

SYSTEM FOR VALUE LOADING ONTO IN-VEHICLE DEVICE**RELATED APPLICATIONS**

[0001] This application claims priority to U.S. Patent Application Serial No. 16/514,427, titled “SYSTEM FOR VALUE LOADING ONTO IN-VEHICLE DEVICE” filed on July 17, 2019. The contents of the aforementioned application are incorporated herein by reference in their entirety.

BACKGROUND

[0002] Today, more and more transactions are carried out within vehicles. For example, a toll transponder arranged within a vehicle may be used to pay tolls as the vehicle passes through toll booths or passes by transponder readers. In another example, a garage transponder or badge may be used to enter and park a vehicle in a parking garage. Other types of in-vehicle transactions may involve payment for drive-through services, event access parking passes, and the like.

[0003] Typically, customers load value onto payment devices, such as the above-described toll and garage transponders, badges, etc., by logging into an online account and entering payment information. Often times, however, customers need to load payment onto the devices in time-constrained circumstances, e.g., immediately prior to approaching a toll booth.

[0004] Accordingly, there is a need for a quick and efficient way to load value onto an in-vehicle device.

SUMMARY

[0005] Various embodiments are directed to using a near-field communication (NFC) contactless card to perform one or more transactions within a vehicle. For example, a user may load value (money, funds, digital currency, etc.) onto an in-vehicle device

(transponder, badge, card, etc.) by performing one-tap authentication or one-tap payment, or both, via the contactless card. Thus, even under time-constrained circumstances, payment may be loaded to the in-vehicle device in a quick, efficient, and safe manner.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] FIG. 1A illustrates an example data transmission system in accordance with one or more embodiments.

[0007] FIG. 1B illustrates an example sequence diagram for providing authenticated access in accordance with one or more embodiments.

[0008] FIG. 2 illustrates an example system using a contactless card in accordance with one or more embodiments.

[0009] FIG. 3A illustrates an example contactless card in accordance with one or more embodiments.

[0010] FIG. 3B illustrates an example contact pad of a contactless card in accordance with one or more embodiments.

[0011] FIG. 4 illustrates an example sequence diagram relating to secure password generation in accordance with one or more embodiments.

[0012] FIG. 5 illustrates an example password generation for a password manager application in accordance with one or more embodiments.

[0013] FIG. 6 illustrates another example of a sequence diagram relating to secure password generation in accordance with one or more embodiments.

[0014] FIG. 7 illustrates another example of password generation for a website in accordance with one or more embodiments.

DETAILED DESCRIPTION

[0015] Various embodiments are generally directed to a system for loading value (e.g., money) onto an in-vehicle device using at least a contactless near-field communication (NFC) smartcard. In examples, the in-vehicle device may be any suitable

device arranged or located within a vehicle and may be used to perform various transactions. In some examples, the in-vehicle device may be built into the vehicle.

[0016] According to one embodiment, the in-vehicle device may be a toll transponder. When a user wishes to reload or add funds onto an existing web-based account corresponding to the toll transponder, the user may tap a mobile computing device, such as a smartphone, to the toll transponder, which may read one or more types of account-related information so that the mobile computing device can access the account. Thus, when the smartphone, for instance, is tapped, the smartphone may read a uniform resource locator (URL) from the toll transponder, which allows the smartphone to launch a toll-specific payment application or a website. The user may then tap a contactless smartcard to the smartphone to reload the account. In examples, the reload amount may be a predetermined value set by the user, e.g., \$20. It may be understood that a toll transponder may be just an example of the in-vehicle device and not limited thereto. The in-vehicle device may any type of transponder that allows payments to be deducted from an associated account.

[0017] According to another embodiment, a contactless card may be directly tapped to an in-vehicle device without the use of a mobile computing device. For example, value (e.g., funds) may be loaded onto the in-vehicle transponder directly via “contactless” authentication and payment (e.g., using the contactless smartcard) without the use of an external web-based account.

