via near field communication (NFC). In examples, the URL may direct the user to a download location for downloading a banking application (otherwise referred to herein as "banking app") if the banking application is not already on the mobile device. If the user already has the banking app on the mobile device, the banking app may be launched instead. It may be understood that the term "tap" or "tapped"

may broadly be referred to as brining the card physically close to the mobile device such that the NFC reader coil of the mobile device can read or receive data from the card.

[0018] For example, the banking app may launch upon download and the user may be guided through a registration process if the user is a new customer. Otherwise, existing customer may login to the banking app. As will be further described below, existing customers may be able to login to the banking app using "one-tap" authentication, which is a highly secure way of verifying user identity to ensure, for example, that is the user who is actually logging in to the banking app and not a fraudster.

[0019] In embodiments, the card activation experience may begin in the banking app. For instance, the user may be instructed to point a camera of the mobile device at the card. As described above, various types of information related to the card and/or user selectable options may be displayed in AR. In a further instance, in AR, the border of the card may be outlined in a first color (e.g., red) to indicate that the card has not yet been activated. Instructions may also be provided to user in AR for completing the activation process. In one example, the user may again tap the card to the mobile device, which proceeds to activate the card. When the card is placed back in front of the camera, the border of the card may be outlined in a second color different from the first color (e.g., green) to indicate that the card has been activated. In another example, while in AR view, the user can physically tap the card with a finger, which completes the activation process. The border of the card can again be outlined in a particular color.

[0020] In previous solutions, the card activation experience lacked excitement and was generally uninformative. The embodiments and examples described herein overcome and are advantageous over the previous solutions in that a user can experience card activation in new, exciting, and informative ways. Allowing the user to interact with the card in AR during card activation engages the user in the process. Moreover, it is advantageous in allowing the user to change card-related options, such as the addition or subtraction of authorized users or setting up auto payment, also enhances the activation experience.

[0021] Reference is now made to the drawings, where like reference numerals are used to refer to like elements throughout. In the following description, for the purpose of explanation, numerous specific details are set forth in order to provide a thorough understanding thereof. It may be evident, however, that the novel embodiments can be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form to facilitate a description thereof. The intention is to cover all modification, equivalents, and alternatives within the scope of the claims.

[0022] **FIG. 1A** illustrates an example data transmission system according to one or more embodiments. As further discussed below, system 100 may include contactless card 105, client

device 110, network 115, and server 120. Although FIG. 1A illustrates single instances of the components, system 100 may include any number of components.

[0023] System 100 may include one or more contactless cards 105, which are further explained below with reference to FIG. 3A and FIG. 3B. In some embodiments, contactless card 105 may be in wireless communication, utilizing NFC in an example, with client device 110.

[0024] System 100 may include client device 110, 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 smartphone, a handheld PC, a personal digital assistant, a thin client, a fat client, an Internet browser, or other device. Client device 110 also may be a mobile computing device, for example, an iPhone, iPod, iPad from Apple® or any other suitable device running Apple's iOS® operating system, any device running Microsoft's Windows® Mobile operating system, any device running Google's Android® operating system, and/or any other suitable mobile computing device, such as a smartphone, a tablet, or like wearable mobile device.

[0025] The client device 110 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, anti-collision algorithms, controllers, command decoders, security primitives and tamper-proofing hardware, as necessary to perform the functions described herein. The client device 110 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.

[0026] In some examples, client device 110 of system 100 may execute one or more applications, such as software applications, that enable, for example, network communications with one or more components of system 100 and transmit and/or receive data.

[0027] Client device 110 may be in communication with one or more servers 120 via one or more networks 115 and may operate as a respective front-end to back-end pair with server 120. Client device 110 may transmit, for example from a mobile device application executing on client device 110, one or more requests to server 120. The one or more requests may be

associated with retrieving data from server 120. Server 120 may receive the one or more requests from client device 110. Based on the one or more requests from client device 110, server 120 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 120 may be configured to transmit the received data to client device 110, the received data being responsive to one or more requests.

[0028] System 100 may include one or more networks 115. In some examples, network 115 may be one or more of a wireless network, a wired network or any combination of wireless network and wired network and may be configured to connect client device 110 to server 120. For example, network 115 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 802.11b, 802.15.1, 802.11n and 802.11g, Bluetooth, NFC, Radio Frequency Identification (RFID), Wi-Fi, and/or the like.

