

SYSTEMS AND METHODS FOR SECURE REPROVISIONING

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority to U.S. Patent Application No. 17/161,285 filed January 28, 2021, the disclosure of which is incorporated herein by reference in its entirety.

FIELD OF THE DISCLOSURE

[0002] The present disclosure relates to systems and methods for secure reprovisioning, including the secure reprovisioning of contact-based cards and contactless cards.

BACKGROUND

[0003] Card-based transactions are becoming increasingly common. These transactions often involve the use of a card, such as a contact-based card or a contactless card, in communication with a point of sale device, a server, or other device. It is necessary to protect such communications from interception and unauthorized access. However, transmission of data is susceptible to phishing attacks and replay attacks, resulting in increased security risks and account or card misuse.

[0004] For contact-based cards, there is an increased security risk of card skimming which may further result in compromised security. Security risks may also be increased when using contactless cards, which communicate with other devices wirelessly. A contactless card using near field communication (NFC), Wi-Fi, or Bluetooth, for example, to transmit data encounters the risk that the data transmission will be intercepted or observed by an unauthorized or malicious reader.

[0005] If a security risk, misuse, unauthorized access, or other problem is encountered, reissuance of the card may be required. Reissuance of the card can further lead to security concerns, as malicious attackers may be aware of the original card, as well as the disruption of the ability of a

user to engage in activity with the associated account. For example, a card that is mailed may be intercepted en route to a user and subject to misuse. Additionally, fraudulent actors may change the address such that the card is reissued to the address of their choice. Further, a card that has been mailed may be read contactlessly through the envelope and the card number may be skimmed.

[0006] These and other deficiencies exist. Accordingly, there is a need for systems and methods for authenticating secure card reprovisioning that overcome these deficiencies and results in a transition from a first account to a second account in a secure and reliable manner by protecting communications from interception and unauthorized access.

SUMMARY OF THE DISCLOSURE

[0007] Embodiments of the present disclosure provide a secure reprovisioning system. The secure reprovisioning system may include a first device. The first device having an association with a first account. The first device may include a memory containing one or more applets, a counter value, and transmission data. The first device may include a communication interface. The first device may include one or more processors in communication with the memory and communication interface. The first device may be configured to create a cryptogram based on the counter value, wherein the cryptogram includes the counter value and the transmission data. The first device may be configured to transmit, after entry of the communication interface into a communication field, the cryptogram. The first device may be configured to update, after transmission of the cryptogram, the counter value. The first device may be configured to receive, via the communication interface, one or more encrypted keys and one or more parameters. The first device may be configured to decrypt the one or more encrypted keys. The first device may be

configured to, after decryption of the one or more encrypted keys, switch an association from the first account to a second account.

[0008] Embodiments of the present disclosure provide a method for secure reprovisioning. The method may include creating a cryptogram based on a counter value, wherein the cryptogram includes the counter value and transmission data. The method may include transmitting, via a communication interface, the cryptogram. The method may include updating the counter value. The method may include receiving, via the communication interface, a first set of one or more encrypted keys and a first set of one or more parameters. The method may include decrypting the first set of one or more encrypted keys. The method may include changing an association from a first account to a second account.

[0009] Embodiments of the present disclosure provide a computer readable non-transitory medium comprising computer-executable instructions that are executed on a processor and comprising the steps of: creating a cryptogram based on a counter value, wherein the cryptogram includes the counter value and transmission data; transmitting, via a communication interface, the cryptogram; updating the counter value; receiving, via the communication interface, a command-application protocol data unit including one or more encrypted keys, one or more parameters, one or more applet identifiers, and one or more instructions associated with a class; decrypting the one or more encrypted keys in accordance with the one or more instructions; switching an association from a first account to a second account; and transmitting a response-application protocol data unit indicating an execution status associated with the one or more instructions.

[00010] These and other objects, features and advantages of the exemplary embodiments of the present disclosure will become apparent upon reading the following detailed description of the

exemplary embodiments of the present disclosure, when taken in conjunction with the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[00011] Various embodiments of the present disclosure, together with further objects and advantages, may best be understood by reference to the following description taken in conjunction with the accompanying drawings.

[00012] Figure 1 depicts a secure reprovisioning system according to an exemplary embodiment.

[00013] Figure 2A is an illustration of a first device according to an exemplary embodiment.

[00014] Figure 2B is an illustration of a contact pad of a first device according to an exemplary embodiment.

[00015] Figure 3 depicts a method of secure reprovisioning according to an exemplary embodiment.

[00016] Figure 4 depicts a sequence diagram of a process for secure reprovisioning according to an exemplary embodiment.

[00017] Figure 5 depicts a method of secure reprovisioning according to an exemplary embodiment.

[00018] Figure 6 depicts a method of secure according to an exemplary embodiment.

DETAILED DESCRIPTION

[00019] The following description of embodiments provides non-limiting representative examples referencing numerals to particularly describe features and teachings of different aspects of the invention. The embodiments described should be recognized as capable of implementation

separately, or in combination, with other embodiments from the description of the embodiments. A person of ordinary skill in the art reviewing the description of embodiments should be able to learn and understand the different described aspects of the invention. The description of embodiments should facilitate understanding of the invention to such an extent that other implementations, not specifically covered but within the knowledge of a person of skill in the art having read the description of embodiments, would be understood to be consistent with an application of the invention.

[00020] Benefits of the systems and methods disclosed herein include improved security for authenticating secure card reprovisioning that results in a transition from a first account to a second account in a secure and reliable manner by protecting communications from interception and unauthorized access. The systems and methods disclosed herein allow for the avoidance of phishing attacks and preventing replay attacks, thereby increasing security. Security can also be increased by reducing the risks of other common attacks. For example, the systems and methods disclosed herein reduce the risk of card skimming attacks for contact-based cards and the risk of the unauthorized observance or interception of data transmissions for contactless cards through the use of encrypted data communications. As another example, the systems and methods disclosed herein provide for securely reprovisioning cards via multifactor authentication.

[00021] Accordingly, keys of cards may be securely generated, encrypted, and reissued, rather than collecting the cards, and programming each card for reissuance, thereby mitigating security risks, reducing costs, and improving transaction efficiency. These benefits may be achieved without inconveniencing the user or otherwise degrading the user experience with a reissuance process. This avoids disruption, reduces the time and costs associated with card reissuance

processes, and allows the user to continue engaging in activity with the associated account. By having the card reissuance handled at an automated teller machine (ATM), authentication and controlled access to the ATM is more secure. As another benefit, the need to deliver cards through the mail can be reduced or eliminated, which improves security and reduces the risk of cards being intercepted in the mail, the risk of fraudulent manipulation of delivery addresses to redirect cards to incorrect or unauthorized addresses, and the risk of card number skimming of cards in the mail.

[00022] Accordingly, the systems and methods disclosed herein reduce the risk of fraudulent activity, such as misuse of the card or an account associated with the card, in a secure and unobtrusive manner that does not inconvenience the user.

[00023] Figure 1 illustrates a secure reprovisioning system 100. The system 100 may comprise a first device 105, a second device 110, a network 115, a server 120, and a database 125. Although Figure 1 illustrates single instances of components of system 100, system 100 may include any number of components.

[00024] System 100 may include a first device 105. The first device 105 may comprise a contactless card, a contact-based card, a network-enabled computer, or other device described herein. As further explained below in FIGs. 2A-2B, first device 105 may include one or more processors 102, and memory 104. Memory 104 may include one or more applets 106 and one or more counters 108. Each counter 108 may include a counter value. Memory 104 may include the counter value, transmission data, and one or more keys.

[00025] First device 105 may include a communication interface 107. The communication interface 107 may comprise communication capabilities with physical interfaces and contactless interfaces. For example, the communication interface 107 may be configured to communicate

with a physical interface, such as by swiping through a card swipe interface or inserting into a card chip reader found on an automated teller machine (ATM) or other device configured to communicate over a physical interface. In other examples, the communication interface 107 may be configured to establish contactless communication with a card reading device via a short-range wireless communication method, such as NFC, Bluetooth, Wi-Fi, RFID, and other forms of contactless communication. As shown in FIG. 1, the communication interface 107 may be configured to communicate directly with the second device 110, server 120, and/or database 125 via network 115.

[00026] First device 105 may be in data communication with any number of components of system 100. For example, first device 105 may transmit data via network 115 to second device 110, and/or server 120. First device 105 may transmit data via network 115 to database 125. In some examples, first device 105 may be configured to transmit data via network 115 after entry into one or more communication fields of any device. Without limitation, each entry may be associated with a tap, a swipe, a wave, and/or any combination thereof.

[00027] System 100 may include a second device 110. The second device 110 may include one or more processors 112, and memory 114. Memory 114 may include one or more applications 116, including but not limited to a first application. Second device 110 may be in data communication with any number of components of system 100. For example, second device 110 may transmit data via network 115 to server 120. Second device 110 may transmit data via network 115 to database 125. Without limitation, second device 110 may be a network-enabled computer. As referred to herein, a network-enabled computer may include, but is not limited to a computer device, or communications device including, e.g., a server, a network appliance, a personal computer, a

workstation, a phone, a handheld PC, a personal digital assistant, a contactless card, a thin client, a fat client, an Internet browser, a kiosk, a tablet, a terminal, an ATM, or other device. Second device 110 also may be a mobile device; for example, a mobile device may include an iPhone, iPod, iPad from Apple® or any other mobile device running Apple's iOS® operating system, any device running Microsoft's Windows® Mobile operating system, any device running Google's Android® operating system, and/or any other smartphone, tablet, or like wearable mobile device.

[00028] The second device 110 may include processing circuitry and may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamperproofing hardware, as necessary to perform the functions described herein. The second 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.

[00029] System 100 may include a network 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 to any one of components of system 100. For example, first device 105 may be configured to connect to server 120 via network 115. In some examples,

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.

[00030] In addition, network 115 may include, without limitation, telephone lines, fiber optics, IEEE Ethernet 902.3, 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 comprise a plurality of interconnected networks, such as, for example, the Internet, a service provider's network, a cable television network, corporate networks, such as credit card association networks, and home networks.

[00031] System 100 may include one or more servers 120. In some examples, server 120 may include one or more processors 122 coupled to memory 124. 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 first device 105. Server 120 may be in data communication with the applet 106 and/or application 116. For example, a server 120 may be in data communication with applet 106 via one or more networks 115. First device 105 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. First device 105 may transmit, for example from applet 106 executing thereon, 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 first device 105. Based on the one or more requests from applet 106, server 120 may be configured to retrieve the requested data. Server 120 may be configured to transmit the received data to applet 106, the received data being responsive to one or more requests.

