Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 3155736 A1 2021/07/08

(21) 3 155 736

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2020/11/24
(87) Date publication PCT/PCT Publication Date: 2021/07/08
(85) Entrée phase nationale/National Entry: 2022/04/22
(86) N° demande PCT/PCT Application No.: US 2020/061930
(87) N° publication PCT/PCT Publication No.: 2021/137973
(30) Priorité/Priority: 2019/12/31 (US16/731,835)

(51) Cl.Int./Int.Cl. *G06F 21/34* (2013.01), *G06Q 20/08* (2012.01), *G07F 7/10* (2006.01)

(71) Demandeur/Applicant:
CAPITAL ONE SERVICES, LLC, US

(72) Inventeurs/Inventors:
RULE, JEFFREY, US;
HART, COLIN, US;
NEWMAN, KAITLIN, US

(74) Agent: ROBIC

(54) Titre : BRANCHEMENT D'UNE CARTE SANS CONTACT A UN DISPOSITIF INFORMATIQUE POUR FOURNIR UN NUMERO VIRTUEL

(54) Title: TAPPING A CONTACTLESS CARD TO A COMPUTING DEVICE TO PROVISION A VIRTUAL NUMBER

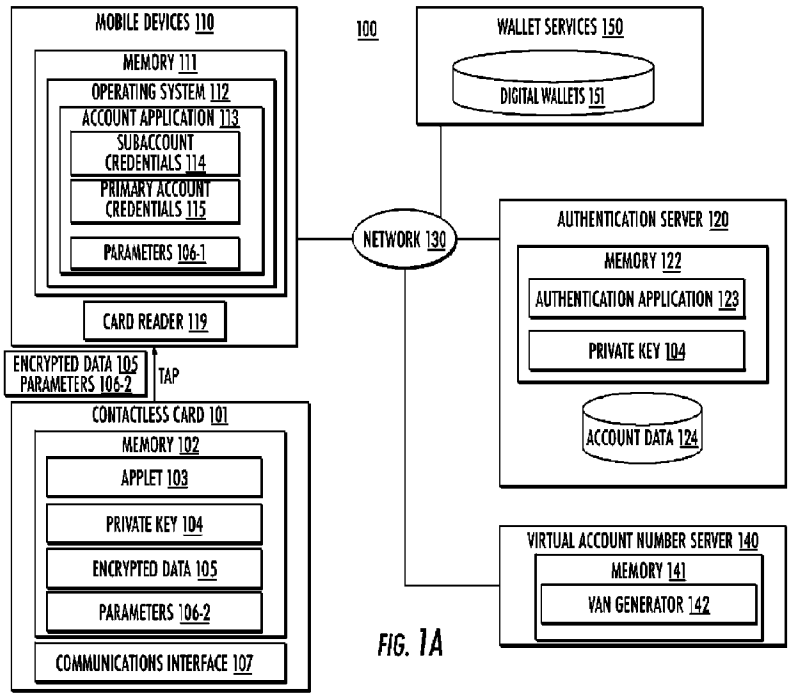

FIG. 1A

(57) Abrégé/Abstract:
Systems, methods, articles of manufacture, and computer-readable media for tapping a contactless card to a computing device to provision a virtual number. At least one parameter for authorizing a virtual account number for a subaccount associated with a primary account may be received. An application executing on a processor circuit may receive authentication credentials for the primary account. A card reader may receive encrypted data from a communications interface of a contactless card. The application may transmit the encrypted data to an authentication server. The application may receive verification of the encrypted data from the authentication server. The application may provide the at least one parameter for authorizing the virtual account number and receive a virtual account number for the subaccount generated by a virtual card number server, the virtual account number restricted to a spending limit based on the amount parameter associated with the virtual account number.

Date Submitted: 2022/04/22

CA App. No.: 3155736

Abstract:

Systems, methods, articles of manufacture, and computer-readable media for tapping a contactless card to a computing device to provision a virtual number. At least one parameter for authorizing a virtual account number for a subaccount associated with a primary account may be received. An application executing on a processor circuit may receive authentication credentials for the primary account. A card reader may receive encrypted data from a communications interface of a contactless card. The application may transmit the encrypted data to an authentication server. The application may receive verification of the encrypted data from the authentication server. The application may provide the at least one parameter for authorizing the virtual account number and receive a virtual account number for the subaccount generated by a virtual card number server, the virtual account number restricted to a spending limit based on the amount parameter associated with the virtual account number.

TAPPING A CONTACTLESS CARD TO A COMPUTING DEVICE TO PROVISION A VIRTUAL NUMBER

RELATED APPLICATIONS

[0001] This application claims priority to U.S. Patent Application Serial No. 16/731,835, titled "TAPPING A CONTACTLESS CARD TO A COMPUTING DEVICE TO PROVISION A VIRTUAL NUMBER" filed on December 31, 2019. The contents of the aforementioned application are incorporated herein by reference in their entirety.

TECHNICAL FIELD

[0002] Embodiments herein generally relate to computing platforms, and more specifically, to tapping a contactless card to a computing device to provision a virtual number.

BACKGROUND

[0003] Cardholders (e.g., credit card holders, bank card holders, etc.) often obtain additional physical cards for trusted individuals, such as family members, employees, and the like. However, obtaining additional physical cards is impractical in many situations. For example, it is impractical to obtain additional physical cards that have nominal spending limits. Similarly, it is impractical to obtain additional physical cards for users who make infrequent purchases or to deactivate and/or reactivate existing physical cards for such users.

SUMMARY

[0004] Embodiments disclosed herein provide systems, methods, articles of manufacture, and computer-readable media for tapping a contactless card to a computing device to provision a virtual number. According to one example, at least one parameter for authorizing a virtual account number for a subaccount associated with a primary account may be received, the at least one parameter comprising an amount parameter associated

with the virtual account number. An application executing on a processor circuit may receive authentication credentials for the primary account. A card reader may receive encrypted data from a communications interface of a contactless card associated with the primary account, the encrypted data generated by an applet executing in a memory of the contactless card using a cryptographic algorithm and a private key stored in the memory of the contactless card. The application may transmit the encrypted data to an authentication server associated with an issuer of the contactless card. The application may receive verification of the encrypted data from the authentication server, the authentication server to verify the encrypted data based on the cryptographic algorithm and an instance of the private key stored in a memory of the authentication server. The application may provide the at least one parameter for authorizing the virtual account number and receive a virtual account number for the subaccount generated by a virtual card number server, the virtual account number restricted to a spending limit based on the amount parameter associated with the virtual account number.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] Figures 1A-1C illustrate embodiments of a system to tap a contactless card to a computing device to provision a virtual number.

[0006] Figures 2A-2B illustrate embodiments of tapping a contactless card to a computing device to provision a virtual number.

[0007] Figures 3A-3D illustrate embodiments of tapping a contactless card to a computing device to provision a virtual number.

[0008] Figure 4 illustrates an embodiment of an interface for requesting to provision a virtual number.

[0009] Figure 5 illustrates an embodiment of an interface to manage provisioned virtual numbers.

[0010] Figure 6 illustrates an embodiment of a first logic flow.

[0011] Figure 7 illustrates an embodiment of a second logic flow.

[0012] Figure 8 illustrates an embodiment of a third logic flow.

[0013] Figure 9 illustrates an embodiment of a fourth logic flow.

[0014] Figure 10 illustrates an embodiment of a computing architecture.

[0015] Figures 11A-11B illustrate an example contactless card.

DETAILED DESCRIPTION

[0016] Embodiments disclosed herein provide secure techniques to tap a contactless card to a computing device to provision a virtual account number from one account (referred to herein as a "primary account") to one or more other accounts (referred to herein as "subaccounts"). Generally, a user may provide input to an application executing on a computing device specifying the parameters for the virtual account number. For example, the user may specify to generate a $20 virtual account number for a child to be used within one week at a general store. The user may then tap their contactless card to the computing device, which may cause the contactless card to come within communications range of the computing device. Doing so causes the contactless card to generate encrypted data which is transmitted to the computing device. The application may receive the encrypted data generated by the contactless card and transmit the encrypted data to an authentication server for validation. Once validated, the authentication server may instruct a virtual account number server to generate a virtual account number, an expiration date, and a card verification value (CVV) account associated with the contactless card. The generated virtual account number (which includes the expiration date and/or CVV) may then be transmitted to the device of the user and/or the recipient of the virtual account number. The virtual account number may also be added to a digital wallet of the recipient. The recipient may then use the virtual account number based on the input parameters. For example, the child may have one week to spend the $20 allocated to the virtual account number at the general store.