[0029] In addition, network 115 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 115 may support an Internet network, a wireless communication network, a cellular network, or the like, or any combination thereof. Network 115 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 115 may utilize one or more protocols of one or more network elements to which they are communicatively coupled. Network 115 may translate to or from other protocols to one or more protocols of network devices. Although network 115 is depicted as a single network, it should be appreciated that according to one or more examples, network 115 may include a plurality of interconnected networks, such as, for example, the Internet, a service provider's network, a cable television network, corporate networks, such as credit card association networks, and home networks.

[0030] System 100 may include one or more servers 120. In some examples, server 120 may include one or more processors, which are coupled to memory. Server 120 may be configured as a central system, server or platform to control and call various data at different times to execute a plurality of workflow actions. Server 120 may be configured to connect to the one or more databases. Server 120 may be connected to at least one client device 110.

[0031] **FIG. 1B** illustrates an example sequence diagram for providing authenticated access according to one or more embodiments. The diagram may include contactless card 105 and client device 110, which may include an application 122 and processor 124. FIG. 1B may reference similar components as illustrated in FIG. 1A.

[0032] At step 102, the application 122 communicates with the contactless card 105 (e.g., after being brought near the contactless card 105). Communication between the application 122 and the contactless card 105 may involve the contactless card 105 being sufficiently close to a card reader (not shown) of the client device 110 to enable NFC data transfer between the application 122 and the contactless card 105.

[0033] At step 104, after communication has been established between client device 110 and contactless card 105, the contactless card 105 generates a message authentication code (MAC) cryptogram. In some examples, this may occur when the contactless card 105 is read by the application 122. 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.

[0034] For example, a reader, such as application 122, 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 105 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).

[0035] 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).

[0036] In some examples, application 122 may be configured to transmit a request to contactless card 105, the request comprising an instruction to generate a MAC cryptogram.

[0037] At step 106, the contactless card 105 sends the MAC cryptogram to the application 122. 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.

[0038] At step 108, the application 122 communicates the MAC cryptogram to the processor 124. At step 112, the processor 124 verifies the MAC cryptogram pursuant to an instruction from the application 122. For example, the MAC cryptogram may be verified, as explained below.

[0039] In some examples, verifying the MAC cryptogram may be performed by a device other than client device 110, such as a server 120 in data communication with the client device 110 (as shown in FIG. 1A). For example, processor 124 may output the MAC cryptogram for transmission to server 120, which may verify the MAC cryptogram.

[0040] 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.

[0041] It may be understood that in some examples, the contactless card 105 may initiate communication after the contactless card is brought near the client device 110. By way of example, the contactless card 105 may send the client device 110 a message, for instance, indicating that the contactless card has established communication. Thereafter, the application 122 of client device 110 may proceed to communicate with the contactless card at step 102, as described above.

[0042] **FIG. 2** illustrates an example system 200 using a contactless card. System 200 may include a contactless card 205, one or more client devices 210, network 215, servers 220, 225, one or more hardware security modules 230, and a database 235. Although FIG. 2 illustrates single instances of the components, system 200 may include any number of components.

[0043] System 200 may include one or more contactless cards 205, which are further explained below with respect to FIG. 3A and FIG. 3B. In some examples, contactless card 205 may be in wireless communication, for example NFC communication, with client device 210. For example, contactless card 205 may include one or more chips, such as a radio frequency identification chip, configured to communication via NFC or other short-range protocols. In other embodiments, contactless card 205 may communicate with client device 210 through other means including, but not limited to, Bluetooth, satellite, Wi-Fi, wired communications, and/or any combination of wireless and wired connections. According to some embodiments, contactless card 205 may be configured to communicate with card reader 213 (which may otherwise be referred to herein as NFC reader, NFC card reader, or reader) of client device 210 through NFC when contactless card 205 is within range of card reader 213. In other examples,

communications with contactless card 205 may be accomplished through a physical interface, e.g., a universal serial bus interface or a card swipe interface.

[0044] System 200 may include client device 210, which may be a network-enabled computer. As referred to herein, a network-enabled computer may include, but is not limited to: e.g., a computer device, or communications device including, e.g., a server, a network appliance, a personal computer, a workstation, a mobile device, a phone, a handheld PC, a personal digital assistant, a thin client, a fat client, an Internet browser, or other device. One or more client devices 210 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 or like wearable mobile device. In some examples, the client device 210 may be the same as, or similar to, a client device 110 as described with reference to FIG. 1A or FIG. 1B.

[0045] Client device 210 may be in communication with one or more servers 220 and 225 via one or more networks 215. Client device 210 may transmit, for example from an application 211 executing on client device 210, one or more requests to one or more servers 220 and 225. The one or more requests may be associated with retrieving data from one or more servers 220 and 225. Servers 220 and 225 may receive the one or more requests from client device 210. Based on the one or more requests from client device 210, one or more servers 220 and 225 may be configured to retrieve the requested data from one or more databases 235. Based on receipt of the requested data from the one or more databases 235, one or more servers 220 and 225 may be configured to transmit the received data to client device 210, the received data being responsive to one or more requests.