[00032] In some examples, server 120 can be a dedicated server computer, such as bladed servers, or can be personal computers, laptop computers, notebook computers, palm top computers, network computers, mobile devices, wearable devices, or any processor-controlled device capable of supporting the system 100. While FIG. 1 illustrates a single server 120, it is understood that other embodiments can use multiple servers or multiple computer systems as necessary or desired to support the users and can also use back-up or redundant servers to prevent network downtime in the event of a failure of a particular server.

[00033] Server 120 may include an application comprising instructions for execution thereon. For example, the application may comprise instructions for execution on the server 120. The application may be in communication with any components of system 100. For example, server 120 may execute one or more applications that enable, for example, network and/or data

communications with one or more components of system 100 and transmit and/or receive data. Without limitation, server 120 may be a network-enabled computer. As referred to herein, a network-enabled computer may include, but is not limited to a computer device, or communications device including, e.g., a server, a network appliance, a personal computer, a workstation, a phone, a handheld PC, a personal digital assistant, a contactless card, a thin client, a fat client, an Internet browser, or other device. Server 120 also may be a mobile device; for example, a mobile device may include an iPhone, iPod, iPad from Apple® or any other mobile device running Apple's iOS® operating system, any device running Microsoft's Windows® Mobile operating system, any device running Google's Android® operating system, and/or any other smartphone, tablet, or like wearable mobile device.

[00034] The server 120 may include processing circuitry and may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamperproofing hardware, as necessary to perform the functions described herein. The server 120 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.

[00035] System 100 may include one or more databases 125. The database 125 may comprise a

relational database, a non-relational database, or other database implementations, and any combination thereof, including a plurality of relational databases and non-relational databases. In some examples, the database 125 may comprise a desktop database, a mobile database, or an in-memory database. Further, the database 125 may be hosted internally by any component of system 100, such as the first device 105 or server 120, or the database 125 may be hosted externally to any component of the system 100, such as the first device 105 or server 120, by a cloud-based platform, or in any storage device that is in data communication with the first device 105 and server 120. In some examples, database 125 may be in data communication with any number of components of system 100. For example, server 120 may be configured to retrieve the requested data from the database 125 that is transmitted by applet 106. Server 120 may be configured to transmit the received data from database 125 to applet 106 via network 115, the received data being responsive to the transmitted one or more requests. In other examples, applet 106 may be configured to transmit one or more requests for the requested data from database 125 via network 115.

[00036] In some examples, exemplary procedures in accordance with the present disclosure described herein can be performed by a processing arrangement and/or a computing arrangement (e.g., computer hardware arrangement). Such processing/computing arrangement can be, for example entirely or a part of, or include, but not limited to, a computer/processor that can include, for example one or more microprocessors, and use instructions stored on a computer-accessible medium (e.g., RAM, ROM, hard drive, or other storage device). For example, a computer-accessible medium can be part of the memory of the first device 105, second device 110, server 120, and/or database 125, or other computer hardware arrangement.

[00037] In some examples, a computer-accessible medium (e.g., as described herein above, a storage device such as a hard disk, floppy disk, memory stick, CD-ROM, RAM, ROM, etc., or a collection thereof) can be provided (e.g., in communication with the processing arrangement). The computer-accessible medium can contain executable instructions thereon. In addition or alternatively, a storage arrangement can be provided separately from the computer-accessible medium, which can provide the instructions to the processing arrangement so as to configure the processing arrangement to execute certain exemplary procedures, processes, and methods, as described herein above, for example.

[00038] The one or more processors 102 may be configured to create a cryptogram using the at least one key and the counter value. The cryptogram may include the counter value and the transmission data. The one or more processors 102 may be configured to transmit the cryptogram via the communication interface 107. For example, the one or more processors 102 may be configured to transmit the cryptogram to one or more applications. In some examples, the one or more processors 102 may be configured to transmit the cryptogram to application 116 comprising instructions for execution on a second device 110. The one or more processors 102 may be configured to update the counter value after transmission of the cryptogram.

[00039] In some examples, the application 116 comprising instructions for execution on the second device 110 may be configured to encrypt one or more keys. Without limitation, the second device 110 may comprise an ATM, a kiosk, a point of sale device, or other device. The application 116 may be configured to transmit the one or more encrypted keys. In some examples, the application 116 may be configured to transmit one or more parameters. Without limitation, the one or more parameters may include at least one selected from the group of primary account number

information, expiration date information, card verification code, and/or any combination thereof. In some examples, the one or more parameters may comprise dynamic information, such as changed personalization data including but not limited to card master keys, such as secret and public/private keys, and one or more spending limits. The application 116 may be configured to transmit one or more commands-application protocol data unit (C-APDU) including the one or more encrypted keys, the one or more parameters, one or more applet identifiers, and one or more instructions associated with a class of a header. In some examples, the application 116 may be configured to transmit the one or more commands-application protocol data unit to the first device 105 after one or more entries of the communication interface 107 into a communication field of the second device 110. Communication between the application 116 and first device 105 via near field communication (NFC). Without limitation, the one or more commands-application protocol data unit may be transmitted via Bluetooth, Wi-Fi, and Radio-Frequency Identification (RFID).

[00040] The first device 105 may be configured to receive the one or more encrypted keys and one or more parameters after input authentication. The first device 105 may be configured to receive the command-application protocol data unit including the one or more encrypted keys, the one or more parameters, one or more applet identifiers, and one or more instructions associated with a class of a header. In some examples, one or more session keys may be generated at the second device 110 or server 120, which may be used to encrypt one or more master keys. For example, one or more limited use session keys may be generated based on a cryptogram and a counter to encrypt data. The first device 105 may be configured to receive the encrypted data and decrypt it for storage. The one or more instructions may each be associated with a code, and include decrypting and/or confirmation of the one or more decrypted keys, storing and/or confirmation of

the one or more decrypted keys. In some examples, the first device 105 may be configured to receive the one or more commands-application protocol data unit after input authentication. For example, input for the authentication may include, without limitation, at least one or more selected from the group of a personal identification number, a username and/or password, a mobile device number, an account number, a card number, and a biometric (e.g., facial scan, a retina scan, a fingerprint, and a voice input for voice recognition). The application 116 of the second device 110 may be configured to authenticate the input. In other examples, application 116 may be configured to transmit the input to server 120 for authentication of the input.

[00041] The first device 105 may be configured to receive the one or more commands-application protocol data unit on a predetermined basis. In some examples, the predetermined basis may be any number of seconds, minutes, hours, days, weeks, months, years, etc. In other examples, the first device may be configured to receive the one or more commands-application protocol data unit after determination of a security concern. For example, the server 120 may be configured to determine one or more security concerns. Without limitation, the one or more security concerns may be associated with identity theft, unauthorized usage based on transaction history and/or transaction frequency evaluated over any determined time period, a notice of fraudulent charges, and/or any combination thereof. For example, the server 120 may, responsive to determining any number of one or more security concerns associated with the first device 105, be configured to transmit one or more messages to the application 116 of the second device 110 to transmit the one or more commands-application protocol data unit. In this manner, the application 116 of the second device 110 may be configured to receive the one or more messages from the server 120, the one or more messages indicative of transmitting the one or more commands-application protocol data

unit after determination of one or more security concerns.

[00042] The first device 105 may be subject to eligibility criteria. For example, after determination of the one or more security concerns, the first device 105 may subject to a prioritized list associated with eligibility prior to receipt of the one or more commands-application protocol data unit. In some examples, the server 120 may be configured to screen the first device 105 based on at least one selected from the group of time elapsed since issuance of the card, card usage for transactions, transaction type, card type, one or more determinations of the security concerns associated with the first device 105, and/or any combination thereof. In this manner, the server 120 may be configured to evaluate and rank how many first devices 105 and which types of first devices 105 may be configured to receive the one or more commands-application protocol data unit based on the eligibility criteria before signaling to the application 116 of the second device 110 to transmit the one or more commands-application protocol data unit. In one example, one or more sets of first devices 105 may be prioritized to receive the one or more commands-application protocol data unit after the server 120 is configured to determine whether the first device 105 is a credit card and is associated with a notice of fraudulent charges. In another example, one or more sets of first devices 105 may be prioritized to receive the one or more commands-application protocol data unit after the server 120 is configured to determine whether the first device 105 is an identification card that has been abnormally used, for example exceeding a predetermined threshold, for one or more transactions. In yet another example, one or more sets of first device 105 may be prioritized to receive the one or more commands-application protocol data unit after the server 120 is configured to determine how much time has elapsed since issuance of the first device 105. In these non-limiting examples, the server 120 may be further configured to prioritize

which of these determinations are to be made first, second, third, etc. In this manner, a designated number of first devices 105 may be reprovisioned on an individual basis and/or in a batch. The first devices 105 may also be reprovisioned on an as-needed basis, according to a predetermined schedule, and/or any combination thereof.

[00043] The first device 105 may be configured to receive the one or more commands-application protocol data unit. For example, the first device 105 may be configured to receive the one or more commands-application protocol data unit from the application 116 of the second device 110. The first device 105 may be configured to decrypt the one or more encrypted keys. One or more applets, such as applet 106, of the first device 105 may be configured to store one or more decrypted keys in a secure element. An applet 106, such as a first applet, may be configured to transmit, via a communication channel 111, the one or more decrypted keys and the one or more parameters to a second applet 109. After decryption of the one or more encrypted keys, the first device 105 may be configured to change an association from a first account to a second account. Moreover, the first device 105 may be restricted to a predetermined usage after decryption of the one or more encrypted keys. In one example, the first device 105 may be subject to one or more predetermined spending thresholds. In another example, the first device 105 may be subject to a predetermined number of uses. For example, the first device 105 may be used for only a designated set of transactions, such as for lunch only and/or for office furniture. In another example, the first device 105 may be subject to a predetermined number of usages for one or more types of transactions, including but not limited to a debit card transaction or a credit card transaction.

[00044] In another example, the first device 105 may be used for only transactions occurring during a certain time (e.g., business hours of 9:00am to 5:00pm), on certain days of the week (e.g.,

weekdays, weekends, only Mondays, only Thursdays and Fridays), of on a certain date (e.g., Wednesday, July 1, 2020). In another example, the first device 105 may be used only for certain purposes, such as for expense account purposes (e.g., travel expenses including airfare, meals, and hotels), for a designated project (e.g., a certain type of equipment or hardware needed for a project), with designated or approved merchants, or with a specified list of merchants known to offer goods or services needed for a particular purposes.

[00045] It is understood that the foregoing listings are exemplary and that any of these examples can be used in combination with one another. Thus, a user may use the same card configured for a variety of purposes and with a variety of accounts.