[0017] Advantageously, embodiments disclosed herein improve the security of all devices and associated data. For example, by eliminating the need for physical cards, the

risks associated with physical cards are avoided. Furthermore, the validation performed by the authentication server provides safeguards to ensure that an authorized user who has access to the physical card is requesting to generate the virtual account number. Further still, by enforcing rules associated with the generation of the virtual account number, the security of the account authorizing the generation of the virtual account number is preserved.

[0018] With general reference to notations and nomenclature used herein, one or more portions of the detailed description which follows may be presented in terms of program procedures executed on a computer or network of computers. These procedural descriptions and representations are used by those skilled in the art to most effectively convey the substances of their work to others skilled in the art. A procedure is here, and generally, conceived to be a self-consistent sequence of operations leading to a desired result. These operations are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical, magnetic, or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It proves convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like. It should be noted, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to those quantities.

[0019] Further, these manipulations are often referred to in terms, such as adding or comparing, which are commonly associated with mental operations performed by a human operator. However, no such capability of a human operator is necessary, or desirable in most cases, in any of the operations described herein that form part of one or more embodiments. Rather, these operations are machine operations. Useful machines for performing operations of various embodiments include digital computers as selectively activated or configured by a computer program stored within that is written in accordance with the teachings herein, and/or include apparatus specially constructed for the required purpose or a digital computer. Various embodiments also relate to apparatus or systems for performing these operations. These apparatuses may be specially constructed for the

required purpose. The required structure for a variety of these machines will be apparent from the description given.

[0020] Reference is now made to the drawings, wherein like reference numerals are used to refer to like elements throughout. In the following description, for the purpose of explanation, numerous specific details are set forth in order to provide a thorough understanding thereof. It may be evident, however, that the novel embodiments can be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form in order to facilitate a description thereof. The intention is to cover all modification, equivalents, and alternatives within the scope of the claims.

[0021] Figure 1A depicts a schematic of an exemplary system 100, consistent with disclosed embodiments. As shown, the system 100 includes one or more contactless cards 101, one or more computing devices 110, an authentication server 120, a virtual account number server 140, and one or more wallet services 150. The contactless cards 101 are representative of any type of payment cards, such as a credit card, debit card, ATM card, gift card, and the like. The contactless cards 101 may comprise one or more communications interfaces 107, such as a radio frequency identification (RFID) chip, configured to communicate with the computing devices 110 via NFC, the EMV standard, or other short-range protocols in wireless communication. Although NFC is used as an example communications protocol, the disclosure is equally applicable to other types of wireless communications, such as the EMV standard, Bluetooth, and/or Wi-Fi. The computing devices 110 are representative of any type of network-enabled computing devices, such as smartphones, tablet computers, wearable devices, laptops, portable gaming devices, mobile devices, workstations, desktop computers, servers, and the like. The servers 120, 140 and wallet service 150 are representative of any type of computing device, such as a server, workstation, compute cluster, cloud computing platform, virtualized computing system, and the like.

[0022] As shown, a memory 111 of the computing device 110 includes an instance of an operating system (OS) 112. Example operating systems 112 include the Android® OS, iOS®, macOS®, Linux®, and Windows® operating systems. As shown, the OS 112 includes an account application 113. The account application 113 allows users to perform

various account-related operations, such as viewing account balances, purchasing items, processing payments, and virtual account number generation and management. Initially, a user may authenticate using authentication credentials to access certain features of the account application 113. For example, the authentication credentials may include a username and password, biometric credentials (e.g., fingerprints, Face ID, etc.), and the like. As shown, the account application 113 may receive primary account credentials 114 for a primary account and/or subaccount credentials 115 for a subaccount.

[0023] Generally, a user associated with the primary account may use the account application 113 to generate a virtual account number for a subaccount according to one or more parameters 106-1 specified by the user. Similarly, a user associated with a subaccount may use the account application to request generation of a virtual account number from the primary account according to one or more parameters 106-1 specified by the user associated with the subaccount (which may be modified and/or accepted by the user of the primary account). However, in some embodiments, one or more of the parameters 106-2 stored in the memory 102 of the contactless card 101 may be used to generate the virtual account number (e.g., as default parameters that may be automatically populated in a form of the account application 113). Generally, by provisioning a virtual account number, the user of the primary account allocates funds and/or extends credit to the user of the subaccount. In at least one embodiment, the subaccount is the generated virtual account number.

[0024] For example, an employer (as primary account holder) may desire to allocate a virtual account number to an employee (as a subaccount holder) to allow the employee to purchase $2,000 worth of office furniture from one or more merchants who sell office furniture. The employer may provide the primary account credentials 115 to authenticate the primary account in the account application 113. The employer may then enter the parameters 106-1 in a form of the account application 113. The parameters 106-1 may include indications of the subaccount (or a recipient of the subaccount, if the subaccount does not exist), an amount for the virtual account number, a period of time the virtual account number can be used, and one or more merchants the virtual account number can be used. In some embodiments, the employee may provide the subaccount credentials 114 to the account application 113 to process provisioning of the virtual account number.

[0025] In response, the account application 113 may output a notification on the computing device 110 (which may be of the primary account holder and/or the subaccount holder). The notification may instruct the user to tap the contactless card 101 of the primary account holder to the computing device 110, thereby bringing the contactless card 101 sufficiently close to the card reader 119 of the computing device 110 to enable data transfer (e.g., NFC data transfer, Bluetooth data transfer, etc.) between the communications interface 107 of the contactless card 101 and the card reader 119 of the computing device 110. The applet 103 executing on a processor (not pictured) of the contactless card 101 may then generate and transmit encrypted data 105 to the computing device 110 via the communications interface 107. For example, the applet 103 of the contactless card 101 may use a cryptographic algorithm to generate a cryptographic payload of encrypted data 105 based at least in part on the private key 104 stored in the memory 102 of the contactless card 101. In such an embodiment, the private key 104 and some other piece of data (e.g., a customer identifier, an account identifier, etc.) may be provided as the input to the cryptographic algorithm, which outputs the encrypted data 105. Generally, the applet 103 may use any type of cryptographic algorithm and/or system to generate the encrypted data 105, and the use of a specific cryptographic algorithm as an example herein should not be considered limiting of the disclosure.

[0026] In some embodiments, the applet 103 may perform encryption using a key diversification technique to generate the encrypted data 105. For example, the applet may use the private key 105 in conjunction with a counter value to enhance security using key diversification. The counters may comprise values that are synchronized between the contactless card 101 and server 120. The counter value may comprise a number that changes each time data is exchanged between the contactless card 101 and the server 120 (and/or the contactless card 101 and the mobile device 110). When preparing to send data (e.g., to the server 120 and/or the mobile device 110), the contactless card 101 may increment the counter value. The contactless card 101 may then provide the master key 105 and the counter value as input to a cryptographic algorithm, which produces a diversified key as output. The diversified key may then be used to generate the encrypted data 105. The server 120 may then encrypt the private key 104 and the counter value to generate an instance of the diversified key, and decrypt the encrypted data 105 using the diversified key. The cryptographic algorithm may include encryption algorithms, hash-

based message authentication code (HMAC) algorithms, cipher-based message authentication code (CMAC) algorithms, and the like. Non-limiting examples of the cryptographic algorithm may include a symmetric encryption algorithm such as 3DES or AES128; a symmetric HMAC algorithm, such as HMAC-SHA-256; and a symmetric CMAC algorithm such as AES-CMAC. Examples of key diversification techniques are described in greater detail in United States Patent Application 16/205,119, filed November 29, 2018. The aforementioned patent application is incorporated by reference herein in its entirety.