[0046] System 200 may include one or more hardware security modules (HSM) 230. For example, one or more HSMs 230 may be configured to perform one or more cryptographic operations as disclosed herein. In some examples, one or more HSMs 230 may be configured as special purpose security devices that are configured to perform the one or more cryptographic operations. The HSMs 230 may be configured such that keys are never revealed outside the HSM 230, and instead are maintained within the HSM 230. For example, one or more HSMs 230 may be configured to perform at least one of key derivations, decryption, and MAC operations. The one or more HSMs 230 may be contained within, or may be in data communication with, servers 220 and 225.

[0047] System 200 may include one or more networks 215. In some examples, network 215 may be one or more of a wireless network, a wired network or any combination of wireless network and wired network, and may be configured to connect client device 210 to servers 220

and/or 225. For example, network 215 may include one or more of a fiber optics network, a passive optical network, a cable network, a cellular 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 802.11b, 802.15.1, 802.11n and 802.11g, Bluetooth, NFC, RFID, Wi-Fi, and/or any combination of networks thereof. As a non-limiting example, communications from contactless card 205 and client device 210 may include NFC communication, cellular network between client device 210 and a carrier, and Internet between the carrier and a back-end.

[0048] In addition, network 215 may include, without limitation, telephone lines, fiber optics, IEEE Ethernet 802.3, a wide area network, a wireless personal area network, a local area network, or a global network such as the Internet. In addition, network 215 may support an Internet network, a wireless communication network, a cellular network, or the like, or any combination thereof. Network 215 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 215 may utilize one or more protocols of one or more network elements to which they are communicatively coupled. Network 215 may translate to or from other protocols to one or more protocols of network devices. Although network 215 is depicted as a single network, it should be appreciated that according to one or more examples, network 215 may include a plurality of interconnected networks, such as, for example, the Internet, a service provider's network, a cable television network, corporate networks, such as credit card association networks, and home networks.

[0049] In various examples according to the present disclosure, client device 210 of system 200 may execute one or more applications 211, and include one or more processors 212, and one or more card readers 213. For example, one or more applications 211, such as software applications, may be configured to enable, for example, network communications with one or more components of system 200 and transmit and/or receive data. It is understood that although only single instances of the components of client device 210 are illustrated in FIG. 2, any number of devices 210 may be used. Card reader 213 may be configured to read from and/or communicate with contactless card 205. In conjunction with the one or more applications 211, card reader 213 may communicate with contactless card 205. In examples, the card reader 213 may include circuitry or circuitry components, e.g., NFC reader coil, that generates a magnetic field to allow communication between the client device 210 and the contactless card 205.

[0050] The application 211 of any of client device 210 may communicate with the contactless card 205 using short-range wireless communication (e.g., NFC). The application 211 may be configured to interface with a card reader 213 of client device 210 configured to communicate with a contactless card 205. As should be noted, those skilled in the art would understand that a distance of less than twenty centimeters is consistent with NFC range.

[0051] In some embodiments, the application 211 communicates through an associated reader (e.g., card reader 213) with the contactless card 205.

[0052] In some embodiments, card activation may occur without user authentication. For example, a contactless card 205 may communicate with the application 211 through the card reader 213 of the client device 210 through NFC. The communication (e.g., a tap of the card proximate the card reader 213 of the client device 210) allows the application 211 to read the data associated with the card and perform an activation. In some cases, the tap may activate or launch application 211 and then initiate one or more actions or communications with an account server 225 to activate the card for subsequent use. In some cases, if the application 211 is not installed on client device 210, a tap of the card against the card reader 213 may initiate a download of the application 211 (e.g., navigation to an application download page). Subsequent to installation, a tap of the card may activate or launch the application 211, and then initiate (e.g., via the application or other back-end communication) activation of the card. After activation, the card may be used in various transactions including commercial transactions.

[0053] According to some embodiments, the contactless card 205 may include a virtual payment card. In those embodiments, the application 211 may retrieve information associated with the contactless card 205 by accessing a digital wallet implemented on the client device 210, wherein the digital wallet includes the virtual payment card. In some examples, virtual payment card data may include one or more static or dynamically generated virtual card numbers.

[0054] Server 220 may include a web server in communication with database 235. Server 225 may include an account server. In some examples, server 220 may be configured to validate one or more credentials from contactless card 205 and/or client device 210 by comparison with one or more credentials in database 235. Server 225 may be configured to authorize one or more requests, such as payment and transaction, from contactless card 205 and/or client device 210.