[00046] The first device 105 may be configured to transmit, responsive to the one or more commands-application protocol data unit, one or more responses-application protocol data unit (R-APDU). The one or more responses-application protocol data unit may include one or bytes indicative of a status of the command. For example, at least one of the one or more responses-application protocol data unit may be configured to indicate an execution status associated with the one or more instructions. The first device 105 may be configured to transmit the one or more responses-application protocol data unit to the application 116 of the second device 110. In some examples, the first device 105 may be configured to return a successful execution status associated with the one or more instructions. To the extent that the execution status of the one or more instructions is not successful, the first device 105 may be configured to return a warning or unsuccessful execution status. For example, the one or more responses-application protocol data unit may be configured to indicate if and when the one or more encrypted keys were decrypted and/or if and when the one or more decrypted keys were stored.

[00047] The application 116 may be configured to receive the one or more responses-application protocol data unit from the first device 105. For example, the one or more responses-application protocol data unit may be received after one or more entries of the communication interface 107 into a communication field of the second device 110. The one or more entries may be associated with at least one selected from the group of a tap, a swipe, a wave, and/or any combination thereof. Depending on the results of the execution status of the one or more instructions, the application 116 may be configured to take one or more corrective actions. In one example, the application 116 may be configured to re-send the one or more commands-application protocol data unit if the execution status of the one or more instructions is unsuccessful. In another example, the application 116 may be configured to re-send the one or more commands-application protocol data unit if the execution status of the one or more instructions is not received from the first device 105 within a predetermined time, including but not limited to any number of seconds, minutes, hours, days, etc. In yet another example, the application 116 may be configured to notify the server 120 if the one or more commands-application protocol data unit if the execution status of the one or more instructions is successful. In yet another example, the application 116 may be configured to notify the server 120 if the one or more commands-application protocol data unit if the execution status of the one or more instructions is received within the predetermined time.

[00048] FIG. 2A illustrates one or more first devices 200. First device 200 may reference the same or similar components of first device 105, as explained above with respect to FIG. 1. Although Figure 2A and 2B illustrate single instances of components of first device 200, any number of components may be utilized.

[00049] First device 200 may be configured to communicate with one or more components of system 100. First device 200 may comprise a contact-based card or contactless card, which may comprise a payment card, such as a credit card, debit card, or gift card, issued by a service provider 205 displayed on the front or back of the first device 200. In some examples, the first device 200 is not related to a payment card, and may comprise, without limitation, an identification card, a membership card, and a transportation card. In some examples, the payment card may comprise a dual interface contactless payment card. The first device 200 may comprise a substrate 210, 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 first device 200 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 first device 200 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.

[00050] The first device 200 may also include identification information 215 displayed on the front and/or back of the card, and a contact pad 220. The contact pad 220 may be configured to establish contact with another communication device, including but not limited to a user device, smart phone, laptop, desktop, or tablet computer. The first device 200 may also include processing circuitry, antenna and other components not shown in FIG. 2A. These components may be located

behind the contact pad 220 or elsewhere on the substrate 210. The first device 200 may also include a magnetic strip or tape, which may be located on the back of the card (not shown in FIG. 2A).

[00051] As illustrated in FIG. 2B, the contact pad 220 of FIG. 2A may include processing circuitry 225 for storing and processing information, a processor 230, such as a microprocessor, and a memory 235. It is understood that the processing circuitry 225 may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamperproofing hardware, as necessary to perform the functions described herein.

[00052] The memory 235 may be a read-only memory, write-once read-multiple memory or read/write memory, e.g., RAM, ROM, and EEPROM, and the first device 200 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.

[00053] The memory 235 may be configured to store one or more applets 240, one or more counters 245, and a customer identifier 250. The one or more applets 240 may comprise one or more software applications configured to execute on one or more contactless cards, such as Java Card applet. However, it is understood that the one or more applets 240 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 245 may comprise a numeric counter

sufficient to store an integer. The customer identifier 250 may comprise a unique alphanumeric identifier assigned to a user of the first device 200, and the identifier may distinguish the user of the contactless card from other contactless card users. In some examples, the customer identifier 250 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.

[00054] 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 contact pad 220 or entirely separate from it, or as further elements in addition to processor 230 and memory 235 elements located within the contact pad 220.

[00055] In some examples, the first device 200 may comprise one or more antennas 255. The one or more antennas 255 may be placed within the first device 200 and around the processing circuitry 225 of the contact pad 220. For example, the one or more antennas 255 may be integral with the processing circuitry 225 and the one or more antennas 255 may be used with an external booster coil. As another example, the one or more antennas 255 may be external to the contact pad 220 and the processing circuitry 225.

[00056] In an embodiment, the coil of first device 200 may act as the secondary of an air core transformer. The terminal may communicate with the first device 200 by cutting power or amplitude modulation. The first device 200 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 first device 200 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.

[00057] Figure 3 depicts a method 300 of secure reprovisioning. Figure 3 may reference the same or similar components of system 100, and first device 200 of FIG. 2A and FIG. 2B.

[00058] At block 305, the method 300 may include creating a cryptogram using at least one key and a counter value. For example, one or more processors of a first device may be configured to create a cryptogram using the at least one key and the counter value. The cryptogram may include the counter value and the transmission data. The first device may include a memory containing one or more keys, including the at least one key, a counter value, and the transmission data. The first device may further include a communication interface.

[00059] At block 310, the method 300 may include transmitting the cryptogram. For example, the one or more processors may be configured to transmit the cryptogram via the communication interface. For example, the one or more processors may be configured to transmit the cryptogram to one or more applications. In some examples, the one or more processors may be configured to transmit the cryptogram to an application comprising instructions for execution on a second device.

[00060] At block 315, the method 300 may include updating the counter value. For example, the one or more processors may be configured to update the counter value after transmission of the cryptogram.

[00061] At block 320, the method 300 may include receiving, via the communication interface, a first set of one or more encrypted keys and a first set of one or more parameters. In some examples, the application comprising instructions for execution on the second device may be configured to

encrypt one or more keys. Without limitation, the second device may comprise an ATM, a kiosk, a register, or other point of sale device. The application may be configured to transmit the one or more encrypted keys. In some examples, the application may be configured to transmit one or more parameters. Without limitation, the one or more parameters may include at least one selected from the group of primary account number information, expiration date information, card verification code, and/or any combination thereof. In some examples, the one or more parameters may comprise dynamic information, such as changed personalization data including but not limited to card master keys, such as secret and public/private keys, and one or more spending limits. The application may be configured to transmit one or more commands-application protocol data unit including the one or more encrypted keys, the one or more parameters, one or more applet identifiers, and one or more instructions associated with a class of a header. In some examples, one or more session keys may be generated at the second device or server, which may be used to encrypt one or more master keys. In some examples, the application may be configured to transmit the one or more commands-application protocol data unit to the first device after one or more entries of the communication interface into a communication field of the second device. Communication between the application and first device via NFC. Without limitation, the one or more commands-application protocol data unit may be transmitted via Bluetooth, Wi-Fi, and RFID.

[00062] The first device may be configured to receive the one or more commands-application protocol data unit on a predetermined basis. In some examples, the predetermined basis may be any number of seconds, minutes, hours, days, weeks, months, years, etc. In other examples, the first device may be configured to receive the one or more commands-application protocol data unit

after determination of a security concern. For example, the server may be configured to determine one or more security concerns. Without limitation, the one or more security concerns may be associated with identity theft, unauthorized usage based on transaction history and/or transaction frequency evaluated over any determined time period, a notice of fraudulent charges, and/or any combination thereof. For example, the server may, responsive to determining any number of one or more security concerns associated with the first device, be configured to transmit one or more messages to the application of the second device to transmit the one or more commands-application protocol data unit. In this manner, the application of the second device may be configured to receive the one or more messages from the server, the one or more messages indicative of transmitting the one or more commands-application protocol data unit after determination of one or more security concerns.

[00063] The first device may be subject to eligibility criteria. For example, after determination of the one or more security concerns, the first device may subject to a prioritized list associated with eligibility prior to receipt of the one or more commands-application protocol data unit. In some examples, the server may be configured to screen the first device based on at least one selected from the group of time elapsed since issuance of the card, card usage for transactions, transaction type, card type, one or more determinations of the security concerns associated with the first device, and/or any combination thereof. In this manner, the server may be configured to evaluate and rank how many first devices and which types of first devices may be configured to receive the one or more commands-application protocol data unit based on the eligibility criteria before signaling to the application of the second device to transmit the one or more commands-application protocol data unit. In one example, one or more sets of first devices may be prioritized to receive

the one or more commands-application protocol data unit after the server is configured to determine whether the first device is a credit card and is associated with a notice of fraudulent charges. In another example, one or more sets of first devices may be prioritized to receive the one or more commands-application protocol data unit after the server is configured to determine whether the first device is an identification card that has been abnormally used, for example exceeding a predetermined threshold, for one or more transactions. In yet another example, one or more sets of first device may be prioritized to receive the one or more commands-application protocol data unit after the server is configured to determine how much time has elapsed since issuance of the first device. In these non-limiting examples, the server may be further configured to prioritize which of these determinations are to be made first, second, third, etc. In this manner, a designated number of first devices may be reprovisioned on an individual basis and/or in a batch. The first devices may also be reprovisioned on an as-needed basis, according to a predetermined schedule, and/or any combination thereof.

[00064] The first device may be configured to receive the one or more encrypted keys and one or more parameters after input authentication. The first device may be configured to receive the command-application protocol data unit including the one or more encrypted keys, the one or more parameters, one or more applet identifiers, and one or more instructions associated with a class of a header. In some examples, one or more session keys may be generated at the second device or server, which may be used to encrypt one or more master keys. For example, one or more limited use session keys may be generated based on a cryptogram and a counter to encrypt data. The first device may be configured to receive the encrypted data and decrypt it for storage. The one or more instructions may each be associated with a code, and include decrypting and/or confirmation of

the one or more decrypted keys, storing and/or confirmation of the one or more decrypted keys. In some examples, the first device may be configured to receive the one or more commands-application protocol data unit after input authentication. For example, input for the authentication may include, without limitation, at least one or more selected from the group of a personal identification number, a username and/or password, a mobile device number, an account number, a card number, and a biometric (e.g., facial scan, a retina scan, a fingerprint, and a voice input for voice recognition). The application of the second device may be configured to authenticate the input. In other examples, application may be configured to transmit the input to a server for authentication of the input.

[00065] At block 325, the method 300 may include decrypting the first set of one or more encrypted keys. The first device may be configured to receive the one or more commands-application protocol data unit. For example, the first device may be configured to receive the one or more commands-application protocol data unit from the application of the second device. The first device may be configured to decrypt the one or more encrypted keys. One or more applets of the first device may be configured to store one or more decrypted keys in a secure element. A first applet may be configured to transmit, via a communication channel, the one or more decrypted keys and the one or more parameters to a second applet.