[0027] In some embodiments, the computing device 110 may transmit a device identifier to the applet 103. The device identifier may be any identifier such as a media access control (MAC) address, unique device identifier, a software fingerprint of applications installed on the computing device 110, etc. In some such embodiments, the applet 103 determines whether the received device identifier matches (or is like) one or more permitted device identifiers stored in the parameters 106-2. If the received identifier is a match, the applet 103 may generate the encrypted data 105. If the received identifier is not a match, to preserve security, the applet 103 may refrain from generating the encrypted data 105. Furthermore, the applet 103 may apply other rules in the parameters 106-2 when determining whether to generate the encrypted data 105. For example, the parameters 106-2 may specify a threshold number of permitted virtual account numbers, and the applet 103 may determine whether the generation of an additional virtual account number would exceed the threshold. As another example, the computing device 110 may transmit the parameters 106-1 specified by the user. If the parameters 106-1 specified by the user exceed a corresponding threshold in the parameters 106-2, the applet 103 may refrain from generating the encrypted data 105. For example, if the dollar amount specified as a parameter 106-1 exceeds a maximum dollar amount specified in the parameters 106-2, the applet may refrain from generating the encrypted data 105.

[0028] Once generated, the applet 103 may transmit the encrypted data 105 to the account application 113 of the computing device 110, e.g., via NFC. In some embodiments, the applet 103 may also transmit one or more parameters from the parameters 106-2 to the account application 113. The account application 113 may transmit the encrypted data 105 and the parameters 106 (which may include one or more

of the parameters 106-1 and/or one or more of the parameters 106-2) to the authentication application 123 of the authentication server 120. The parameters 106 may include, without limitation, a primary account identifier, a subaccount identifier, a value for the virtual account, any restrictions, etc. In some embodiments, the account application 113 may determine whether the parameters 106 specified for generation of the virtual account number are permitted (e.g., based on one or more rules as described above) prior to transmitting the encrypted data 105 and/or the parameters 106 to the authentication server 120. For example, if the requested dollar amount exceeds a threshold value, the account application 113 may reject the request to generate the virtual account number. As another example, if the requested location is not located within one or more permitted areas specified in the parameters 106, the account application 113 may reject the request to generate the virtual account number. In some embodiments, the account application 113 transmits additional data to the authentication application 123 (e.g., the device identifier of the computing device 110, etc.).

[0029] Figure 1B illustrates an embodiment where the account application 113 transmits the encrypted data 105 and parameters 106 to the authentication server 120. Once received, the authentication application 123 may authenticate the encrypted data 105. For example, the authentication application 123 may attempt to decrypt the encrypted data 105 using a copy of the private key 104 stored in the memory 122 of the authentication server 120. The private key 104 may be identical to the private key 104 stored in the memory 102 of the contactless card 101, where each contactless card 101 is manufactured to include a unique private key 104 (and the authentication server 120 stores a corresponding copy of each unique private key 104). Therefore, the authentication application 123 may successfully decrypt the encrypted data 105, thereby verifying the encrypted data 105. Although the private key 104 is depicted as being stored in the memory 122, the private key 104 may be stored elsewhere, such as in a secure element and/or a hardware security module (HSM). In such embodiments, the secure element and/or the HSM may decrypt the encrypted data 105 using the private key 104 and a cryptographic function.

[0030] For example, as stated, the customer identifier (e.g., of the primary account) may be used to generate the encrypted data 105. In such an example, the authentication

application 123 may decrypt the encrypted data 105 using the private key 104 of the authentication server 120. If the result of the decryption yields the customer identifier associated with the primary account in the account data 124, the authentication application 123 verifies the encrypted data 105 and instructs the VAN generator 142 to generate a virtual account number 126 (including an expiration date and CVV) for the account associated with the contactless card 101. If the authentication application 123 is unable to decrypt the encrypted data to yield the expected result (e.g., the customer identifier of the primary account associated with the contactless card 101), the authentication application 123 does not validate the encrypted data 105. Due to the failed verification, the authentication application 123 does not instruct the VAN generator 142 to generate a virtual account number to preserve the security of the primary account.

[0031] In some embodiments, the authentication application 123 processes data received from the computing device 110 as a condition to instructing the VAN generator 142 to generate the virtual account number. For example, as with the applet 103 and/or the account application 113, the authentication application 123 may confirm whether the parameters 106 for generating the virtual account number conform with one or more rules (e.g., in the account data 124, the parameters 106-1, and/or 106-2). For example, if the requested dollar amount exceeds a threshold, the authentication application 123 may reject the request to generate the virtual account number. As another example, the authentication application 123 may determine whether the device identifier of the computing device 110 is specified as a known device identifier for the associated account in the account data 124. If the device identifier is not a known identifier, the authentication application 123 may refrain from instructing the VAN generator 142 to generate the virtual account number. Otherwise, the authentication application 123 may instruct the VAN generator 142 to generate the virtual account number. As another example, the authentication application 123 may determine whether the software fingerprint matches a known software fingerprint for the associated account in the account data 124. If the software fingerprint is not a known software fingerprint, the authentication application 123 may refrain from instructing the VAN generator 142 to generate the virtual account number. Otherwise, the authentication application 123 may instruct the VAN generator 142 to generate the virtual account number. As yet another example, the authentication application 123 may determine whether the GPS coordinates of the device 110 indicate the user is at home, at

work, or some other known address associated with the account in the account data 124. If the location of the device 110 is not within a threshold distance of the known address, the authentication application 123 may refrain from instructing the VAN generator 142 to generate the virtual account number. Otherwise, the authentication application 123 may instruct the VAN generator 142 to generate the virtual account number. As yet another example, the authentication application 123 may determine whether the GPS coordinates of the requested location to use the virtual account number are within one or more permitted locations specified in the account data 124. For example, if the requested location is within 1 mile of the home address associated with the account, and the account data 124 restricts the use of virtual card numbers to 4 miles from the home address, the authentication application 123 may instruct the VAN generator 142 to generate the virtual account number. If, however, the requested location is not within one or more permitted locations, the authentication application 123 may refrain from instructing the VAN generator 142 to generate the virtual account number.

[0032] As shown in Figure 1B, once the authentication application 123 validates the encrypted data 105, the authentication application 123 instructs the virtual account number (VAN) generator 142 in the memory 141 of the virtual account number server 140 to generate a virtual account number 126, which may include a virtual account number, expiration date, and CVV for the subaccount. In at least one embodiment, the virtual account number generated by the VAN generator 142 is restricted to one or more merchants specified in the parameters 106. The virtual account number may further include other restrictions (e.g., time restrictions, amount restrictions, location restrictions, etc.) specified by the parameters 106. For example, the virtual account number may be restricted by a location restriction defining one or more locations the virtual account number may be used. Once generated, the VAN generator 142 may transmit the virtual account number 126 (including the expiration date and/or CVV) to the account application 113 of computing device 110 (which may be the computing device 110 of the primary account holder and/or the subaccount holder). The VAN generator 142 may further transmit the virtual account number 126 to the authentication server 120. The authentication server 120 may then store the virtual account number 126 in the profile for the subaccount in the account data 124. Doing so allows the subaccount user to access the virtual account number 126 remotely.

[0033] Figure 1C depicts an embodiment where the virtual account number 126 (including the expiration date and/or CVV) generated by the VAN generator 142 is added to a digital wallet 151-1 of the subaccount holder. As shown, the virtual account number 126 may be stored in a digital wallet 151-1 in the wallet service 150 and/or the device 110. For example, the VAN generator 142 may provide the virtual account number 126 to an application program interface (API) of the wallet service 150 and/or the digital wallet 151-1. The API of the wallet service 150 and/or the digital wallet 151-1 may then add the virtual account number, CVV, and expiration date, to the digital wallet 151-1 of the subaccount user. The subaccount user may then use the virtual account number 126 in the digital wallet 151-1 as a form of payment. However, as stated, in some embodiments, the virtual account number 126 may be used as a form of payment without adding the virtual account number 126 to a digital wallet.