[0055] **FIG. 3A** illustrates one or more contactless cards 300, which may include a payment card, such as a credit card, debit card, or gift card, issued by a service provider 305 displayed on the front or back of the card 300. In some examples, the contactless card 300 is not related to a payment card, and may include, without limitation, an identification card. In some examples, the payment card may include a dual interface contactless payment card. The contactless card 300 may include a substrate 310, 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 300 may have physical characteristics compliant with the ID-1 format of the ISO/IEC 7810 standard, and the contactless card may otherwise be compliant with the ISO/IEC 14443 standard. However, it is understood that the contactless card 300 according to the present disclosure may have different characteristics, and the present disclosure does not require a contactless card to be implemented in a payment card.

[0056] The contactless card 300 may also include identification information 315 displayed on the front and/or back of the card, and a contact pad 320. The contact pad 320 may be configured to establish contact with another communication device, such as a user device, smart phone, laptop, desktop, or tablet computer. The contactless card 300 may also include processing circuitry, antenna and other components not shown in FIG. 3A. These components may be located behind the contact pad 320 or elsewhere on the substrate 310. The contactless card 300 may also include a magnetic strip or tape, which may be located on the back of the card (not shown in FIG. 3A).

[0057] As illustrated in **FIG. 3B**, the contact pad 320 of FIG. 3A may include processing circuitry 325 for storing and processing information, including a microprocessor 330 and a memory 335. It is understood that the processing circuitry 325 may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anti-collision algorithms, controllers, command decoders, security primitives and tamper-proofing hardware, as necessary to perform the functions described herein.

[0058] The memory 335 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 300 may include one or more of these memories. A read-only memory may be factory programmable as read-only or one-time programmable. One-time programmability provides the opportunity to write once then read many times. A write once/read-multiple memory may be programmed at a point in time after the memory chip has left the factory. Once the memory is programmed, it may not be rewritten, but it may be read many times. A read/write memory may be programmed and re-programed many times after leaving the factory. It may also be read many times.

[0059] The memory 335 may be configured to store one or more applets 340, one or more counters 345, one or more diversified keys 347, one or more customer identifiers 350, and one or more uniform resource locators (URLs). The one or more applets 340 may include one or more software applications configured to execute on one or more contactless cards, such as Java Card applet. However, it is understood that applets 340 are not limited to Java Card applets, and

instead may be any software application operable on contactless cards or other devices having limited memory. The one or more counters 345 may include a numeric counter sufficient to store an integer. As will be further described below, the one or more diversified keys 347 may be used to encrypt various information, such as information about the user or customer (e.g., customer identifier 450) to generate cryptogram(s) that can be sent to, for example, a mobile device for at least authentication purposes. The customer identifier 350 may include a unique alphanumeric identifier assigned to a user of the contactless card 300, and the identifier may distinguish the user of the contactless card from other contactless card users. In some examples, the customer identifier 350 may identify both a customer and an account assigned to that customer and may further identify the contactless card associated with the customer's account. The one or more URLs 355 may include unique addresses associated with a World Wide Web page or the like, and in some instance, may be generated by the processing circuitry 325 based on a URL generation event (e.g., the card 300 is tapped to a computing device).

[0060] The processor and memory elements of the foregoing exemplary embodiments are described with reference to the contact pad, but the present disclosure is not limited thereto. It is understood that these elements may be implemented outside of the pad 320 or entirely separate from it, or as further elements in addition to processor 330 and memory 335 elements located within the contact pad 320.

[0061] In some examples, the contactless card 300 may include one or more antennas 355. The one or more antennas 355 may be placed within the contactless card 300 and around the processing circuitry 325 of the contact pad 320. For example, the one or more antennas 355 may be integral with the processing circuitry 325 and the one or more antennas 355 may be used with an external booster coil. As another example, the one or more antennas 355 may be external to the contact pad 320 and the processing circuitry 325.

[0062] In an embodiment, the coil of contactless card 300 may act as the secondary of an air core transformer. The terminal may communicate with the contactless card 300 by cutting power or amplitude modulation. The contactless card 300 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 300 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.

[0063] As explained above, the contactless cards 300 may be built on a software platform operable on smart cards or other devices having limited memory, such as JavaCard, and one or more or more applications or applets may be securely executed. Applets may be added to contactless cards to provide a one-time password (OTP) for multifactor authentication (MFA) in

various mobile application-based use cases. Applets 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, and produce an NDEF message that includes a cryptographically secure OTP encoded as an NDEF text tag.