[00066] At block 330, the method 300 may include changing an association from a first account to a second account. After decryption of the one or more encrypted keys, the first device may be configured to change an association from a first account to a second account. Moreover, the first device may be restricted to a predetermined usage after decryption of the one or more encrypted keys. In one example, the first device may be subject to one or more predetermined spending

thresholds. In another example, the first device may be subject to a predetermined number of uses. For example, the first device may be used for only a designated set of transactions, such as for lunch only and/or for office furniture. In another example, the first device may be subject to a predetermined number of usages for one or more types of transactions, including but not limited to a debit card transaction or a credit card transaction.

[00067] In another example, the first device may be used for only transactions occurring during a certain time (e.g., business hours of 9:00am to 5:00pm), on certain days of the week (e.g., weekdays, weekends, only Mondays, only Thursdays and Fridays), of on a certain date (e.g., Wednesday, July 1, 2020). In another example, the first device may be used only for certain purposes, such as for expense account purposes (e.g., travel expenses including airfare, meals, and hotels), for a designated project (e.g., a certain type of equipment or hardware needed for a project), with designated or approved merchants, or with a specified list of merchants known to offer goods or services needed for a particular purposes.

[00068] It is understood that the foregoing listings are exemplary and that any of these examples can be used in combination with one another. Thus, a user may use the same card configured for a variety of purposes and with a variety of accounts.

[00069] The first device may be configured to transmit, responsive to the one or more commands-application protocol data unit, one or more responses-application protocol data unit. The one or more responses-application protocol data unit may include one or bytes indicative of a status of the command. For example, at least one of the one or more responses-application protocol data unit may be configured to indicate an execution status associated with the one or more instructions. The first device may be configured to transmit the one or more responses-application protocol data

unit to the application of the second device. In some examples, the first device may be configured to return a successful execution status associated with the one or more instructions. To the extent that the execution status of the one or more instructions is not successful, the first device may be configured to return a warning or unsuccessful execution status. For example, the one or more responses-application protocol data unit may be configured to indicate if and when the one or more encrypted keys were decrypted and/or if and when the one or more decrypted keys were stored.

[00070] The application may be configured to receive the one or more responses-application protocol data unit from the first device. For example, the one or more responses-application protocol data unit may be received after one or more entries of the communication interface into a communication field of the second device. The one or more entries may be associated with at least one selected from the group of a tap, a swipe, a wave, and/or any combination thereof. Depending on the results of the execution status of the one or more instructions, the application may be configured to take one or more corrective actions. In one example, the application may be configured to re-send the one or more commands-application protocol data unit if the execution status of the one or more instructions is unsuccessful. In another example, the application may be configured to re-send the one or more commands-application protocol data unit if the execution status of the one or more instructions is not received from the first device within a predetermined time, including but not limited to any number of seconds, minutes, hours, days, etc. In yet another example, the application may be configured to notify the server if the one or more commands-application protocol data unit if the execution status of the one or more instructions is successful. In yet another example, the application may be configured to notify the server if the one or more commands-application protocol data unit if the execution status of the one or more instructions is

received within the predetermined time.

[00071] Figure 4 depicts a sequence diagram 400 of a process for secure reprovisioning according to an exemplary embodiment. Figure 4 may reference the same or similar components of system 100, first device 200 of FIG. 2A and FIG. 2B, and method 300 of FIG. 3.

[00072] At step 405, an application comprising instructions for execution on a device, such as an ATM, a kiosk, a point of sale device, or other device, may be configured to transmit input for authentication to a server. For example, input for the authentication may include, without limitation, at least one or more selected from the group of a personal identification number, a username and/or password, a mobile device number, an account number, a card number, and a biometric (e.g., facial scan, a retina scan, a fingerprint, and a voice input for voice recognition). The application may be configured to authenticate the input. In other examples, the application may be configured to transmit the input to server for authentication of the input.

[00073] The device may include one or more processors, and memory. The memory may include one or more applications, including but not limited to first application. The device may be in data communication with any number of components of FIG. 4. For example, the device may transmit data via a network to a server. The device may transmit data via network to a database. Without limitation, the device may be a network-enabled computer. As referred to herein, a network-enabled computer may include, but is not limited to a computer device, or communications device including, e.g., a server, a network appliance, a personal computer, a workstation, a phone, a handheld PC, a personal digital assistant, a contactless card, a contact-based card, a thin client, a fat client, an Internet browser, a kiosk, a tablet, a terminal, an ATM, or other device. The device also may be a mobile device; for example, a mobile device may include an iPhone, iPod, iPad from

Apple® or any other mobile device running Apple's iOS® operating system, any device running Microsoft's Windows® Mobile operating system, any device running Google's Android® operating system, and/or any other smartphone, tablet, or like wearable mobile device.

[00074] The device may include processing circuitry and may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamperproofing hardware, as necessary to perform the functions described herein. The device 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.

[00075] The network 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 to any one of components of FIG. 4. In some examples, the network 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.

[00076] In addition, the network may include, without limitation, telephone lines, fiber optics, IEEE Ethernet 902.3, a wide area network, a wireless personal area network, a LAN, or a global network such as the Internet. In addition, the network may support an Internet network, a wireless communication network, a cellular network, or the like, or any combination thereof. The network may further include one network, or any number of the exemplary types of networks mentioned above, operating as a stand-alone network or in cooperation with each other. The network may utilize one or more protocols of one or more network elements to which they are communicatively coupled. The network may translate to or from other protocols to one or more protocols of network devices. Although the network is depicted as a single network, it should be appreciated that according to one or more examples, the network may comprise a plurality of interconnected networks, such as, for example, the Internet, a service provider's network, a cable television network, corporate networks, such as credit card association networks, and home networks.

[00077] The server may include one or more processors coupled to memory. The server 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. The server may be in data communication with one or more applets of a card and/or application of the device. For example, a server may be in data communication with an applet via one or more networks. A card may be in communication with one or more servers via one or more networks, and may operate as a respective front-end to back-end pair with server. The card may transmit, for example from applet executing thereon, one or more requests to server. The one or more requests may be associated with retrieving data from

server. The server may receive the one or more requests from the card. Based on the one or more requests from the applet, the server may be configured to retrieve the requested data. The server may be configured to transmit the received data to the applet, the received data being responsive to one or more requests.

[00078] In some examples, the server can be a dedicated server computer, such as blade servers, or can be personal computers, laptop computers, notebook computers, palm top computers, network computers, mobile devices, wearable devices, or any processor-controlled device capable of supporting the system of FIG. 4. While FIG. 4 illustrates a single server, it is understood that other embodiments can use multiple servers or multiple computer systems as necessary or desired to support the users and can also use back-up or redundant servers to prevent network downtime in the event of a failure of a particular server.

[00079] The server may include an application comprising instructions for execution thereon. For example, the application may comprise instructions for execution on the server. The application may be in communication with any components of the system. For example, the server may execute one or more applications that enable, for example, network and/or data communications with one or more components of the system and transmit and/or receive data. Without limitation, server may be a network-enabled computer. As referred to herein, a network-enabled computer may include, but is not limited to a computer device, or communications device including, e.g., a server, a network appliance, a personal computer, a workstation, a phone, a handheld PC, a personal digital assistant, a contactless card, a contact-based card, a thin client, a fat client, an Internet browser, or other device. The server also may be a mobile device; for example, a mobile device may include an iPhone, iPod, iPad from Apple® or any other mobile

device running Apple's iOS® operating system, any device running Microsoft's Windows® Mobile operating system, any device running Google's Android® operating system, and/or any other smartphone, tablet, or like wearable mobile device.

[00080] The server may include processing circuitry and may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamperproofing hardware, as necessary to perform the functions described herein. The server 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.

[00081] The database may comprise a relational database, a non-relational database, or other database implementations, and any combination thereof, including a plurality of relational databases and non-relational databases. In some examples, the database may comprise a desktop database, a mobile database, or an in-memory database. Further, the database may be hosted internally by any component of the system, such as the card, device, and/or the server, or the database may be hosted externally to any component of the system, such as the card, device, and/or the server, by a cloud-based platform, or in any storage device that is in data communication with the card, device, and/or the server. In some examples, the database may be in data communication

with any number of components of the system. For example, the server may be configured to retrieve the requested data from the database that is transmitted by the applet. The server may be configured to transmit the received data from the database to one or more applets via network, the received data being responsive to the transmitted one or more requests. In other examples, the one or more applets may be configured to transmit one or more requests for the requested data from the database via network.

[00082] In some examples, exemplary procedures in accordance with the present disclosure described herein can be performed by a processing arrangement and/or a computing arrangement (e.g., computer hardware arrangement). Such processing/computing arrangement can be, for example entirely or a part of, or include, but not limited to, a computer/processor that can include, for example one or more microprocessors, and use instructions stored on a computer-accessible medium (e.g., RAM, ROM, hard drive, or other storage device). For example, a computer-accessible medium can be part of the memory of the card, device, server, and/or database, or other computer hardware arrangement.

[00083] In some examples, a computer-accessible medium (e.g., as described herein above, a storage device such as a hard disk, floppy disk, memory stick, CD-ROM, RAM, ROM, etc., or a collection thereof) can be provided (e.g., in communication with the processing arrangement). The computer-accessible medium can contain executable instructions thereon. In addition or alternatively, a storage arrangement can be provided separately from the computer-accessible medium, which can provide the instructions to the processing arrangement so as to configure the processing arrangement to execute certain exemplary procedures, processes, and methods, as described herein above, for example.

[00084] At step 410, server may be configured to signal one or more outcomes of eligibility criteria evaluation. For example, the server may be configured to receive the input from the application. The server may be configured to authenticate the input. After input authentication, the server may be configured to signal one or more outcomes of eligibility criteria evaluation associated with the card. The card may be configured to receive the one or more commands-application protocol data unit after determination of a security concern. For example, the server may be configured to determine one or more security concerns. Without limitation, the one or more security concerns may be associated with identity theft, unauthorized usage based on transaction history and/or transaction frequency evaluated over any determined time period, a notice of fraudulent charges, and/or any combination thereof. For example, the server may be configured to, responsive to determining any number of one or more security concerns associated with the card, transmit one or more messages to the application of the device that are indicative of transmitting the one or more commands-application protocol data unit. In this manner, the application of the device may be configured to receive the one or more messages from the server, the one or more messages indicative of transmitting the one or more commands-application protocol data unit after determination of one or more security concerns.