[0018] According to a further embodiment, an in-vehicle device may be integrated into a vehicle and coupled to the various electronic components of the vehicle. For example, the vehicle may have an interface point for reading a contactless smartcard for value loading. The interface point may be located on a dashboard or the center console of the vehicle. In another example, a secure interface may be arranged in the vehicle such that the contactless smartcard can be secured into place when the user is in the vehicle, and further, can be removed when the user leaves the vehicle. In further examples, the in-vehicle device integrated in the vehicle may be used as authentication

mechanism to authenticate the vehicle, e.g., when entering and parking in a parking garage.

[0019] In previous solutions, the value loading process has been a tedious task. As described above, a user typically had to login to the user's online account and enter payment information, all of which was required to be performed prior to driving a vehicle. And generally, previous solutions have been unable to effectively coordinate and facilitate transactions within a vehicle. The embodiments and examples described herein overcome and are advantageous over the previous solutions in that an NFC enabled contactless smart card may be used to quickly load value onto in-vehicle devices, even under time-constrained circumstances (e.g., as the vehicle approaches a toll booth or a transponder reader). Also, because the contactless card itself is uniquely associated with the user, the card can be used to quickly authenticate the user within the vehicle, e.g., parking.

[0020] 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.

[0021] **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.

[0022] 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.

[0023] 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.

[0024] 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.

[0025] 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.

[0026] 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.

[0027] 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 (CDMA) 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.

[0028] 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.

[0029] System 100 may include one or more servers 120. In some examples, server 120 may include one or more processors, which are coupled to the 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.

[0030] **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**.

[0031] 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.

[0032] 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.

[0033] 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).

[0034] 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).

[0035] 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.

[0036] 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.

[0037] 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.

[0038] 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.

[0039] 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.

[0040] 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.

[0041] **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.

[0042] 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 communicate 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 the 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.

[0043] 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**.

[0044] 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.

[0045] 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.

[0046] 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 (CDMA) 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, the cellular network between client device 210 and a carrier, and Internet between the carrier and a back-end.

[0047] 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.

[0048] 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 the 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.

[0049] 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.

[0050] In some embodiments, the application 211 communicates through an associated reader (e.g., card reader 213) with the contactless card 205.

[0051] 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.

[0052] 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.

[0053] 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.

[0054] **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.

[0055] 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**).

[0056] 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.

[0057] 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-programmed many times after leaving the factory. It may also be read many times.

[0058] The memory 335 may be configured to store one or more applets 340, one or more counters 345, and a customer identifier 350. 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. 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.

[0059] 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.

[0060] 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.

[0061] 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.

[0062] 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.

[0063] **FIG. 4** illustrates an example sequence diagram 400 for loading value onto an in-vehicle device 404 using a mobile computing device 402 and a contactless card 406 according to one or more embodiments. The mobile computing device 402 may be a client device, such as a smartphone, a laptop, a tablet computer, a wearable computer, etc., configured to transmit and received information with in-vehicle device 404 and the contactless card 406. As described above, the mobile computing device 402 may include at least an NFC card reader configured to establish NFC communication with the contactless card 406.

[0064] At step 412, the mobile computing device 402 may receive or obtain a unique identifier (ID) associated with the in-vehicle device 404. In examples, the in-vehicle device 404 may be a toll transponder, a device for drive-thru payment service, a garage access transponder or badge, a parking pass, etc. The unique ID associated with the in-vehicle device 404 may be derived from one or more barcodes displayed thereon or any

other suitable identifier, such as an in-vehicle device number, name, transponder identification number, an account number associated with the drive-thru payment service, a badge number associated with the garage access transponder or badge, pass number corresponding to the parking pass, etc. In other examples, the in-vehicle device 404 may include one or more NFC tags or radio frequency identification (RFID) tags that can transmit the unique ID information. Moreover, the computing device 402 may receive or obtain information for accessing an account (online or otherwise) associated with the in-vehicle device 404. For example, the information may include at least a uniform resource locator (URL) for accessing an online account.