[0064] In examples, when preparing to send data (e.g., to a mobile device, to a server, etc.), the contactless card 300 may increment a counter value of a counter of the one or more counters 345. The contactless card 300 may then provide a master key, which may be a distinct key stored on the card 300, and the counter value as input to a cryptographic algorithm, which produces a diversified key as output, which may be one of the diversified keys 347. It is understood that the master key and the counter value is also stored in memory of a device or component receiving data from the contactless card 300 so as to decrypt the data using the diversified key that was used by the card to encrypt the transmitted data. The cryptographic algorithm may include encryption algorithms, hash-based message authentication code (HMAC) algorithms, cipher-based message authentication code (CMAC) algorithms, and the like. Non-limiting examples of the cryptographic algorithm may include a symmetric encryption algorithm such as 3DES or AES128; a symmetric HMAC algorithm, such as HMAC-SHA-256; and a symmetric CMAC algorithm such as AES-CMAC. The contactless card 300 may then encrypt the data (e.g., the customer identifier 350 and any other data) using the diversified key in the form of one or more cryptograms that can be sent to a mobile device, for example, as NFC data exchange format (NDEF) messages. The contactless card 300 may then transmit the encrypted data (e.g., cryptograms) to the mobile device, which can then decrypt the cryptograms using the diversified key (e.g., the diversified key generated by the mobile device using the counter value and the master key stored in memory thereof).

[0065] **FIG. 4** illustrates example URL readings 400 and 460 according to one or more embodiments. In one example, an authorized card user may receive a new card 402 (e.g., credit card, debit card, contactless card). To start the activation experience, the user may be instructed to tap the card 402 to the user's mobile device 404 (e.g., smartphone, tablet, any portable computing device). In some examples, the instructions may be presented to the user by way of a sticker adhered to the card 402. It may be understood that tapping the card 402 to the mobile device 404 may broadly refer to the card being in sufficient or requisite proximity to the mobile device 404 such that at least one near field communication (NFC) reader coil of the mobile device 404 is able to communicate (e.g., read or receive data) with the card 402. As shown in URL reading 400, when the card 402 is tapped to or brought near the mobile device 404, the mobile device 404 can read or receive a URL from the card 402. For instance, the URL may be one or more of the URLs 355 stored in card 300, as described above with respect to FIG. 3B.

[0066] In another example, the authorized card user may receive the new card 402 in an envelope 462 (e.g., in the mail). As illustrated in URL reading 460, the envelope 462 may include a sticker 464, or in some examples, a Quick Response (QR) code 466 (as shown by the dashed lines). The sticker 464 or the QR code 466 may be placed or arranged inside of the envelope 462 for security purposes, which can be accessed by tearing or ripping the envelope 462 open. In other instance, the sticker 464 or QR code 466 may be provided on separate paper, which the authorized user can pull out of the envelope 462.

[0067] The user may then be instructed to tap the mobile device 404 to the sticker 464 (or, vise verse, tap the sticker 464 to the mobile device 404) to read or receive the URL. In embodiments, the sticker 464 may be an NFC-enabled sticker that provides the URL via NFC communication. In other embodiments, the sticker may include a graphic that can be scanned by the mobile device 404 allowing the device 404 to obtain the URL. For instance, the graphic can be the URL itself, which the camera of the mobile device 404 can be configured to read. The QR code 466 may provide similar functionalities as the sticker 464, which can be read or scanned by the camera of the mobile device 404 to acquire the URL.

[0068] **FIG. 5** illustrates an example interface flow 500 for downloading a banking app, user registration, and card activation initiation according to one or more embodiments. Upon reading or receiving a URL from the card (or sticker or QR code), as described above with respect to FIG. 4, the URL directs or redirects the mobile computing device to a download location for downloading a banking app, which, for example, may be a World Wide Web page. As illustrated, the user may land on a download interface 502 if the user does not already have the banking app installed on the mobile device. In examples, the download interface 502 may include screen 504 that indicates the requisite banking app has not yet been downloaded to the mobile device and instructs the user to download the banking app. To do so, the user may select or press the icon 506, which begins the download process.

[0069] After the banking app has been downloaded, the mobile device may automatically launch the app. As illustrated in screen 508, a banking app 510 may request that the user complete registration via the begin registration icon 512. The registration process may involve the user providing personal information or other types of user-related information involved in setting up a user account, such as creating a username, password, and setting up one-tap authentication, which will be further described below. Once the registration process has been completed by the user, the banking app 510 may instruct the user to initiate the activation process. For example, screen 514 may ask the user to point the camera of the mobile device at the card and press the begin activation icon 516. In other examples, the user can select the begin activation icon 516 first and then point the camera at the card.