[0034] In some embodiments, the account number, expiration date, and CVV of the contactless card 101 may be added to the digital wallet 151-1 responsive to a tap of the contactless card 101 to the device 110, subject to verification of the encrypted data 105 generated by the contactless card 101 by the authentication server 120. In such embodiments, the authentication server 120 may provide the account number, expiration date, and CVV of the contactless card 101 to the wallet service 150 along with the account holder's name and addresses. The name and address may be received from the contactless card 101 and/or the account data 124. In another embodiment, the authentication server 120 informs the device 110 that the encrypted data 105 has been verified. The digital wallet 151-1 of the device 110 may then add the account number, expiration date, and CVV of the contactless card 101 to the digital wallet 151-1 of the user (e.g., by communicating with the wallet service 150). The account holder's name and address may further be added to the digital wallet 151-1. The name and address may be received from the contactless card 101 and/or from the account data 124 of the authentication server 120.

[0035] Generally, once generated, the virtual account number 126 may be used in accordance with the restrictions specified by the parameters 106. For example, if the parameters 106 limit the virtual account number 126 to a $50 spending limit at restaurants within 1 mile of a corporate office for one year, each attempt to use the virtual account number 126 as a form of payment will be analyzed according to the parameters 106. For

example, if an employee attempts to spend $75 at a restaurant 10 miles from the corporate office using the virtual account number 126, the payment may be declined due to the spending and location restrictions being violated. If, however, the employee attempts to spend $10 at a restaurant 0.5 miles from the corporate office 1 week after the virtual account number 126 is generated, the payment may be processed using the virtual account number 126.

[0036] Although depicted as being added via the wallet service 150 and/or the digital wallet 151-1, virtual account numbers (including expiration date, CVV, or any other account related data) may be transmitted and/or added using other techniques. For example, the virtual account numbers may be transmitted via email, text message, or any other technique. Furthermore, in one or more embodiments, the OS 112 and/or the account application 113 may detect the receipt of the virtual account numbers (e.g., virtual account number 126, expiration date, CVV, and/or any other data). For example, the OS 112 and/or the account application 113 may analyze the text of an email, text message, push notification, etc., to detect the virtual account number, CVV, expiration date, and/or other account related data. As another example, the account application 113 may receive an indication from the contactless card 101 that a data payload being transmitted includes virtual account number, expiration date, CVV, billing address, etc.

[0037] Responsive to detecting the receipt of a virtual account number (e.g., from the VAN generator 142 and/or the contactless card 101), the OS 112 and/or the account application 113 may perform any number of operations. For example, the OS 112 and/or the account application 113 may output a notification suggesting that the virtual account number be used, e.g., to complete a mobile payment. Additionally and/or alternatively, the OS 112 and/or the account application 113 may provide a selectable option (e.g., a link, button, etc.) that allows the virtual account number, expiration date, and/or CVV to be copied to a clipboard of the OS 112. Additionally and/or alternatively, the OS 112 and/or the account application 113 may autofill the virtual account number, expiration date, and/or CVV to one or more detected form fields of a form (e.g., into one or more payment fields of a form in the account application 113, OS 112, the wallet service 150, the digital wallet 151, the web browser 203, etc.). In some embodiments, the OS 112 and/or the account application 113 may autofill the data responsive to receiving user input specifying to

autofill (e.g., via a link and/or button specifying to perform the autofill that may be selected by the user). More generally, any type of operation may be performed responsive to receiving a virtual account number, CVV, expiration date, and/or any other account related data.

[0038] Figure 2A is a schematic 200 depicting an example embodiment of tapping the contactless card 101 to provision a virtual card number without requiring the recipient to authenticate in the account application 113. As shown, the account application 113 may receive the primary account credentials 115 from the user associated with the primary account. The user may further specify parameters 106-1 via the account application 113, e.g., indicating the recipient of the virtual card number, the associated amount, and/or any restrictions. As stated, in some embodiments, one or more parameters 106-2 are received from the contactless card 101. Once the parameters 106 are submitted, the account application 113 instructs the user of the primary account to tap the contactless card 101 to the computing device 110 to provision the virtual card number.

[0039] As stated, once the user taps the contactless card 101 to the computing device 110, the contactless card 101 generates the encrypted data 105. However, as shown, the memory 102 of the contactless card 101 includes a uniform resource locator (URL) 201. The URL 201 may be stored in the memory 102 and/or may be generated by the applet 103. The URL 201 may be directed to the authentication server 120, or some other URL associated with an entity issuing the contactless card 101. The URL 201 may further include data (e.g., parameters) used by the authentication server 120 to validate the data generated by the contactless card 101. For example, the applet 103 of the contactless card 101 may include the encrypted data 105 as a parameter of the URL.

[0040] In some embodiments, the encrypted data 105 may be a string of characters, for example, "ABC123". The applet 103 may include the generated encrypted data 105 as a parameter of the URL 201, thereby generating a URL with encrypted data 202. For example, the URL 201 to the authentication server 120 may be "http://www.example.com/". Therefore, the URL with encrypted data 202 may be "http://www.example.com/? ABC123". In some embodiments, the applet 103 may encode the encrypted data 105 according to an encoding format compatible with URLs prior to including the encrypted data 105 as a parameter of the URL 201. For example, the

encrypted data 105 may be a string of binary data (e.g., zeroes and ones), which may not be compatible with URLs. Therefore, the applet 103 may encode the encrypted data 105 to the American Standard Code for Information Interchange (ASCII) base64 encoding format. Doing so represents the binary encrypted data 105 in an ASCII string format by translating it into a radix-64 representation (e.g., "ABC123" in the previous example).

[0041] Once generated, the applet 103 may transmit the URL with encrypted data 202 to the mobile device 110, e.g., via NFC. In one embodiment, when received by the OS 112, the OS 112 causes a web browser 203 to access the URL with encrypted data 202. Doing so causes information describing the mobile device 110 to be sent with the request to access the URL with encrypted data 202. For example, the information may include attributes of the mobile device 110, such as the media access control (MAC) address, unique device identifier, and/or the software fingerprint of applications installed on the computing device 110. The account application 113 may further include the parameters 106, e.g., a primary account identifier, subaccount identifier, amount value, any restrictions, and the like in the URL with encrypted data 202.

[0042] In some embodiments, the URL 201 is a universal link that opens one or more pages of the account application 113. For example, the page for specifying the parameters 106 may be loaded when the URL 201 is received. As another example, a login page for receiving the primary account credentials 115 may be loaded when the URL 201 is received. Once the web browser 203 accesses the URL with encrypted data 202, the authentication server 120 and/or the authentication application 123 may extract the encrypted data 105 from the URL with encrypted data 202.

[0043] The authentication application 123 may then attempt to decrypt the encrypted data 105 using the private key 104 associated with the contactless card 101 of the primary account. As stated, in some embodiments, the encrypted data 105 is encoded by the applet 103. In such embodiments, the authentication application 123 may decode the encrypted data 105 prior to the attempted decryption. If the authentication application 123 is unable to decrypt the encrypted data to yield an expected result (e.g., a customer identifier of the primary account, etc.), the authentication application 123 does not validate the encrypted data 105 and does not instruct the VAN generator 142 to generate a virtual account number. If the authentication application 123 decrypts the encrypted data to yield an expected result

(e.g., the customer identifier of the primary account, etc.), the authentication application 123 validates the encrypted data 105, and instructs the VAN generator 142 to generate a virtual account number, expiration date, and CVV value. The authentication application 123 may further include an indication of the parameters 106 received from the account application 113 (e.g., a primary account identifier, subaccount identifier, amount value, any restrictions, etc.).

[0044] Figure 2B depicts an embodiment where the authentication application 123 verifies the encrypted data 105 extracted from the URL with encrypted data 202. In response, the VAN generator 142 generates a virtual account number 204 comprising the virtual account number, expiration date, and CVV value. As stated, the virtual account number 204 may be generated based on the parameters 106. Therefore, the virtual account number 204 may be associated with the subaccount holder and be limited to the amount specified in the parameters 106. The virtual account number 204 may further be limited in duration, limited to a type of merchant, to one or more specific merchants, to one or more geographic locations, etc., based on the parameters 106. The VAN generator 142 may then transmit the virtual account number 204 to an API of the wallet service 150, which may add the virtual account number 204 to the digital wallet 151-1 of the subaccount holder. As another example, the VAN generator 142 may transmit the virtual account number 204 to the computing device, which may add the virtual account number 204 to the digital wallet 151-1 of the subaccount holder.