[0065] Upon receiving the unique ID of the in-vehicle device 404 and the information for accessing an account associated with the device, at step 414, the mobile computing device 402 may access the account associated with the device to at least load funds into the account.

[0066] At step 416, communication may be established between the mobile computing device 402 and the contactless card 406. In examples, the communication may be automatically established upon the contactless card entering the magnetic field generated by an NFC reader of the mobile computing device 402. In other examples, the mobile computing device 402 may first establish communication by sending the contactless card 406 a signal when the computing device 402 detects that the contactless card 406 has entered the magnetic field of the NFC reader. As will be described below, a user may use the contactless card 406 to perform one-tap authentication and one-tap payment on the mobile computing device 402, which advantageously makes the value loading process quick and simple for the user while in the vehicle.

[0067] At step 418, value (e.g., funds, digital currency, entity or business specific value, etc.) may be loaded into the account via the tapping of the contactless card 406 to the mobile computing device 402. Upon loading the account, at step 420, the account associated the in-vehicle device 404 may be updated to reflect the added value. Thereafter, at step 422, the in-vehicle device 404 may communicate with one or more readers to process or deduct payment(s) from the account.

[0068] It may be understood that the steps shown in the sequence diagram 400 are for illustrative purposes and not intended to be limiting in any manner. Thus, the steps are not required to be performed in any specific order.

[0069] **FIG. 5** illustrates an example value loading process using one-tap authentication and one-tap payment according to one or more embodiments. In FIG. 5, a view 500 is shown, which visually represents what a user (e.g., driver, passenger, etc.) would see within a vehicle as the user approaches a toll booth 504 and transponder reader 506. In examples, as the user is approaching the toll area, the user may realize that there are insufficient funds in the user's online toll-pay account to pay the toll.

[0070] To initiate the one-tap value loading process, as shown, the user may tap smartphone 506 to a toll transponder 508. Alternatively, the smartphone 506 may capture one or more images of the toll transponder. In either or both instances, the smartphone may receive at least two pieces of information, as described above. First, the smartphone 506 may receive a unique identifier associated with the transponder, which may be a transponder number, a barcode number, or any other type of information that specifically identifies the transponder 508 so that, for example, the correct transponder is identified and loaded. Second, the smartphone 506 may receive information on where and how to access the user's online toll-pay account. In examples, the information may be in the form of a URL that links to the online account, mobile application, etc. The information may be physically displayed or located on the transponder 508 itself. It may be understood that the transponder ID and account-related information may be stored on the smartphone 506 for future use. Moreover, it may be understood that the aforementioned transponder ID and information may be received, accessed, or retrieved wirelessly from the transponder 508 via NFC and/or RFID communication.

[0071] Upon accessing the toll-pay account corresponding to the user, a contactless card 510 may be used to perform one-tap user authentication and one-tap value loading (e.g., loading or reloading the account, one-time payment, etc.). It may be understood that the contactless card 510 may be similar or identical to the contactless card 300 described above. Moreover, it may be understood that the funds or money loaded into

the toll-pay account may be linked to one or more banking accounts corresponding to the contactless card 510.

[0072] As illustrated, a toll-pay account website, mobile application, or any other suitable payment application or website may be displayed on a graphical user interface (GUI) module 512 to perform one-tap authentication and one-tap payment. In examples, a notification (not shown) may instruct the user to tap the contactless card 510 to the smartphone 506 to authenticate into the user's toll-pay account. Upon the user tapping the contactless card 510 to the smartphone 506, the contactless card 510 may generate encrypted data and transmit the same to the smartphone 506. Once received, the one-tap GUI module 512 may transmit at least the encrypted data to one or more authentication servers, which may decrypt the data and verify the data with a private key stored in the memory of the server. The authentication server may then authenticate the user of the contactless card 510 and send the smartphone 506 confirmation thereof.