[0070] In other embodiments, the banking app 510 may already be downloaded and installed on the mobile device. In that instance, the banking app may be automatically opened and launched when the mobile device reads or receives the URL from the card, as indicated by the dashed lines in FIG. 5. As shown, the user may be instructed to login to the banking app 510 via screen 520. To login, the user may perform one or more various types of authentication. For example, the user may login by providing a username and password. In another example, the user may perform one-tap authentication to login.

[0071] According to embodiments, one-tap authentication may involve the user placing, tapping, or bringing near a contactless card to a designated area of the user's mobile device. The user computing device may detect the contactless card via near field communication (NFC) and receive one or more cryptograms from the contactless card. Information contained in the cryptogram(s), which may identify the true owner of the contactless card, may be compared or matched against authentication information related to the user logging in to the banking app. If they match, a successful user identity verification can be confirmed. In some examples, the contactless card used to perform the one-tap authentication may be an already existing, active card belonging to the user. In other examples, the new card—the card that is being activated—may be used to perform the one-tap authentication. It may be understood that a cryptogram may broadly refer to any encrypted text, data, or information. It may further be understood that the one or more cryptograms may be received as NFC data exchange format (NDEF) messages.

[0072] In examples, the one or more received cryptograms may contain information at least identifying the user or other related information indicating that the card belongs to a particular user. For instance, the card-user information may be any type of data or information (e.g., ID number, customer number, etc.) associating the contactless card to the user, which may be created or established when the contactless card is created for the user and/or at backend systems when the user signs up or applies for the contactless card. Afterwards, the information contained in the one or more received cryptograms may be matched or compared against authentication information associated with the user to verify the identity of the user. The authentication information is any type of data or information identifying the user signed-in to the banking app (e.g., ID number, customer number, etc.).

[0073] In one example, the banking app 510 may receive the one or more cryptograms from the contactless card and send the cryptogram(s) to one or more remote computing devices, which may be secure backend servers, to perform the decryption of the cryptograms and determine whether the information contained in the one or more cryptograms match authentication information related to the user. The one or more remote computing devices may then send to the banking app 510 an indication or confirmation of verification of the user's identity. In at least

that regard, most (if not all) of the identity verification process may be performed at one or more secure and remote computing devices, which may be advantageous in certain applications or use cases.

[0074] In another example, the banking app 510 may be configured to decrypt the one or more cryptograms received from the contactless card using at least one key (e.g., a private key, a decryption key, a key corresponding to a specific encryption-decryption scheme). The banking app 510 may securely access or receive authentication information related to the user from one or more remote computing devices, such as backend servers. The authentication information may contain at least an identifier or any information indicating the identity of the user logged into the banking app 510. The banking app 510 may then determine whether the received authentication information and the decrypted cryptogram information received from the contactless card match to verify that the contactless card actually belongs to the user and/or to verify that the user is actually the user claims to be.

[0075] Upon successful verification and authentication of the user's identity, the banking app 510 may display an indication that the user has successfully logged in. Thereafter, the user may continue with the card activation experience within the banking app 510, as will be further described below.

[0076] **FIG. 6** illustrates card information 600 displayed in augmented reality (AR) according to one or more embodiments. When the customer card 402 (e.g., front-side forward) is placed in front of the camera of the user's mobile device, the banking app 510 may display various types of card information in AR during the activation experience.

[0077] As shown, card information 600 may include an annual percentage rate (APR) associated with the customer card 402 and may be displayed in AR adjacent to the card. For example, the APR may be eighteen percent. As further shown, a line or any suitable indicator may virtually connect the APR information to the card. The line or indicator may be any color, size, thickness, shape, etc. that allows the information to be easily read or deciphered by the user. Moreover, credit limit information may be displayed in AR (e.g., $25,000) adjacent to the card 402. Further, payment due date information may also be displayed adjacent to the card. As shown, for instance, a minimum payment may be due every fifth of each month.

[0078] In further embodiments, user selectable options associated with the customer card may also be displayed adjacent to the card in AR. The user selectable options may be related to, for instance, adding or subtracting authorized card users or setting up or modifying autopay. As illustrated, the user may be able to interact with the "change" icon displayed in AR under the "authorized users" AR component. In response to touching, pressing, or otherwise selecting the change icon, the user may be able to add, subtract, or modify authorized users of the customer

card 402. Similarly, the user may select or press the "change" icon under the "setup autopay" AR component. In response, the user may be able to enroll or disenroll in autopay or modify features associated therewith.