[00085] The card may be subject to eligibility criteria. For example, after determination of the one or more security concerns, the card may subject to a prioritized list associated with eligibility prior to receipt of the one or more commands-application protocol data unit. In some examples, the server may be configured to screen the first device based on at least one selected from the group of time elapsed since issuance of the card, card usage for transactions, transaction type, card type, one or more determinations of the security concerns associated with the card, and/or any

combination thereof. In this manner, the server may be configured to evaluate and rank how many cards and which types of cards may be configured to receive the one or more commands-application protocol data unit based on the eligibility criteria before signaling to the application of the device to transmit the one or more commands-application protocol data unit.

[00086] At step 415, one or more processors of a card may be configured to transmit, via a communication interface, a cryptogram. For example, one or more processors of the card may be configured to create a cryptogram using one or more keys and the counter value. The cryptogram may include the counter value and the transmission data. The first device may include a memory containing one or more keys, a counter value, and the transmission data. The one or more processors may be configured to transmit the cryptogram via a communication interface. For example, the one or more processors may be configured to transmit the cryptogram to one or more applications. In some examples, the one or more processors may be configured to transmit the cryptogram to an application comprising instructions for execution on a second device. The one or more processors may be configured to update the counter value. For example, the one or more processors may be configured to update the counter value after transmission of the cryptogram.

[00087] The card may comprise a contactless card, a contact-based card, or other device described herein. As previously explained, the card may include one or more processors, and memory. The memory may include one or more applets and one or more counters. Each counter may include a counter value. The memory may include the counter value, transmission data, and one or more keys.

[00088] The card may include a communication interface. The communication interface may comprise communication capabilities with physical interfaces and contactless interfaces. For

example, the communication interface may be configured to communicate with a physical interface, such as by swiping through a card swipe interface or inserting into a card chip reader found on the automated teller machine (ATM) or other device configured to communicate over a physical interface. In other examples, the communication interface may be configured to establish contactless communication with a card reading device via a short-range wireless communication method, such as NFC, Bluetooth, Wi-Fi, RFID, and other forms of contactless communication. The communication interface may be configured to communicate directly with the application of the device, the server, and/or database via network.

[00089] The card may be in data communication with any number of components of the system. For example, the card may transmit data via network to the application of the second device, and/or server. The card may transmit data via network to database. In some examples, the card may be configured to transmit data via network after entry into one or more communication fields of any device. Without limitation, each entry may be associated with a tap, a swipe, a wave, and/or any combination thereof.

[00090] At step 420, the application of the device may be configured to transmit one or more commands-application protocol data unit. For example, the application comprising instructions for execution on the device may be configured to encrypt one or more keys. The application may be configured to transmit the one or more encrypted keys. In some examples, the application may be configured to transmit one or more parameters. Without limitation, the one or more parameters may include at least one selected from the group of primary account number information, expiration date information, card verification code, and/or any combination thereof. In some examples, the one or more parameters may comprise dynamic information, such as changed

personalization data including but not limited to card master keys, such as secret and public/private keys, and one or more spending limits. The application may be configured to transmit one or more commands-application protocol data unit including the one or more encrypted keys, the one or more parameters, one or more applet identifiers, and one or more instructions associated with a class of a header. In some examples, one or more session keys may be generated at the second device or server, which may be used to encrypt one or more master keys. In some examples, the application may be configured to transmit the one or more commands-application protocol data unit to the card after one or more entries of the communication interface into a communication field of the device. Communication between the application and the card may occur via near field communication (NFC). Without limitation, the one or more commands-application protocol data unit may be transmitted via Bluetooth, Wi-Fi, RFID.

[00091] The card may be configured to receive the one or more encrypted keys and one or more parameters after input authentication. The card may be configured to receive the command-application protocol data unit including the one or more encrypted keys, the one or more parameters, one or more applet identifiers, and one or more instructions associated with a class of a header. In some examples, one or more session keys may be generated at the second device or server, which may be used to encrypt one or more master keys. For example, one or more limited use session keys may be generated based on a cryptogram and a counter to encrypt data. The first device may be configured to receive the encrypted data and decrypt it for storage. The one or more instructions may each be associated with a code, and include decrypting and/or confirmation of the one or more decrypted keys, storing and/or confirmation of the one or more decrypted keys. In some examples, the card may be configured to receive the one or more commands-application

protocol data unit after input authentication.

[00092] In one example, one or more sets of cards may be prioritized to receive the one or more commands-application protocol data unit after the server is configured to determine whether the first device is a credit card and is associated with a notice of fraudulent charges. In another example, one or more sets of cards may be prioritized to receive the one or more commands-application protocol data unit after the server is configured to determine whether the card is an identification card that has been abnormally used, for example exceeding a predetermined threshold, for one or more transactions. In yet another example, one or more sets of the card may be prioritized to receive the one or more commands-application protocol data unit after the server is configured to determine how much time has elapsed since issuance of the card. In these non-limiting examples, the server may be further configured to prioritize which of these determinations are to be made first, second, third, etc. In this manner, a designated number of cards may be reprovisioned on an individual basis and/or in a batch. The cards may also be reprovisioned on an as-needed basis, according to a predetermined schedule, and/or any combination thereof.

[00093] At step 425, the one or more processors of the card may be configured to decrypt one or more encrypted keys of the one or more commands-application protocol data unit. The card may be configured to receive the one or more commands-application protocol data unit. For example, the card may be configured to receive the one or more commands-application protocol data unit from the application of the device. The card may be configured to decrypt the one or more encrypted keys. One or more applets of the card may be configured to store one or more decrypted keys in a secure element. A first applet may be configured to transmit, via a communication channel, the one or more decrypted keys and the one or more parameters to a

second applet.

[00094] At step 430, the one or more processors the card may be configured to switch from a first account to a second account. For example, after decryption of the one or more encrypted keys, the card may be configured to change an association from a first account to a second account. Moreover, the card may be restricted to a predetermined usage after decryption of the one or more encrypted keys. In one example, the card may be subject to one or more predetermined spending thresholds. In another example, the card may be subject to a predetermined number of uses. For example, the card may be used for only a designated set of transactions, such as for lunch only and/or for office furniture. In another example, the card may be subject to a predetermined number of usages for one or more types of transactions, including but not limited to a debit card transaction or a credit card transaction.

[00095] In another example, the card may be used for only transactions occurring during a certain time (e.g., business hours of 9:00am to 5:00pm), on certain days of the week (e.g., weekdays, weekends, only Mondays, only Thursdays and Fridays), or on a certain date (e.g., Wednesday, July 1, 2020). In another example, the card may be used only for certain purposes, such as for expense account purposes (e.g., travel expenses including airfare, meals, and hotels), for a designated project (e.g., a certain type of equipment or hardware needed for a project), with designated or approved merchants, or with a specified list of merchants known to offer goods or services needed for a particular purposes.

[00096] It is understood that the foregoing listings are exemplary and that any of these examples can be used in combination with one another. Thus, a user may use the same card configured for a variety of purposes and with a variety of accounts.

[00097] At step 435, the one or more processors of the card may be configured to transmit one or more responses-application protocol data unit. For example, the card may be configured to transmit, responsive to the one or more commands-application protocol data unit, one or more responses-application protocol data unit. The one or more responses-application protocol data unit may include one or bytes indicative of a status of the command. For example, at least one of the one or more responses-application protocol data unit may be configured to indicate an execution status associated with the one or more instructions. The card may be configured to transmit the one or more responses-application protocol data unit to the application of the device. In some examples, the card may be configured to return a successful execution status associated with the one or more instructions. To the extent that the execution status of the one or more instructions is not successful, the card may be configured to return a warning or unsuccessful execution status. For example, the one or more responses-application protocol data unit may be configured to indicate if and when the one or more encrypted keys were decrypted and/or if and when the one or more decrypted keys were stored.

[00098] Figure 5 depicts a method 500 of secure reprovisioning according to an exemplary embodiment. Figure 5 may reference the same or similar components of system 100, first device 200 of FIG. 2A and FIG. 2B, method 300 of FIG. 3, and sequence diagram 400 of FIG. 4.

[00099] At block 505, the method 500 may include validating input authentication. In some examples, an application of a device, such as an ATM, a kiosk, a point of sale device, or other device, may be configured to validate input authentication. In other examples, the application of the device may be configured to transmit input to a server for authentication. For example, input for the authentication may include, without limitation, at least one or more selected from the group

of a personal identification number, a username and/or password, a mobile device number, an account number, a card number, and a biometric (e.g., facial scan, a retina scan, a fingerprint, and a voice input for voice recognition).

[000100] The device may include one or more processors, and memory. The memory may include one or more applications, including but not limited to first application. The device may be in data communication with any number of components. For example, the device may transmit data via a network to a server. The device may transmit data via network to a database. Without limitation, the device may be a network-enabled computer. As referred to herein, a network-enabled computer may include, but is not limited to a computer device, or communications device including, e.g., a server, a network appliance, a personal computer, a workstation, a phone, a handheld PC, a personal digital assistant, a contactless card, a thin client, a fat client, an Internet browser, a kiosk, a tablet, a terminal, an ATM, or other device. The device also may be a mobile device; for example, a mobile device may include an iPhone, iPod, iPad from Apple® or any other mobile device running Apple's iOS® operating system, any device running Microsoft's Windows® Mobile operating system, any device running Google's Android® operating system, and/or any other smartphone, tablet, or like wearable mobile device.

[000101] The device may include processing circuitry and may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamperproofing hardware, as necessary to perform the functions described herein. The device 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.

[000102] The network 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 to any one of components. In some examples, the network 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.

[000103] In addition, the network may include, without limitation, telephone lines, fiber optics, IEEE Ethernet 902.3, a wide area network, a wireless personal area network, a LAN, or a global network such as the Internet. In addition, the network may support an Internet network, a wireless communication network, a cellular network, or the like, or any combination thereof. The network may further include one network, or any number of the exemplary types of networks mentioned above, operating as a stand-alone network or in cooperation with each other. The network may utilize one or more protocols of one or more network elements to which they are communicatively

coupled. The network may translate to or from other protocols to one or more protocols of network devices. Although the network is depicted as a single network, it should be appreciated that according to one or more examples, the network may comprise a plurality of interconnected networks, such as, for example, the Internet, a service provider's network, a cable television network, corporate networks, such as credit card association networks, and home networks.

[000104] The server may include one or more processors coupled to memory. The server 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. The server may be in data communication with one or more applets of a card and/or application of the device. For example, a server may be in data communication with an applet via one or more networks. A card may be in communication with one or more servers via one or more networks, and may operate as a respective front-end to back-end pair with server. The card may transmit, for example from applet executing thereon, one or more requests to server. The one or more requests may be associated with retrieving data from server. The server may receive the one or more requests from the card. Based on the one or more requests from the applet, the server may be configured to retrieve the requested data. The server may be configured to transmit the received data to the applet, the received data being responsive to one or more requests.