[0045] Figure 3A is a schematic 300 illustrating an example of tapping the contactless card 101 to provision a virtual card number. As shown, the account application 113 executing on a computing device 110-1 outputs a graphical user interface (GUI) for receiving parameters 106. Illustratively, the GUI includes form fields 301-305, where field 301 corresponds to an amount field, field 302 corresponds to a recipient field (e.g., the subaccount), field 303 corresponds to a duration for using the virtual card number, field 304 corresponds to a merchant field, and field 305 corresponds to a location field. The form fields may be completed by the requesting user as part of a request for a virtual card number and/or by the primary account holder as part of a grant of a virtual card number. The example depicted in Figure 3A corresponds to an embodiment where the primary account holder completes the form fields 301-304. As shown, the primary account holder

user has entered an amount of $30 in field 301, an example recipient "child1" in field 302, a duration of one day in field 303, an example merchant category of hardware stores in field 304, and an example location of 2 miles from home.

[0046] Once the form in the account application 113 on the device 110-1 is submitted, the account application 113 transmits a request to the device 110-2 of the subaccount holder. In one embodiment, the account application 113 transmits the request to the authentication server 120, which may then transmit the request to the device 110-2 of the subaccount holder. Generally, the request includes the parameters 106 (e.g., at least indications of the values entered in form fields 301-305 and/or other parameters resolved based on the values entered in the form fields 301-305. As shown, the account application 113 on the computing device 110-2 has received authentication credentials for the subaccount. In addition, the account application 113 on the computing device 110-2 requires credentials for the primary account (a fingerprint in this example). The account application 113 on the computing device 110-2 may then instruct the primary account holder to tap the contactless card 101 to the computing device 110-2. The applet 103 of the contactless card 101 may then generate and transmit encrypted data 105 to the computing device 110-2. The account application 113 on computing device 110-2 may then transmit the encrypted data 105 to the authentication server 120 along with the parameters 106 (e.g., the values from the form fields 301-304). The authentication server 120 may then validate the encrypted data 105 and instruct the VAN generator 142 to generate a virtual account number, expiration date, and CVV subject to the restrictions specified by the parameters 106. The VAN generator 142 may then transmit the generated virtual account number to the computing device 110-2 of the subaccount holder. The subaccount holder may then view the generated virtual account number and/or otherwise use the virtual account number as a form of payment.

[0047] Figure 3B is a schematic 310 illustrating an example of tapping the contactless card 101 to add an account number to a digital wallet 151. As shown, the computing device 110-1 outputs a GUI specifying to tap the contactless card to add a card to a digital wallet. The GUI may be part of the account application 113 and/or a different application (e.g., a GUI provided by one or more wallet services 150). As shown, the GUI provides the user with an option to specify whether to add a virtual account number, e.g., by checking the

checkbox 311. If the user selects the checkbox 311, a virtual account number generated by the VAN generator 142 may be added to the corresponding wallet 151. If the user does not select the checkbox 311, the card number associated with the contactless card may be added to the corresponding wallet 151. Furthermore, as shown, the GUI includes checkboxes 312-313 to allow the user to specify which wallets 151 the account number should be added to. For example, as shown, the user has selected checkbox 312, but not checkbox 313. Therefore, the account number may be added to the example wallet 151 of "wallet x", but not "wallet y". The different wallets "wallet x" and "wallet y" may be provided by the same wallet service 150 and/or different wallet services 150.

[0048] Once the user taps the contactless card 101 to the device 110-1, the applet 103 of the contactless card 101 may then generate and transmit encrypted data 105 to the computing device 110-1. The computing device 110-1 may then transmit the encrypted data 105 to the authentication server 120. In some embodiments, the applet 103 transmits additional data to the computing device 110-1 (e.g., the account number of the contactless card 101, the expiration date of the contactless card 101, the CVV of the contactless card 101, the name of the account holder, and one or more addresses of the account holder). In such embodiments, the computing device 110-1 may transmit the additional data to the authentication server 120. The computing device 110-1 may further transmit, to the authentication server 120, whether the user specified to generate a virtual account number and indications of each selected wallet (e.g., generate a virtual account number for wallet x).

[0049] The authentication application 123 may then validate the encrypted data 105 as described above. In one embodiment, the authentication application 123 may transmit the account number, expiration date, and CVV of the contactless card 101 to the wallet service 150 for addition to the specified wallet 151. The authentication application 123 may further provide additional information to the wallet service 150 for addition to the wallet 151, e.g., a name and/or addresses to be associated with the virtual account number. The name and/or addresses may be received from the contactless card 101 and/or received from the account data 124 by the authentication application 123. In another embodiment, the authentication application 123 may transmit an indication of the validation of the encrypted data to the device 110-1, where the user may use a GUI provided by the wallet service 150 to add the

account number to the wallet 151. In such embodiments, the authentication application 123 may optionally transmit the account number, expiration date, CVV, name, and/or addresses to the device 110-1.

[0050] If the user specified to generate a virtual account number via the GUI in Figure 3B, the authentication application 123 may validate the encrypted data 105 and instruct the VAN generator 142 to generate a virtual account number, expiration date, and CVV. The VAN generator 142 may then generate the virtual account number, expiration date, and CVV. In one embodiment, the VAN generator 142 may transmit the virtual account number, expiration date, and CVV to the wallet service 150. The VAN generator 142 may specify an identifier of the wallet 151 the virtual account number, expiration date, and CVV should be added to by the wallet service 150. The VAN generator 142 may further provide additional information to the wallet service 150 for addition to the wallet 151, e.g., a name and/or addresses to be associated with the virtual account number. The name and/or addresses may be received from the contactless card 101 and/or received from the account data 124 (e.g., by the VAN generator 142 and/or the authentication application 123). In another embodiment, the VAN generator 142 transmits the generated virtual account number, expiration date, and CVV to the device 110-1, where the user may use the GUI provided by the wallet service 150 to add the virtual account number to the wallet 151. In such embodiments, the VAN generator 142 may optionally transmit the account holder name, and/or addresses to the device 110-1.

[0051] Figure 3C is a schematic 315 depicting an embodiment where the VAN generator 142 directly added a virtual account number to the user's wallet 151 in the wallet service 150. However, as stated, if a virtual account number is not generated, the authentication server 120 may directly add the account number, expiration date, and CVV of the contactless card 101 to the user's wallet 151 in the wallet service 150. In such an example, the GUI depicted in Figure 3C may be updated accordingly.

[0052] As stated, the GUI depicted in Figure 3B may be provided by the wallet service 150 (and/or an application associated with the wallet service 150). Figure 3D is a schematic 320 reflecting such an example. In Figure 3D, the authentication server 120 has validated the encrypted data 105 generated by the contactless card 101 responsive to a tap of the contactless card 101 to the device 110-1. Once validated, the authentication server 120

may transmit an indication of the validation of the encrypted data 105 to the GUI provided by the wallet service 150 on the device 110-1. As shown, the GUI provided by the wallet service 150 on the device 110-1 then outputs fields 321-325. The fields 321-325 may be automatically populated with data. The populated values in fields 321-325 are examples and should not be considered limiting of the disclosure.

[0053] For example, field 321 corresponds to an account number, and may be populated to include the virtual account number generated by the VAN generator 142 and/or the account number of the contactless card 101. The account number may be obfuscated to preserve privacy. Similarly, field 322 corresponds to an expiration date, and may be populated to include the expiration date generated by the VAN generator 142 and/or the expiration date of the contactless card 101. Field 323 corresponds to CVV value and may be populated to include the CVV generated by the VAN generator 142 and/or the CVV of the contactless card 101. Field 324 corresponds to an account holder name and may be populated to include the account holder name received from the authentication server 120, VAN generator 142, and/or the contactless card 101. Field 325 corresponds to an account holder address and may be populated to include the account holder address received from the authentication server 120, VAN generator 142, and/or the contactless card 101. The user may then submit the information in populated fields 321-325 to the wallet service 150 for addition to the user's wallet 151 via the submit button 326.