[0079] In yet further embodiments, other types of information, such as information related to components graphically depicted or physically indicated on the customer card 402 itself, may be displayed adjacent to the card in AR. As shown, information related to the embedded microchip may be displayed (e.g., "chip enabled" or "NFC enabled"). If the customer is a new customer, words of appreciation can be displayed next to the customer's name (e.g., "you're new! Thank you for banking with us!"). In other examples, next to the electronic funds transfer company graphic (e.g., company facilitating the exchange of funds associated with the card transactions), the user may select the "view" icon under the "see merchants that support this card" AR component to view information regarding the respective merchants or businesses that support the customer card 402.

[0080] In examples, a border or outline of the customer card 402 can be color coded in AR to indicate activation-related information. For instance, the border 604 customer card 402 may be outlined in red to indicate that the card 402 has not yet been activated and thus cannot be used at merchants. As will be further described below, upon completing the activation process, the border 604 of the card 402 may be outlined in green to indicate that the user has successfully activated the card.

[0081] As further illustrated, at least two activation instructions may be displayed in AR underneath the customer card 402, both of which will be further explained below with respect to at least FIG. 8. In one example, the user may be instructed to tap the card 402 to the mobile device to complete the activation experience. In another example, the user may be instructed to physically tap the card with the user's finger to complete the activation experience.

[0082] Since the user may view the card information 600 in AR from different angles and at different positions, it may be understood that the banking app 510 may be configured to perform automatic scaling or scale-to-fit procedures such that the card information 600 remain displayed in their respective and correct positions relative to the customer card 402 regardless of the differing viewing angles or positions.

[0083] **FIG. 7** illustrates card information 700 displayed in augmented reality (AR) according to one or more embodiments. As shown, the backside of the customer card 402 may be placed in front of the camera of the user's mobile device during the activation experience, which causes the banking app 510 to display card information 700 in AR.

[0084] Similar to the card information 600, described above, card information 700 may also include various types of information about different components (graphical or otherwise)

arranged, depicted, or illustrated on the back of the card 402. For example, information related to the graphic or symbol indicating that the customer card 402 is contactless may be virtually displayed adjacent to the card and read "Your card is contactless, which means you can simply tap the card to pay or perform other actions." In a further example, information related to the magnetic stripe may displayed in AR adjacent to the stripe and state "You can swipe your card the old-fashioned way."

[0085] Moreover, reminder information may be displayed in AR, such as "Don't forget to sign your card after you activate" adjacent to the signature line. In yet another example, various facts can be displayed, such as "Fun Fact: We have over 700 branches and numerous café locations" adjacent to the card issuer graphic on the back of the customer card 402. And similar to the border 604 described above, a border 704 may be displayed around the card 402 and may be color-coded (e.g., red) to indicate that the card still has not yet been activated.

[0086] In examples, the card activation experience may be advantageously enhanced by the banking app 510 seamlessly transitioning AR display from information 600 to information 700 as the user flips the customer card 402 from the front-side to the backside, and transitioning AR display from information 700 to information 600 as the user flips the card 402 from the backside to the front-side. In at least that regard, the user may be able to enjoy a wholly interactive card activation experience in augmented reality with the physical card itself.

[0087] **FIG. 8** illustrate example card activation actions 800 according to one or more embodiments. At least two different activation actions are shown: tapping the customer card 402 to the mobile device 404 and tapping the card 402 itself with the user's finger.

[0088] After the user has experienced the display of the card information 600 and 700 in AR, the user may wish to complete the activation experience and officially activate the card. In one example, the user may tap the customer card 402 to the mobile device 404, which the banking app 510 may detect, to activate the card. Upon detecting that the card 402 has been tapped, the mobile device 404 via the banking app 510 may communicate with one or more backend servers to signal that a card activation action has been performed and to confirm official activation of the card so that the customer card 404 is active and ready for use. After tapping the card to the phone, the user may place the card 402 back in front of the camera of the mobile device 404. As shown, a border 802 around the card 402 may now be color-coded, e.g., in green, to indicate that the card has been successfully activated.

[0089] In another example, the user may tap the customer card 402 with the user's finger in front of the camera of the mobile device 404. Similar to the card tapping action, this finger tapping action may cause the banking app 510 to communicate with the one or more backend servers to complete the activation process. As further illustrated, a border 804 around the card

402 may also be color-coded, e.g., in green, to indicate that the card has been successfully activated and ready for use.