[0073] Moreover, confirmation of the authentication of the user via the one-tap authentication may also be used to authenticate and automatically log the user into the user's toll-pay account, for example, without requiring the user to enter login information and a password. In examples, the authentication server may communicate with one or more toll-pay account servers to verify or confirm such authentication, or in other examples, the user may identify or register with the toll-pay account beforehand the contactless card 510 as an authentication tool.

[0074] As shown, after the user has been authenticated and logged into the toll-pay account, the GUI module 512 may display various information, such as a current balance on the account and a preset load value, which may be \$50 as indicated in FIG. 5. Moreover, the GUI module 512 may display a notification 514 that directs the user to tap the contactless card 510 for payment to or loading or reloading of the account. It may be understood that, in some examples, both the authentication and value loading processes may be performed automatically based on a single tap of the contactless card 510, as opposed to a separate tap for authentication and another tap for payment. Furthermore, the one-tap authentication and payment features may be audibly presented to the user so

that the user does not have to look at the smartphone 506 or otherwise be distracted if driving.

[0075] When the contactless card 506 is tapped to the smartphone 506, a merchant ID and a transaction ID may be sent to the above-described one or more authentication servers. A virtual account number (VAN) generator may be used to generate virtual card data (e.g., a virtual card number, expiration date, and/or CVV) associated with the contactless card 510. The VAN generator may then transmit the virtual card data, the merchant ID, transaction ID, and any usernames and/or addresses corresponding to the user to one or more merchant servers (e.g., toll-pay merchant or provider). The merchant server may then process the transaction using the data received from the VAN generator, e.g., by generating a transaction record in a transaction database using at least the received virtual card number, expiration date, CVV, etc. The transaction record may further include the user's name, billing address, shipping address, and an indication of each item and/or service purchased. The merchant server may then transmit an order (e.g., value reload) confirmation to the mobile computing device 404.

[0076] The one-tap authentication and payment via the smartphone 506, the transponder 508, and the contactless card 510 may be used, performed, operated, completed, etc. in the vehicle and prior to the user passing through the toll booth 504 and/or the transponder reader 516, at which point the requisite fee may be deducted from the user's online account. Accordingly, the use of the contactless card 510 and user's mobile computing device advantageously allows the value loading process to be quick, easy, and safe.

[0077] **FIG. 6** illustrates an example value loading process directly between a contactless card 601 and an in-vehicle device 602 according to one or more embodiments. As described above, the in-vehicle device 602 may be a toll transponder, a garage access transponder or badge, a device for a drive-thru payment service, a parking pass, etc. As shown, the in-vehicle device 602 may include various components, such as one or more processors 604, memory 606, NFC reader 608, an insert interface 610 (which may be optional in some examples), a power interface 612, and an amplifier 614.

It may be understood that the contactless card 601 may be similar or identical to the contactless card 300 described above.

[0078] In examples, a user may tap the contactless card 601 directly to the in-vehicle device 602 without the use of a mobile computing device. In alternative example, the contactless card 601 may be inserted into the insert interface 610, which may be a card slot to accommodate the contactless card 601. A banking account associated with the contactless card 601 may be linked to an account associated with the in-vehicle device 602 (e.g., upon contact or beforehand), or in other examples, the funds in the banking account may be accessed by the in-vehicle device 602 in real-time or near real-time for loading the account associated with the in-vehicle device 602.

[0079] According to embodiments, the in-vehicle device 602 may determine whether the contactless card 601 has established communication with the in-vehicle device via the NFC reader or the insert interface. The value loading process may initiate upon a determination of established communication. Moreover, the in-vehicle device 602 may determine whether communication has been established with an external in-vehicle device reader (not shown). It may be understood that when the user taps the contactless card 601, or inserts it into the insert interface 610, to initiate the value loading process, the in-vehicle device 602 may “look for” the communication with the external reader for a predetermined period of time (e.g., 10 minutes, 5 minutes, 1 minute, 30 seconds, etc.) in the event, for example, it takes the user some time to pass through or by the external reader.