[0054] As stated, the data populated in fields 321-325 may be received from the contactless card 101 responsive to a tap of the contactless card. In such embodiments, the GUI provided by the wallet service 150 on the device 110-1 may instruct the user to tap the contactless card 101 to the device 110-1 (e.g., without presenting the GUI of Figure 3B). Responsive to a single tap of the contactless card 101, the applet 103 may generate the encrypted data 105 and transmit the encrypted data 105 to the device 110-1 along with the account number, expiration date, and CVV of the contactless card 101. The GUI provided by the wallet service 150 (and/or the account application 113) may then transmit the encrypted data 105 to the authentication server 120, which may validate the encrypted data 105. Once the GUI provided by the wallet service 150 receives an indication that the authentication server 120 validated the encrypted data 105, the values may be programmatically populated into the fields 321-325 of the GUI. In one embodiment, the

account holder name and/or address are received from the applet 103 with the encrypted data 105. In another embodiment, the account holder name and/or address are received from the authentication server 120. The user may then submit the populated data via the submit button 326, which adds the data of the contactless card 101 to the wallet 151 in the wallet service 150.

[0055] Figure 4 is a schematic 400 illustrating an example of tapping the contactless card 101 to provision a virtual account number. As shown, the account application 113 executing on a computing device 110-3 outputs a GUI for receiving parameters 106. Illustratively, the GUI includes form fields 401-403, where field 401 corresponds to an amount field, field 402 corresponds to a primary account field (e.g., the primary account holder), and field 403 corresponds to a merchant field. The form fields may be completed by the requesting user as part of a request for a virtual card number and/or by the primary account holder as part of a grant of a virtual card number. The example depicted in Figure 4 corresponds to an embodiment where an employee completes the form fields 401-403 as part of a request to provision a subaccount. Embodiments are not limited in this context. For example, a child may use the GUI of Figure 4 to request a subaccount authorized via the GUI of Figure 3A.

[0056] As shown in Figure 4, the employee has entered an amount of $300 in field 401, an example primary account of "Employer" in field 402, and an example merchant category of hardware stores in field 403. Once the employee selects the submit button 404, the account application 113 transmits a request to the primary account holder. The request may generally be approved by the primary account holder (e.g., using the GUI depicted in Figure 3A). Although not depicted for the sake of clarity, the account application 113 on the device 110 of the primary account holder may instruct the primary account holder to tap their contactless card 101 to the device 110 to approve the request. In some embodiments, the primary account holder may add and/or modify the requested parameters, e.g., to impose a location restriction on the request. The contactless card 101 may then generate encrypted data 105, which is sent to the account application 113 on the computing device 110 of the primary account holder (e.g., the employer). The account application 113 of the primary account holder may then transmit the encrypted data 105 and parameters 106 (e.g., the values in fields 401-403 and/or indications thereof) to the

authentication application 123. The authentication application 123 may then validate the encrypted data 105 and instruct the VAN generator 142 to generate a virtual account number, expiration date, and CVV that is limited to $300 and can be used at merchants in the hardware store category. The virtual account number may then be sent to the requesting device 110-3 of the subaccount holder and/or added to the digital wallet 151 of the subaccount holder.

[0057] Figure 5 is a schematic 500 illustrating a GUI of the account application 113 for managing provisioned virtual card numbers. As shown, the GUI of the account application 113 on a computing device 110-4 lists one or more previously generated virtual card numbers associated with the primary account and one or more subaccounts. As shown, the GUI of the account application 113 allows the primary account holder to activate and/or deactivate the virtual card numbers. For example, as shown, the checkbox 501 is unchecked, thereby indicating the associated virtual card number is not activated. If, however, the user checks the checkbox 501, the account application 113 may reactivate the virtual account number. In some embodiments, the account application 113 requires the user to tap the contactless card 101 to the device 110-4 to reactivate the virtual account number (e.g., by generating encrypted data 105 that is verified by the authentication server 120, which may then add the requested funds to the reactivated virtual account number).

[0058] Similarly, the checkboxes 502-503 are checked, indicating the associated virtual card numbers are active. If the user unchecks one or more of checkboxes 502-503, the associated virtual account numbers are deactivated. In one embodiment, the account application 113 requires the user to tap the contactless card 101 to deactivate the virtual account numbers. In other embodiments, the virtual account numbers are deactivated without requiring the user tap the contactless card 101 to the device 110-4.

[0059] Operations for the disclosed embodiments may be further described with reference to the following figures. Some of the figures may include a logic flow. Although such figures presented herein may include a particular logic flow, it can be appreciated that the logic flow merely provides an example of how the general functionality as described herein can be implemented. Further, a given logic flow does not necessarily have to be executed in the order presented unless otherwise indicated. In addition, the given logic

flow may be implemented by a hardware element, a software element executed by a processor, or any combination thereof. The embodiments are not limited in this context.

[0060] Figure 6 illustrates an embodiment of a logic flow 600. The logic flow 600 may be representative of some or all of the operations executed by one or more embodiments described herein. For example, the logic flow 600 may include some or all of the operations to use a contactless card to provision a virtual account number. Embodiments are not limited in this context.

[0061] As shown, the logic flow 600 begins at block 605, where the account application 113 receives parameters 106 for authorizing a virtual account number for a subaccount associated with a primary account. The parameters 106 may include user-defined parameters and/or parameters 106 received from the contactless card 101. The subaccount may be associated with the primary account in any way, such as an organizational relationship, familial relationship, friendship, and the like. For example, a parent may provide parameters 106 specifying to generate a $20 virtual account number for their child which is valid for one week and can be used at bookstores within 2 miles of the city center. At block 610, the account application 113 receives primary account credentials 115 to authenticate the primary account.

[0062] At block 615, a user taps the contactless card 101 to the computing device 110 to cause the contactless card 101 to generate and transmit encrypted data 105. At block 620, the applet 103 of the contactless card 101 may generate the encrypted data 105 using the private key 104, input data (e.g., the customer identifier), and a cryptographic algorithm. The applet 103 may then transmit the encrypted data 105 to the computing device 110 at block 625. At block 630, the account application 113 may transmit the encrypted data 105 received from the contactless card 101 to the authentication server 120. The account application 113 may further transmit one or more parameters 106 to the authentication server 120, e.g., the parameters received at block 605. More generally, the parameters may include the primary account identifier, subaccount identifier, amount value, any restrictions, etc.

[0063] At block 635, the authentication application 123 decrypts the encrypted data 105 using the private key 104 in the memory 122 of the authentication server 120 to

validate the encrypted data 105. At block 640, the authentication application 123 transmits an indication to the VAN generator 142 specifying to generate a virtual account number, expiration date, and CVV. The authentication application 123 may further transmit the received parameters 106 and/or any data from the account data 124 to the VAN generator 142. At block 645, the VAN generator 142 generates the virtual account number, expiration date, and CVV in accordance with the parameters 106. For example, the VAN generator 142 may limit the virtual account number to $30 that can be used by the child at bookstores within 2 miles of the city center for one week. At block 650, the VAN generator 142 transmits the virtual account number, expiration date, and CVV to the computing device 110. As stated, responsive to receiving the virtual account number, expiration date, and CVV, the account application 113 and/or the OS 112 may detect the virtual account number, expiration date, and CVV and perform an operation. For example, the account application 113 and/or the OS 112 may autofill the virtual account number, expiration date, and/or CVV into one or more form fields, copy the virtual account number, expiration date, and/or CVV to a clipboard, etc.

[0064] At block 655, the account application 113 and/or the VAN generator 142 may provide the virtual account number, expiration date, and CVV to the digital wallet 151 of the subaccount holder (e.g., via the device 110 and/or the wallet service 150). Similarly, the VAN generator 142 may provide the virtual account number, expiration date, and CVV to the authentication server 120, which may store the virtual account number, expiration date, and CVV in the account data 124 (or another database for storing virtual card numbers) of the subaccount holder. At block 660, the subaccount holder optionally uses the virtual account number, expiration date, and CVV to complete a transaction. For example, the child may use the virtual account number, expiration date, and CVV to purchase $20 worth of books from a bookstore the day after the VAN generator 142 generates the virtual account number, expiration date, and CVV.