[0090] **FIG. 9** illustrates an example flow diagram 900 according to one or more embodiments. The flow diagram 900 is related to enhancing a card activation experience by displaying various types of card information in augmented reality. It may be understood that the blocks of the flow diagram 900 and the features described therein are not required to be performed in any particular order. Moreover, it may be understood that the flow diagram 900 and the features described therein may be executed by one or more processors.

[0091] At block 902, a plurality of images of a customer card may be received by a camera of, e.g., a mobile computing device. The customer card may be a new card associated with an authorized user that requires activation and may be placed in front of the camera. The images may be processed by a banking app, which may be downloaded and installed (if not already downloaded and installed on the mobile device) via a URL reading, as described above.

[0092] At block 904, information related to the customer card may be displayed in augmented reality (AR). In examples, information such as the credit limit, annual percentage rate, and due date of monthly minimum payments may be displayed adjacent to the card. In further examples, information related to selectable options associated with the card, such as adding or subtracting authorized users and setting up autopay may be displayed. The user may select an AR icon to change these options, as described above. Moreover, information related to various components arranged on or graphically or textually depicted on the card may be displayed. For example, "chip enabled" may be displayed in AR adjacent to the card chip. Other types of information, such as a statement thanking the customer for being a customer can be displayed next to the customer's name on the card. Card information for both the front and back of the card may be displayed in AR.

[0093] At block 906, an activation action for the customer card may be detected. As described above, the activation action may be tapping the card to the mobile device. In another example, the action may be tapping the card with the user's finger. When the activation action is detected, the customer card may be activated at block 908. The successful activation of the card may be communicated to the user by displaying an indication in AR, such as color coding, e.g., in green, the outline of the card.

[0094] The components and features of the devices described above may be implemented using any combination of discrete circuitry, application specific integrated circuits (ASICs), logic gates and/or single chip architectures. Further, the features of the devices may be implemented using microcontrollers, programmable logic arrays and/or microprocessors or any combination of the foregoing where suitably appropriate. It is noted that hardware, firmware

and/or software elements may be collectively or individually referred to herein as "logic" or "circuit."

[0095] At least one computer-readable storage medium may include instructions that, when executed, cause a system to perform any of the computer-implemented methods described herein.

[0096] Some embodiments may be described using the expression "one embodiment" or "an embodiment" along with their derivatives. These terms mean that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment. Moreover, unless otherwise noted the features described above are recognized to be usable together in any combination. Thus, any features discussed separately may be employed in combination with each other unless it is noted that the features are incompatible with each other.

[0097] With general reference to notations and nomenclature used herein, the detailed descriptions herein may be presented in terms of program procedures executed on a computer or network of computers. These procedural descriptions and representations are used by those skilled in the art to most effectively convey the substance of their work to others skilled in the art.

[0098] A procedure is here, and generally, conceived to be a self-consistent sequence of operations leading to a desired result. These operations are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It proves convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like. It should be noted, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to those quantities.

[0099] Further, the manipulations performed are often referred to in terms, such as adding or comparing, which are commonly associated with mental operations performed by a human operator. No such capability of a human operator is necessary, or desirable in most cases, in any of the operations described herein, which form part of one or more embodiments. Rather, the operations are machine operations.

[00100] Some embodiments may be described using the expression "coupled" and "connected" along with their derivatives. These terms are not necessarily intended as synonyms for each other. For example, some embodiments may be described using the terms "connected"

and/or "coupled" to indicate that two or more elements are in direct physical or electrical contact with each other. The term "coupled," however, may also mean that two or more elements are not in direct contact with each other, but yet still co-operate or interact with each other.

[00101] Various embodiments also relate to apparatus or systems for performing these operations. This apparatus may be specially constructed for the required purpose and may be selectively activated or reconfigured by a computer program stored in the computer. The procedures presented herein are not inherently related to a particular computer or other apparatus. The required structure for a variety of these machines will appear from the description given.

[00102] It is emphasized that the Abstract of the Disclosure is provided to allow a reader to quickly ascertain the nature of the technical disclosure. It is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, it can be seen that various features are grouped together in a single embodiment for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter lies in less than all features of a single disclosed embodiment. Thus, the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separate embodiment. In the appended claims, the terms "including" and "in which" are used as the plain-English equivalents of the respective terms "comprising" and "wherein," respectively. Moreover, the terms "first," "second," "third," and so forth, are used merely as labels, and are not intended to impose numerical requirements on their objects.

[00103] What has been described above includes examples of the disclosed architecture. It is, of course, not possible to describe every conceivable combination of components and/or methodologies, but one of ordinary skill in the art may recognize that many further combinations and permutations are possible. Accordingly, the novel architecture is intended to embrace all such alterations, modifications and variations that fall within the spirit and scope of the appended claims.