[000105] In some examples, the server can be a dedicated server computer, such as bladed servers, or can be personal computers, laptop computers, notebook computers, palm top computers, network computers, mobile devices, wearable devices, or any processor-controlled device capable of supporting system components of FIG. 5. It is understood that other embodiments can use multiple servers or multiple computer systems as necessary or desired to

support the users and can also use back-up or redundant servers to prevent network downtime in the event of a failure of a particular server.

[000106] The server may include an application comprising instructions for execution thereon. For example, the application may comprise instructions for execution on the server. The application may be in communication with any components of the system. For example, the server may execute one or more applications that enable, for example, network and/or data communications with one or more components of the system and transmit and/or receive data. Without limitation, server may be a network-enabled computer. As referred to herein, a network-enabled computer may include, but is not limited to a computer device, or communications device including, e.g., a server, a network appliance, a personal computer, a workstation, a phone, a handheld PC, a personal digital assistant, a contactless card, a thin client, a fat client, an Internet browser, or other device. The server also may be a mobile device; for example, a mobile device may include an iPhone, iPod, iPad from Apple® or any other mobile device running Apple's iOS® operating system, any device running Microsoft's Windows® Mobile operating system, any device running Google's Android® operating system, and/or any other smartphone, tablet, or like wearable mobile device.

[000107] The server may include processing circuitry and may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamperproofing hardware, as necessary to perform the functions described herein. The server 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.

[000108] The database may comprise a relational database, a non-relational database, or other database implementations, and any combination thereof, including a plurality of relational databases and non-relational databases. In some examples, the database may comprise a desktop database, a mobile database, or an in-memory database. Further, the database may be hosted internally by any component of the system, such as the card, device, and/or the server, or the database may be hosted externally to any component of the system, such as the card, device, and/or the server, by a cloud-based platform, or in any storage device that is in data communication with the card, device, and/or the server. In some examples, the database may be in data communication with any number of components of the system. For example, the server may be configured to retrieve the requested data from the database that is transmitted by the applet. The server may be configured to transmit the received data from the database to one or more applets via network, the received data being responsive to the transmitted one or more requests. In other examples, the one or more applets may be configured to transmit one or more requests for the requested data from the database via network.

[000109] In some examples, exemplary procedures in accordance with the present disclosure described herein can be performed by a processing arrangement and/or a computing arrangement (e.g., computer hardware arrangement). Such processing/computing arrangement can be, for

example entirely or a part of, or include, but not limited to, a computer/processor that can include, for example one or more microprocessors, and use instructions stored on a computer-accessible medium (e.g., RAM, ROM, hard drive, or other storage device). For example, a computer-accessible medium can be part of the memory of the card, device, server, and/or database, or other computer hardware arrangement.

[000110] In some examples, a computer-accessible medium (e.g., as described herein above, a storage device such as a hard disk, floppy disk, memory stick, CD-ROM, RAM, ROM, etc., or a collection thereof) can be provided (e.g., in communication with the processing arrangement). The computer-accessible medium can contain executable instructions thereon. In addition or alternatively, a storage arrangement can be provided separately from the computer-accessible medium, which can provide the instructions to the processing arrangement so as to configure the processing arrangement to execute certain exemplary procedures, processes, and methods, as described herein above, for example.

[000111] At block 510, the method 500 may include determining one or more security concerns. For example, the server may be configured to determine one or more security concerns. Without limitation, the one or more security concerns may be associated with identity theft, unauthorized usage based on transaction history and/or transaction frequency evaluated over any determined time period, a notice of fraudulent charges, and/or any combination thereof.

[000112] At block 515, the method 500 may include evaluating eligibility criteria. server may be configured to signal one or more outcomes of eligibility criteria evaluation. For example, the server may be configured to receive the input from the application. The server may be configured to authenticate the input. After input authentication, the server may be configured to signal one or

more outcomes of eligibility criteria evaluation associated with the card. The card may be configured to receive the one or more commands-application protocol data unit after determination of a security concern. For example, the server may be configured to, responsive to determining any number of one or more security concerns associated with the card, transmit one or more messages to the application of the device that are indicative of transmitting the one or more commands-application protocol data unit. In this manner, the application of the device may be configured to receive the one or more messages from the server, the one or more messages indicative of transmitting the one or more commands-application protocol data unit after determination of one or more security concerns.

[000113] The card may be subject to eligibility criteria. For example, after determination of the one or more security concerns, the card may subject to a prioritized list associated with eligibility prior to receipt of the one or more commands-application protocol data unit. In some examples, the server may be configured to screen the first device based on at least one selected from the group of time elapsed since issuance of the card, card usage for transactions, transaction type, card type, one or more determinations of the security concerns associated with the card, and/or any combination thereof. In this manner, the server may be configured to evaluate and rank how many cards and which types of cards may be configured to receive the one or more commands-application protocol data unit based on the eligibility criteria before signaling to the application of the device to transmit the one or more commands-application protocol data unit.

[000114] At block 520, the method 500 may include transmitting, after receipt of a first cryptogram, one or more first commands. For example, one or more processors of a card may be configured to transmit, via a communication interface, a first cryptogram. For example, one or

more processors of the card may be configured to create a first cryptogram using one or more keys and the counter value. The first cryptogram may include the counter value and the transmission data. The card may include a memory containing one or more keys, a counter value, and the transmission data. The one or more processors may be configured to transmit the first cryptogram via a communication interface. For example, the one or more processors may be configured to transmit the first cryptogram to one or more applications. In some examples, the one or more processors may be configured to transmit the first cryptogram to an application comprising instructions for execution on the device. The one or more processors may be configured to update the counter value. For example, the one or more processors may be configured to update the counter value after transmission of the first cryptogram.

[000115] The card may comprise a contactless card, a contact-based card, or other device described herein. As previously explained, the card may include one or more processors, and memory. The memory may include one or more applets and one or more counters. Each counter may include a counter value. The memory may include the counter value, transmission data, and one or more keys.

[000116] The card may include a communication interface. The communication interface may comprise communication capabilities with physical interfaces and contactless interfaces. For example, the communication interface may be configured to communicate with a physical interface, such as by swiping through a card swipe interface or inserting into a card chip reader found on the automated teller machine (ATM) or other device configured to communicate over a physical interface. In other examples, the communication interface may be configured to establish contactless communication with a card reading device via a short-range wireless communication

method, such as NFC, Bluetooth, Wi-Fi, RFID, and other forms of contactless communication. The communication interface may be configured to communicate directly with the application of the device, the server, and/or database via network.

[000117] The card may be in data communication with any number of components of the system. For example, the card may transmit data via network to the application of the second device, and/or server. The card may transmit data via network to database. In some examples, the card may be configured to transmit data via network after entry into one or more communication fields of any device. Without limitation, each entry may be associated with a tap, a swipe, a wave, and/or any combination thereof.

[000118] The application of the device may be configured to transmit one or more first commands-application protocol data unit. For example, the application comprising instructions for execution on the device may be configured to encrypt one or more keys. The application may be configured to transmit the one or more first encrypted keys. In some examples, the application may be configured to transmit one or more first parameters. Without limitation, the one or more parameters may include at least one selected from the group of primary account number information, expiration date information, card verification code, and/or any combination thereof. In some examples, the one or more parameters may comprise dynamic information, such as changed personalization data including but not limited to card master keys, such as secret and public/private keys, and one or more spending limits. The application may be configured to transmit one or more first commands-application protocol data unit including the one or more first encrypted keys, the one or more first parameters, one or more first applet identifiers, and one or more instructions associated with a class of a header. In some examples, one or more session keys

may be generated at the second device or server, which may be used to encrypt one or more master keys. In some examples, the application may be configured to transmit the one or more first commands-application protocol data unit to the card after one or more entries of the communication interface into a communication field of the device. Communication between the application of the first device and the card may occur via near field communication (NFC). Without limitation, the one or more first commands-application protocol data unit may be transmitted via Bluetooth, Wi-Fi, RFID.

[000119] At block 525, the method 500 may include switching, after decryption of first encrypted key, from a first account to a second account. The card may be configured to receive the one or more first encrypted keys and one or more first parameters from the application. The card may be configured to receive the first command-application protocol data unit including the one or more first encrypted keys, the one or more first parameters, one or more first applet identifiers, and one or more instructions associated with a class of a header. In some examples, one or more session keys may be generated at the second device or server, which may be used to encrypt one or more master keys. For example, one or more limited use session keys may be generated based on a cryptogram and a counter to encrypt data. The first device may be configured to receive the encrypted data and decrypt it for storage. The one or more instructions may each be associated with a code, and include decrypting and/or confirmation of the one or more first decrypted keys, storing and/or confirmation of the one or more first decrypted keys. In some examples, the card may be configured to receive the one or more first commands-application protocol data unit after input authentication.

[000120] In one example, one or more sets of cards may be prioritized to receive the one or more

first commands-application protocol data unit after the server is configured to determine whether the first device is a credit card and is associated with a notice of fraudulent charges. In another example, one or more sets of cards may be prioritized to receive the one or more first commands-application protocol data unit after the server is configured to determine whether the card is an identification card that has been abnormally used, for example exceeding a predetermined threshold, for one or more transactions. In yet another example, one or more sets of the card may be prioritized to receive the one or more first commands-application protocol data unit after the server is configured to determine how much time has elapsed since issuance of the card. In these non-limiting examples, the server may be further configured to prioritize which of these determinations are to be made first, second, third, etc. In this manner, a designated number of cards may be reprovisioned on an individual basis and/or in a batch. The cards may also be reprovisioned on an as-needed basis, according to a predetermined schedule, and/or any combination thereof.

[000121] The one or more processors of the card may be configured to decrypt one or more first encrypted keys of the one or more first commands-application protocol data unit. The card may be configured to receive the one or more first commands-application protocol data unit. For example, the card may be configured to receive the one or more first commands-application protocol data unit from the application of the first device. The card may be configured to decrypt the one or more first encrypted keys. One or more applets of the card may be configured to store one or more first decrypted keys in a secure element. A first applet may be configured to transmit, via a communication channel, the one or more first decrypted keys and the one or more first parameters to a second applet.

[000122] The one or more processors the card may be configured to switch from a first account

to a second account. For example, after decryption of the one or more first encrypted keys, the card may be configured to change an association from a first account to a second account. Moreover, the card may be restricted to a predetermined usage after decryption of the one or more first encrypted keys. In one example, the card may be subject to one or more predetermined spending thresholds. In another example, the card may be subject to a predetermined number of uses. For example, the card may be used for only a designated set of transactions, such as for lunch only and/or for office furniture. In another example, the card may be subject to a predetermined number of usages for one or more types of transactions, including but not limited to a debit card transaction or a credit card transaction.