[0065] Figure 7 illustrates an embodiment of a logic flow 700. The logic flow 700 may be representative of some or all of the operations executed by one or more embodiments described herein. For example, the logic flow 700 may include some or all of the operations to receive parameters for provisioning a virtual account number using the contactless card 101. Embodiments are not limited in this context.

[0066] As shown, the logic flow 700 begins at block 705, where the account application 113 receives a request to generate a virtual account number comprising one or more parameters 106 from a subaccount user. For example, the child may request $30 from their parent at block 705. At block 710, the account application 113 may receive at least one parameter 106 from the primary account holder. For example, the parent may specify that the requested amount can only be used at bookstores 5 miles from home. At block 715, the account application 113 receives one or more parameters 106-2 from the contactless card 101. For example, the parameters 106 of the contactless card 101 may specify a valid duration of 1 week for any virtual number provisioned using the contactless card 101. At block 720, the account application 113 may receive one or more parameters 106 from the authentication server 120. For example, the account data 124 of the parent may specify a parameter 106 limiting the amount of funds for any virtual number provisioned using the contactless card 101 to a maximum of $20. Therefore, using the parameters received at blocks 705-720, the account application 113 receives parameters 106 specifying to generate a virtual account number limited to $20 in spending for one week at bookstores five miles from the home address associated with the primary account.

[0067] Figure 8 illustrates an embodiment of a logic flow 800. The logic flow 800 may be representative of some or all of the operations executed by one or more embodiments described herein. For example, the logic flow 800 may include some or all of the operations performed by the applet executing in a contactless card. Embodiments are not limited in this context.

[0068] As shown, the logic flow 800 begins at block 805, where the applet 103 executing in the memory 102 of the contactless card 101 of the primary account holder receives an identifier of a subaccount device 110. The identifier may be, for example, and without limitation, a media access control (MAC) address, unique device identifier, and/or the software fingerprint of applications installed on the computing device 110. At block 810, the applet 103 determines that the received identifier is specified as the identifier of an authorized device of the primary account holder. For example, the applet 103 may find a matching identifier in the memory 102 that indicates the device is authorized by the primary account holder. At block 815, the applet 103 generates encrypted data 105 based on the private key 104. The applet 103 may further generate a URL that includes the

encrypted data 105 as a parameter, where the URL is directed to the authentication server. The applet 103 may further include any parameters 106-2 stored in the memory of the contactless card 101. The applet 103 may then transmit the encrypted data 105, URL, and/or parameters 106-2 to the computing device 110 of the subaccount holder.

[0069] Figure 9 illustrates an embodiment of a logic flow 900. The logic flow 900 may be representative of some or all of the operations executed by one or more embodiments described herein. For example, the logic flow 900 may include some or all of the operations performed by the account application 113 to provision a virtual account number. Embodiments are not limited in this context.

[0070] As shown, the logic flow 900 begins at block 905, where the account application 113 receives encrypted data 105 and a URL from the contactless card. In one embodiment, the encrypted data 105 is a parameter of the URL. In some embodiments, the account application 113 and/or the applet 103 may encode the encrypted data 105 into an encoding format compatible with URLs. At block 910, the account application 113 and/or a web browser on the computing device 110 may follow the URL, which may be directed to the authentication server 120 and/or the authentication application 123. As part of following the URL, the account application 113 may provide parameters 106 for generating a virtual account number for a subaccount holder.

[0071] At block 915, the authentication application 123 authenticates the encrypted data 105 included as a parameter in the URL. If the encrypted data is encoded, the authentication application 123 may decode the encrypted data 105. As stated, to authenticate the encrypted data 105, the authentication application 123 decrypts the encrypted data using the private key 104. At block 920, the authentication application 123 transmits an indication to the VAN generator 142 authorizing the generation of a virtual account number, expiration date, and CVV. The authentication application 123 may further provide the parameters 106 to the VAN generator 142 to allow the VAN generator 142 to implement any restrictions on the virtual account number (e.g., amount restrictions, time restrictions, location restrictions, merchant restrictions, etc.). The VAN generator 142 may generate the virtual card data comprising the virtual account number, expiration date, and CVV (and any restrictions) at block 925.

[0072] At block 930, the VAN generator 142 provides the generated virtual account number to an API of the digital wallet service 150. The VAN generator 142 may further provide an indication of the digital wallet 151 of the subaccount holder, which may be received from the account data 142. At block 935, the digital wallet service 150 adds the virtual account number, expiration date, and CVV to the digital wallet 151 of the subaccount holder. The subaccount holder may then use the virtual account number via the digital wallet 151 to pay for transactions.

[0073] Figure 10 illustrates an embodiment of an exemplary computing architecture 1000 comprising a computing system 1002 that may be suitable for implementing various embodiments as previously described. In various embodiments, the computing architecture 1000 may comprise or be implemented as part of an electronic device. In some embodiments, the computing architecture 1000 may be representative, for example, of a system that implements one or more components of the system 100. In some embodiments, computing system 1002 may be representative, for example, of the contactless card 101, computing devices 110, authentication server 120, virtual account number server 140, and/or the wallet services 150 of the system 100. The embodiments are not limited in this context. More generally, the computing architecture 1000 is configured to implement all logic, applications, systems, methods, apparatuses, and functionality described herein with reference to Figures 1-9.

[0074] As used in this application, the terms "system" and "component" and "module" are intended to refer to a computer-related entity, either hardware, a combination of hardware and software, software, or software in execution, examples of which are provided by the exemplary computing architecture 1000. For example, a component can be, but is not limited to being, a process running on a computer processor, a computer processor, a hard disk drive, multiple storage drives (of optical and/or magnetic storage medium), an object, an executable, a thread of execution, a program, and/or a computer. By way of illustration, both an application running on a server and the server can be a component. One or more components can reside within a process and/or thread of execution, and a component can be localized on one computer and/or distributed between two or more computers. Further, components may be communicatively coupled to each other by various types of communications media to coordinate operations. The coordination may

involve the uni-directional or bi-directional exchange of information. For instance, the components may communicate information in the form of signals communicated over the communications media. The information can be implemented as signals allocated to various signal lines. In such allocations, each message is a signal. Further embodiments, however, may alternatively employ data messages. Such data messages may be sent across various connections. Exemplary connections include parallel interfaces, serial interfaces, and bus interfaces.

[0075] The computing system 1002 includes various common computing elements, such as one or more processors, multi-core processors, co-processors, memory units, chipsets, controllers, peripherals, interfaces, oscillators, timing devices, video cards, audio cards, multimedia input/output (I/O) components, power supplies, and so forth. The embodiments, however, are not limited to implementation by the computing system 1002.

[0076] As shown in Figure 10, the computing system 1002 comprises a processor 1004, a system memory 1006 and a system bus 1008. The processor 1004 can be any of various commercially available computer processors, including without limitation an AMD® Athlon®, Duron® and Opteron® processors; ARM® application, embedded and secure processors; IBM® and Motorola® DragonBall® and PowerPC® processors; IBM and Sony® Cell processors; Intel® Celeron®, Core®, Core (2) Duo®, Itanium®, Pentium®, Xeon®, and XScale® processors; and similar processors. Dual microprocessors, multi-core processors, and other multi processor architectures may also be employed as the processor 1004.

[0077] The system bus 1008 provides an interface for system components including, but not limited to, the system memory 1006 to the processor 1004. The system bus 1008 can be any of several types of bus structure that may further interconnect to a memory bus (with or without a memory controller), a peripheral bus, and a local bus using any of a variety of commercially available bus architectures. Interface adapters may connect to the system bus 1008 via a slot architecture. Example slot architectures may include without limitation Accelerated Graphics Port (AGP), Card Bus, (Extended) Industry Standard Architecture ((E)ISA), Micro Channel Architecture (MCA), NuBus, Peripheral Component Interconnect (Extended) (PCI(X)), PCI Express, Personal Computer Memory Card International Association (PCMCIA), and the like.