[0080] When communication between the in-vehicle device 602 and the external reader has been established, one or more payment values may be loaded to the account associated with the in-vehicle device 602 from the linked user banking account so that loaded values can be deducted by the external reader. For example, the communicative presence of the external reader may trigger the in-vehicle device 602 to transmit data to the external reader indicating at least “the user has specified and allocated the requisite payment value from an authorized banking account, so load that payment value to the in-vehicle device account and deduct the payment.” Thus, for instance, if a toll fee is five

dollars, the transmitted data to a toll transponder reader may be “the user authorized the five-dollar toll payment from the user’s contactless card, so load that amount and deduct.” In at least that regard, the account associated with the in-vehicle device may not be a conventional web-based account, such as the one described above in FIGS. 4 and 5, but may simply be a “pass-through” account that passes the requisite payment values from the contactless card banking account to the entity requesting payment.

[0081] In some examples, the facilitation of the value loading and deduction may be performed by one or more server computers (which may be managed by the entity requesting and receiving payment) based at least in part on the data transmitted from the in-vehicle device 602 to the external reader (which may be in communication with the one or more servers).

[0082] As shown, the in-vehicle device 602 may include or incorporate a power interface 612 for drawing power from the vehicle, which may be done via a vehicle power socket, or in other examples, the power may be provided by one or more energy storage components, such as a battery, a capacitor, etc. Moreover, the amplifier 614 may be configured to amplify signals from the in-vehicle device 602 to the external reader, for example, to improve or lengthen communication capabilities between the in-vehicle device 602 and the external reader.

[0083] **FIG. 7** illustrates an example authentication and/or value loading process using components integrated in a vehicle 700 according to one or more embodiments. As shown from view 702, an in-vehicle device 710 may be integrated in the vehicle 700 on the driver-side of the center console. While the device 710 is shown to have a generally oval shape, it may be understood that the reader can be rectangular, square, or any other suitable shape, design, or configuration. An NFC reader and/or RFID reader may be incorporated in the in-vehicle device 710. Moreover, the vehicle 700 may include one or more vehicle computing devices (not shown) and other components for at least performing and facilitating transactions in the vehicle.

[0084] In one example, a user may tap a contactless card 720 to the in-vehicle device 710 to perform authentication. For example, the in-vehicle device 710 may be used to

authenticate a user when entering a parking garage by providing authentication information to an external reader. In other examples, the vehicle 700 may include a secure storage area 712 where the contactless card 720 can be locked into place. The storage area 712 may also include an NFC reader and/or an RFID reader.

[0085] In further examples, the in-vehicle device 710, the vehicle computing device, and the mobile computing device 722 may all separately include Bluetooth interfaces (or any other suitable interfaces) for short-range wireless communication. The authentication information, for instance, may be transmitted to the vehicle computing device from the in-vehicle device 710 via the respective short-range wireless communication interfaces. Moreover, the mobile computing device 722 may communicate with the vehicle computing device and/or the in-vehicle device 710. For example, the user may control or manage value loading onto an account associated with the in-vehicle device 710 using the mobile computing device 722, such as transferring funds from the contactless card 720 to the in-vehicle device 710 via the Bluetooth interfaces of the vehicle computing device to the in-vehicle device 710. It may be understood that the short-range wireless communications among the interfaces of the in-vehicle device 710, the vehicle computing device, and the mobile computing device 722 may be authenticated and secure.

[0086] Accordingly, the user may be able to optionally tap the contactless card 720 to either the in-vehicle device 710 or the mobile computing device 722 to perform authentication and/or value loading. Moreover, in some examples, the user may use the vehicle computing device to control the authentication and value loading features (e.g., via a display device in the vehicle) and/or the user may use the mobile computing device 722 to control such features, as described above.

[0087] 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.”

[0088] 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.

[0089] 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 used 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.

[0090] 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.

[0091] 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.

[0092] 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.

[0093] 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.

[0094] 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.

[0095] 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.

[0096] 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.