[000123] In another example, the card may be used for only transactions occurring during a certain time (e.g., business hours of 9:00am to 5:00pm), on certain days of the week (e.g., weekdays, weekends, only Mondays, only Thursdays and Fridays), of on a certain date (e.g., Wednesday, July 1, 2020). In another example, the card may be used only for certain purposes, such as for expense account purposes (e.g., travel expenses including airfare, meals, and hotels), for a designated project (e.g., a certain type of equipment or hardware needed for a project), with designated or approved merchants, or with a specified list of merchants known to offer goods or services needed for a particular purposes.

[000124] It is understood that the foregoing listings are exemplary and that any of these examples can be used in combination with one another. Thus, a user may use the same card configured for a variety of purposes and with a variety of accounts.

[000125] At block 530, the method 500 may include transmitting one or more first responses. For example, the one or more processors of the card may be configured to transmit one or more first

responses-application protocol data unit. For example, the card may be configured to transmit, responsive to the one or more first commands-application protocol data unit, one or more first responses-application protocol data unit. The one or more first responses-application protocol data unit may include one or bytes indicative of a status of the command. For example, at least one of the one or more first responses-application protocol data unit may be configured to indicate an execution status associated with the one or more instructions. The card may be configured to transmit the one or more first responses-application protocol data unit to the application of the device. In some examples, the card may be configured to return a successful execution status associated with the one or more instructions. To the extent that the execution status of the one or more instructions is not successful, the card may be configured to return a warning or unsuccessful execution status. For example, the one or more first responses-application protocol data unit may be configured to indicate if and when the first encrypted key was decrypted and/or if and when the one or more first decrypted key was stored.

[000126] At block 535, the method 500 may include transmitting, after receipt of a second cryptogram, one or more second commands. For example, one or more processors of a card may be configured to transmit, via a communication interface, a second cryptogram. For example, one or more processors of the card may be configured to create a second cryptogram using one or more keys and the counter value. The second cryptogram may include the counter value and the transmission data. The card may include a memory containing one or more keys, a counter value, and the transmission data. The one or more processors may be configured to transmit the second cryptogram via a communication interface. For example, the one or more processors may be configured to transmit the second cryptogram to one or more applications. In some examples, the

one or more processors may be configured to transmit the second cryptogram to an application comprising instructions for execution on the second device. The application comprising instructions for execution on the second device may be different from the application comprising instructions for execution on the first device. In some examples, application for the first device may comprise an application comprising instructions for execution on a first ATM at a first location, and an application for the second device may comprise an application comprising instructions for execution on a second ATM at a second location. The one or more processors may be configured to update the counter value. For example, the one or more processors may be configured to update the counter value after transmission of the second cryptogram.

[000127] The application of a second device may be configured to transmit one or more second commands-application protocol data unit. For example, the application comprising instructions for execution on the second device may be configured to encrypt one or more second keys. The application of the second device may be configured to transmit the one or more second encrypted keys. In some examples, the application may be configured to transmit one or more second parameters. Without limitation, the one or more second parameters may include at least one selected from the group of primary account number information, expiration date information, card verification code, and/or any combination thereof. In some examples, the one or more second parameters may comprise dynamic information, such as changed personalization data including but not limited to card master keys, such as secret and public/private keys, and one or more spending limits. The application may be configured to transmit one or more second commands-application protocol data unit including the one or more second encrypted keys, the one or more second parameters, one or more second applet identifiers, and one or more instructions associated

with a class of a header. In some examples, one or more session keys may be generated at the second device or server, which may be used to encrypt one or more master keys. In some examples, the application may be configured to transmit the one or more second commands-application protocol data unit to the card after one or more entries of the communication interface into a communication field of the device. Communication between the application of the second device and the card may occur via near field communication (NFC). Without limitation, the one or more second commands-application protocol data unit may be transmitted via Bluetooth, Wi-Fi, RFID.

[000128] At block 540, the method 500 may include switching, after decryption of the second encrypted key, from the second account to the first account. The card may be configured to receive the one or more second encrypted keys and one or more second parameters from the application. The card may be configured to receive the second command-application protocol data unit including the one or more second encrypted keys, the one or more second parameters, one or more second applet identifiers, and one or more instructions associated with a class of a header. In some examples, one or more session keys may be generated at the second device or server, which may be used to encrypt one or more master keys. For example, one or more limited use session keys may be generated based on a cryptogram and a counter to encrypt data. The first device may be configured to receive the encrypted data and decrypt it for storage. The one or more instructions may each be associated with a code, and include decrypting and/or confirmation of the one or more second decrypted keys, storing and/or confirmation of the one or more second decrypted keys. In some examples, the card may be configured to receive the one or more second commands-application protocol data unit after input authentication.

[000129] In one example, one or more sets of cards may be prioritized to receive the one or more

second commands-application protocol data unit after the server is configured to determine whether the card is a credit card and is associated with a notice of fraudulent charges. In another example, one or more sets of cards may be prioritized to receive the one or more second commands-application protocol data unit after the server is configured to determine whether the card is an identification card that has been abnormally used, for example exceeding a predetermined threshold, for one or more transactions. In yet another example, one or more sets of the card may be prioritized to receive the one or more second commands-application protocol data unit after the server is configured to determine how much time has elapsed since issuance of the card. In these non-limiting examples, the server may be further configured to prioritize which of these determinations are to be made first, second, third, etc. In this manner, a designated number of cards may be reprovisioned on an individual basis and/or in a batch. The cards may also be reprovisioned on an as-needed basis, according to a predetermined schedule, and/or any combination thereof.

[000130] The one or more processors of the card may be configured to decrypt one or more second encrypted keys of the one or more second commands-application protocol data unit. The card may be configured to receive the one or more second commands-application protocol data unit. For example, the card may be configured to receive the one or more second commands-application protocol data unit from the application of the second device. The card may be configured to decrypt the one or more second encrypted keys. One or more applets of the card may be configured to store one or more second decrypted keys in a secure element. A first applet may be configured to transmit, via a communication channel, the one or more second decrypted keys and the one or more second parameters to a second applet.

[000131] The one or more processors the card may be configured to switch from the second account to the first account. For example, after decryption of the one or more second encrypted keys, the card may be configured to change an association from the second account to a first account. Moreover, the card may be restricted to a predetermined usage after decryption of the one or more second encrypted keys. In one example, the card may be subject to one or more predetermined spending thresholds. In another example, the card may be subject to a predetermined number of uses. For example, the card may be used for only a designated set of transactions, such as for lunch only and/or for office furniture. In another example, the card may be subject to a predetermined number of usages for one or more types of transactions, including but not limited to a debit card transaction or a credit card transaction.

[000132] In another example, the card may be used for only transactions occurring during a certain time (e.g., business hours of 9:00am to 5:00pm), on certain days of the week (e.g., weekdays, weekends, only Mondays, only Thursdays and Fridays), or on a certain date (e.g., Wednesday, July 1, 2020). In another example, the card may be used only for certain purposes, such as for expense account purposes (e.g., travel expenses including airfare, meals, and hotels), for a designated project (e.g., a certain type of equipment or hardware needed for a project), with designated or approved merchants, or with a specified list of merchants known to offer goods or services needed for a particular purposes.

[000133] It is understood that the foregoing listings are exemplary and that any of these examples can be used in combination with one another. Thus, a user may use the same card configured for a variety of purposes and with a variety of accounts.

[000134] At block 545, the method 500 may include transmitting one or more second responses.

For example, the one or more processors of the card may be configured to transmit one or more second responses-application protocol data unit. For example, the card may be configured to transmit, responsive to the one or more second commands-application protocol data unit, one or more responses-application protocol data unit. The one or more second responses-application protocol data unit may include one or bytes indicative of a status of the command. For example, at least one of the one or more second responses-application protocol data unit may be configured to indicate an execution status associated with the one or more instructions. The card may be configured to transmit the one or more second responses-application protocol data unit to the application of the device. In some examples, the card may be configured to return a successful execution status associated with the one or more instructions. To the extent that the execution status of the one or more instructions is not successful, the card may be configured to return a warning or unsuccessful execution status. For example, the one or more second responses-application protocol data unit may be configured to indicate if and when the second encrypted key was decrypted and/or if and when the one or more second decrypted key was stored.

[000135] Figure 6 depicts a method 600 for secure reprovisioning according to an exemplary embodiment. Figure 6 may reference the same or similar components of system 100, first device 200 of FIG. 2A and FIG. 2B, method 300 of FIG. 3, sequence diagram 400 of FIG. 4, and method 500 of FIG. 5.

[000136] At block 605, the method 600 may include identifying one or more security concerns. In some examples, a first device may be configured to receive one or more commands-application protocol data unit after determination of a security concern. For example, a server may be configured to determine one or more security concerns. Without limitation, the one or more

security concerns may be associated with identity theft, unauthorized usage based on transaction history and/or transaction frequency evaluated over any determined time period, a notice of fraudulent charges, and/or any combination thereof.

[000137] At block 610, the method 600 may include notifying an application of a device to request input. Based on one or more determinations by the server, one or more notifications may be transmitted to an application comprising instructions for execution on a second device. For example, the application may be configured to request input for authentication. For example, input for the authentication may include, without limitation, at least one or more selected from the group of a personal identification number, a username and/or password, a mobile device number, an account number, a card number, and a biometric (e.g., facial scan, a retina scan, a fingerprint, and a voice input for voice recognition). The application may be configured to authenticate the input. In other examples, the server may be configured to authenticate the input based on one or more requests transmitted from the application to the server.

[000138] At block 615, the method 600 may include prioritizing card reprovisioning sequence. For example, the server may be configured to prioritize card reprovisioning. The first device may be subject to eligibility criteria. For example, after determination of the one or more security concerns, the first device may subject to a prioritized list associated with eligibility prior to receipt of the one or more commands-application protocol data unit. In some examples, the server may be configured to screen the first device based on at least one selected from the group of time elapsed since issuance of the card, card usage for transactions, transaction type, card type, one or more determinations of the security concerns associated with the first device, and/or any combination thereof. In this manner, the server may be configured to evaluate and rank how many first devices

and which types of first devices may be configured to receive the one or more commands-application protocol data unit based on the eligibility criteria before signaling to the application of the second device to transmit the one or more commands-application protocol data unit. In one example, one or more sets of first devices may be prioritized to receive the one or more commands-application protocol data unit after the server is configured to determine whether the first device is a credit card and is associated with a notice of fraudulent charges. In another example, one or more sets of first devices may be prioritized to receive the one or more commands-application protocol data unit after the server is configured to determine whether the first device is an identification card that has been abnormally used, for example exceeding a predetermined threshold, for one or more transactions. In yet another example, one or more sets of first device may be prioritized to receive the one or more commands-application protocol data unit after the server is configured to determine how much time has elapsed since issuance of the first device. In these non-limiting examples, the server may be further configured to prioritize which of these determinations are to be made first, second, third, etc. In this manner, a designated number of first devices may be reprovisioned on an individual basis and/or in a batch. The first devices may also be reprovisioned on an as-needed basis, according to a predetermined schedule, and/or any combination thereof.

[000139] At block 620, the method 600 may include transmitting, via a communication interface, a command-application protocol data unit. In some examples, the application comprising instructions for execution on the second device may be configured to encrypt one or more keys. Without limitation, the second device may comprise an ATM, a kiosk, a point of sale device, or other device. The application may be configured to transmit the one or more encrypted keys. In

some examples, the application may be configured to transmit one or more parameters. Without limitation, the one or more parameters may include at least one selected from the group of primary account number information, expiration date information, card verification code, and/or any combination thereof. In some examples, the one or more parameters may comprise dynamic information, such as changed personalization data including but not limited to card master keys, such as secret and public/private keys, and one or more spending limits. The application may be configured to transmit one or more commands-application protocol data unit including the one or more encrypted keys, the one or more parameters, one or more applet identifiers, and one or more instructions associated with a class of a header. In some examples, one or more session keys may be generated at the second device or server, which may be used to encrypt one or more master keys. In some examples, the application may be configured to transmit the one or more commands-application protocol data unit to the first device after one or more entries of the communication interface into a communication field of the second device. Communication between the application and first device via near field communication (NFC). Without limitation, the one or more commands-application protocol data unit may be transmitted via Bluetooth, Wi-Fi, RFID.

[000140] At block 625, the method 600 may include decrypting one or more keys. The first device may be configured to receive the command-application protocol data unit including the one or more encrypted keys, the one or more parameters, one or more applet identifiers, and one or more instructions associated with a class of a header. In some examples, one or more session keys may be generated at the second device or server, which may be used to encrypt one or more master keys. For example, one or more limited use session keys may be generated based on a cryptogram and a counter to encrypt data. The first device may be configured to receive the encrypted data and

decrypt it for storage. The one or more instructions may each be associated with a code, and include decrypting and/or confirmation of the one or more decrypted keys, storing and/or confirmation of the one or more decrypted keys.

[000141] The first device may be configured to receive the one or more commands-application protocol data unit. For example, the first device may be configured to receive the one or more commands-application protocol data unit from the application of the second device. The first device may be configured to decrypt the one or more encrypted keys. One or more applets of the first device may be configured to store one or more decrypted keys in a secure element. A first applet may be configured to transmit, via a communication channel, the one or more decrypted keys and the one or more parameters to a second applet.

[000142] At block 630, the method 600 may include changing an association from a first account to a second account. After decryption of the one or more encrypted keys, the first device may be configured to change an association from a first account to a second account. Moreover, the first device may be restricted to a predetermined usage after decryption of the one or more encrypted keys. In one example, the first device may be subject to one or more predetermined spending thresholds. In another example, the first device may be subject to a predetermined number of uses. For example, the first device may be used for only a designated set of transactions, such as for lunch only and/or for office furniture. In another example, the first device may be subject to a predetermined number of usages for one or more types of transactions, including but not limited to a debit card transaction or a credit card transaction.

[000143] In another example, the first device may be used for only transactions occurring during a certain time (e.g., business hours of 9:00am to 5:00pm), on certain days of the week (e.g.,

weekdays, weekends, only Mondays, only Thursdays and Fridays), of on a certain date (e.g., Wednesday, July 1, 2020). In another example, the first device may be used only for certain purposes, such as for expense account purposes (e.g., travel expenses including airfare, meals, and hotels), for a designated project (e.g., a certain type of equipment or hardware needed for a project), with designated or approved merchants, or with a specified list of merchants known to offer goods or services needed for a particular purposes.

[000144] It is understood that the foregoing listings are exemplary and that any of these examples can be used in combination with one another. Thus, a user may use the same card configured for a variety of purposes and with a variety of accounts.

[000145] At block 635, the method 600 may include transmitting, via the communication interface, a response-application protocol data unit. The first device may be configured to transmit, responsive to the one or more commands-application protocol data unit, one or more responses-application protocol data unit. The one or more responses-application protocol data unit may include one or bytes indicative of a status of the command. For example, at least one of the one or more responses-application protocol data unit may be configured to indicate an execution status associated with the one or more instructions. The first device may be configured to transmit the one or more responses-application protocol data unit to the application of the second device. In some examples, the first device may be configured to return a successful execution status associated with the one or more instructions. To the extent that the execution status of the one or more instructions is not successful, the first device may be configured to return a warning or unsuccessful execution status. For example, the one or more responses-application protocol data unit may be configured to indicate if and when the one or more encrypted keys were decrypted

and/or if and when the one or more decrypted keys were stored.

[000146] It is further noted that the systems and methods described herein may be tangibly embodied in one of more physical media, such as, but not limited to, a compact disc (CD), a digital versatile disc (DVD), a floppy disk, a hard drive, read only memory (ROM), random access memory (RAM), as well as other physical media capable of data storage. For example, data storage may include random access memory (RAM) and read only memory (ROM), which may be configured to access and store data and information and computer program instructions. Data storage may also include storage media or other suitable type of memory (e.g., such as, for example, RAM, ROM, programmable read-only memory (PROM), erasable programmable read-only memory (EPROM), electrically erasable programmable read-only memory (EEPROM), magnetic disks, optical disks, floppy disks, hard disks, removable cartridges, flash drives, any type of tangible and non-transitory storage medium), where the files that comprise an operating system, application programs including, for example, web browser application, email application and/or other applications, and data files may be stored. The data storage of the network-enabled computer systems may include electronic information, files, and documents stored in various ways, including, for example, a flat file, indexed file, hierarchical database, relational database, such as a database created and maintained with software from, for example, Oracle® Corporation, Microsoft® Excel file, Microsoft® Access file, a solid state storage device, which may include a flash array, a hybrid array, or a server-side product, enterprise storage, which may include online or cloud storage, or any other storage mechanism. Moreover, the figures illustrate various components (e.g., servers, computers, processors, etc.) separately. The functions described as being performed at various components may be performed at other components, and the various

components may be combined or separated. Other modifications also may be made.

[000147] In the preceding specification, various embodiments have been described with references to the accompanying drawings. It will, however, be evident that various modifications and changes may be made thereto, and additional embodiments may be implemented, without departing from the broader scope of the invention as set forth in the claims that follow. The specification and drawings are accordingly to be regarded as an illustrative rather than restrictive sense.

WE CLAIM:

1. A secure reprovisioning system, comprising:

a first device having an association with a first account, comprising:

a memory containing one or more applets, a counter value, and transmission data;

a communication interface; and

one or more processors in communication with the memory and the communication interface;

wherein the first device is configured to:

create a cryptogram based on the counter value, wherein the cryptogram includes the counter value and the transmission data,

transmit, after entry of the communication interface into a communication field, the cryptogram,

update, after transmission of the cryptogram, the counter value,

receive, via the communication interface, one or more encrypted keys and one or more parameters,

decrypt the one or more encrypted keys, and

after decryption of the one or more encrypted keys, switch an association from the first account to a second account.

2. The secure reprovisioning system of claim 1, wherein the first device is configured to receive the one or more encrypted keys and the one or more parameters after a determination of a security concern.

3. The secure reprovisioning system of claim 1, wherein the first device is subject to one or more eligibility criteria prior to receiving the one or more encrypted keys and the one or more parameters.

4. The secure reprovisioning system of claim 1, wherein the one or more parameters comprises a primary account number.

5. The secure reprovisioning system of claim 1, wherein the one or more applets are configured to store the one or more decrypted keys in a secure element.

6. The secure reprovisioning system of claim 1, wherein the first device is configured to receive the one or more encrypted keys and the one or more parameters on a predetermined time basis.

7. The secure reprovisioning system of claim 1, wherein the one or more encrypted keys and the one or more parameters are received from a first automated teller machine (ATM) at a first location.

8. The secure reprovisioning system of claim 1, wherein the first device is restricted to a predetermined use.

9. The secure reprovisioning system of claim 1, wherein a first applet is configured to transmit, via a communication channel, the one or more decrypted keys and one or more parameters to a second applet.

10. The secure reprovisioning system of claim 1, wherein the first device is configured to receive a command-application protocol data unit including the one or more encrypted keys, the one or more parameters, one or more applet identifiers, and one or more instructions associated with a class.

11. The secure reprovisioning system of claim 10, wherein the first device is configured to transmit, responsive to the command-application protocol data unit, a response-application protocol data unit indicating an execution status associated with the one or more instructions.

12. A method of secure reprovisioning, comprising:

creating a cryptogram based on a counter value, wherein the cryptogram includes the counter value and transmission data;

transmitting, via a communication interface, the cryptogram;

updating the counter value;

receiving, via the communication interface, a first set of one or more encrypted keys and a first set of one or more parameters;

decrypting the first set of one or more encrypted keys; and

changing an association from a first account to a second account.

13. The method of claim 12, further comprising receiving the first set of one or more encrypted keys and the first set of one or more parameters after a determination of a security concern.

14. The method of claim 12, wherein the association is changed from the first account to the second account in response to a detection of a type of transaction.

15. The method of claim 12, wherein the first set of one or more encrypted keys and the first set of one or more parameters are received from a first automated teller machine (ATM) at a first location.

16. The method of claim 15, further comprising:

receiving, via the communication interface from a second ATM at a second location, a second set of one or more encrypted keys and a second set of one or more parameters;

decrypting the second set of one or more encrypted keys; and

changing the association from the second account to the first account.

17. The method of claim 12, further comprising transmitting a response-application protocol data unit indicating an execution status responsive to one or more instructions of a command-application protocol data unit.

18. The method of claim 12, further comprising transmitting, via a communication channel, a first set of one or more decrypted keys and first set of one or more parameters from a first applet to a second applet.

19. The method of claim 12, further comprising receiving, after input authentication, the first set of one or more encrypted keys and the first set of one or more parameters.

20. A non-transitory computer-readable medium storing instructions that, when executed by a processor, cause the processor to perform operations comprising:

creating a cryptogram based on a counter value, wherein the cryptogram includes the counter value and transmission data;

transmitting, via a communication interface, the cryptogram;

updating the counter value;

receiving, via the communication interface, a command-application protocol data unit including one or more encrypted keys, one or more parameters, one or more applet identifiers, and one or more instructions associated with a class;

decrypting the one or more encrypted keys in accordance with the one or more instructions;

switching an association from a first account to a second account; and
transmitting a response-application protocol data unit indicating an execution status
associated with the one or more instructions.