[0078] The system memory 1006 may include various types of computer-readable storage media in the form of one or more higher speed memory units, such as read-only memory (ROM), random-access memory (RAM), dynamic RAM (DRAM), Double-Data-Rate DRAM (DDRAM), synchronous DRAM (SDRAM), static RAM (SRAM), programmable ROM (PROM), erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM), flash memory (e.g., one or more flash arrays), polymer memory such as ferroelectric polymer memory, ovonic memory, phase change or ferroelectric memory, silicon-oxide-nitride-oxide-silicon (SONOS) memory, magnetic or optical cards, an array of devices such as Redundant Array of Independent Disks (RAID) drives, solid state memory devices (e.g., USB memory, solid state drives (SSD) and any other type of storage media suitable for storing information. In the illustrated embodiment shown in Figure 10, the system memory 1006 can include non-volatile memory 1010 and/or volatile memory 1012. A basic input/output system (BIOS) can be stored in the non-volatile memory 1010.

[0079] The computing system 1002 may include various types of computer-readable storage media in the form of one or more lower speed memory units, including an internal (or external) hard disk drive (HDD) 1014, a magnetic floppy disk drive (FDD) 1016 to read from or write to a removable magnetic disk 1018, and an optical disk drive 1020 to read from or write to a removable optical disk 1022 (e.g., a CD-ROM or DVD). The HDD 1014, FDD 1016 and optical disk drive 1020 can be connected to the system bus 1008 by a HDD interface 1024, an FDD interface 1026 and an optical drive interface 1028, respectively. The HDD interface 1024 for external drive implementations can include at least one or both of Universal Serial Bus (USB) and IEEE 1394 interface technologies. The computing system 1002 is generally is configured to implement all logic, systems, methods, apparatuses, and functionality described herein with reference to Figures 1-9.

[0080] The drives and associated computer-readable media provide volatile and/or nonvolatile storage of data, data structures, computer-executable instructions, and so forth. For example, a number of program modules can be stored in the drives and memory units 1010, 1012, including an operating system 1030, one or more application programs 1032, other program modules 1034, and program data 1036. In one embodiment, the one or more application programs 1032, other program modules 1034, and program data 1036 can

include, for example, the various applications and/or components of the system 100, e.g., the applet 103, private keys 104, encrypted data 105, parameters 106, operating system 112, account application 113, the authentication application 123, the wallet services 150, and/or digital wallets 151.

[0081] A user can enter commands and information into the computing system 1002 through one or more wire/wireless input devices, for example, a keyboard 1038 and a pointing device, such as a mouse 1040. Other input devices may include microphones, infra-red (IR) remote controls, radio-frequency (RF) remote controls, game pads, stylus pens, card readers, dongles, finger print readers, gloves, graphics tablets, joysticks, keyboards, retina readers, touch screens (e.g., capacitive, resistive, etc.), trackballs, trackpads, sensors, styluses, and the like. These and other input devices are often connected to the processor 1004 through an input device interface 1042 that is coupled to the system bus 1008, but can be connected by other interfaces such as a parallel port, IEEE 1394 serial port, a game port, a USB port, an IR interface, and so forth.

[0082] A monitor 1044 or other type of display device is also connected to the system bus 1008 via an interface, such as a video adaptor 1046. The monitor 1044 may be internal or external to the computing system 1002. In addition to the monitor 1044, a computer typically includes other peripheral output devices, such as speakers, printers, and so forth.

[0083] The computing system 1002 may operate in a networked environment using logical connections via wire and/or wireless communications to one or more remote computers, such as a remote computer 1048. The remote computer 1048 can be a workstation, a server computer, a router, a personal computer, portable computer, microprocessor-based entertainment appliance, a peer device or other common network node, and typically includes many or all of the elements described relative to the computing system 1002, although, for purposes of brevity, only a memory/storage device 1050 is illustrated. The logical connections depicted include wire/wireless connectivity to a local area network (LAN) 1052 and/or larger networks, for example, a wide area network (WAN) 1054. Such LAN and WAN networking environments are commonplace in offices and companies, and facilitate enterprise-wide computer networks, such as intranets, all of which may connect to a global communications network, for example, the Internet. In

embodiments, the network 130 of Figure 1 is one or more of the LAN 1052 and the WAN 1054.

[0084] When used in a LAN networking environment, the computing system 1002 is connected to the LAN 1052 through a wire and/or wireless communication network interface or adaptor 1056. The adaptor 1056 can facilitate wire and/or wireless communications to the LAN 1052, which may also include a wireless access point disposed thereon for communicating with the wireless functionality of the adaptor 1056.

[0085] When used in a WAN networking environment, the computing system 1002 can include a modem 1058, or is connected to a communications server on the WAN 1054, or has other means for establishing communications over the WAN 1054, such as by way of the Internet. The modem 1058, which can be internal or external and a wire and/or wireless device, connects to the system bus 1008 via the input device interface 1042. In a networked environment, program modules depicted relative to the computing system 1002, or portions thereof, can be stored in the remote memory/storage device 1050. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers can be used.

[0086] The computing system 1002 is operable to communicate with wired and wireless devices or entities using the IEEE 802 family of standards, such as wireless devices operatively disposed in wireless communication (e.g., IEEE 802.16 over-the-air modulation techniques). This includes at least Wi-Fi (or Wireless Fidelity), WiMax, and Bluetooth™ wireless technologies, among others. Thus, the communication can be a predefined structure as with a conventional network or simply an ad hoc communication between at least two devices. Wi-Fi networks use radio technologies called IEEE 802.11x (a, b, g, n, etc.) to provide secure, reliable, fast wireless connectivity. A Wi-Fi network can be used to connect computers to each other, to the Internet, and to wire networks (which use IEEE 802.3-related media and functions).

[0087] Figure 11A illustrates a contactless card 101, which may comprise a payment card, such as a credit card, debit card, and/or a gift card. As shown, the contactless card 101 may be issued by a service provider 1102 displayed on the front or back of the card 101. In some examples, the contactless card 101 is not related to a payment card, and may

comprise, without limitation, an identification card. In some examples, the payment card may comprise a dual interface contactless payment card. The contactless card 101 may comprise a substrate 1110, which may include a single layer or one or more laminated layers composed of plastics, metals, and other materials. Exemplary substrate materials include polyvinyl chloride, polyvinyl chloride acetate, acrylonitrile butadiene styrene, polycarbonate, polyesters, anodized titanium, palladium, gold, carbon, paper, and biodegradable materials. In some examples, the contactless card 101 may have physical characteristics compliant with the ID-1 format of the ISO/IEC 7810 standard, and the contactless card may otherwise be compliant with the ISO/IEC 14443 standard. However, it is understood that the contactless card 101 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.

[0088] The contactless card 101 may also include identification information 1115 displayed on the front and/or back of the card, and a contact pad 1120. The contact pad 1120 may be configured to establish contact with another communication device, such as the mobile devices 110, a user device, smart phone, laptop, desktop, or tablet computer. The contactless card 101 may also include processing circuitry, antenna and other components not shown in FIG. 11A. These components may be located behind the contact pad 1120 or elsewhere on the substrate 1110. The contactless card 101 may also include a magnetic strip or tape, which may be located on the back of the card (not shown in FIG. 11A).

[0089] As illustrated in FIG. 11B, the contact pad 1120 of contactless card 101 may include processing circuitry 1125 for storing and processing information, including a microprocessor 1130 and the memory 102. It is understood that the processing circuitry 1125 may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anti-collision algorithms, controllers, command decoders, security primitives and tamper proofing hardware, as necessary to perform the functions described herein.

[0090] The memory 102 may be a read-only memory, write-once read-multiple memory or read/write memory, e.g., RAM, ROM, and EEPROM, and the contactless card 101 may include one or more of these memories. A read-only memory may be factory

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

[0091] The memory 102 may be configured to store one or more applets 103, the private key 104, the encrypted data 105, the parameters 106-2, and one or more customer (or user) identifiers (IDs) 1107. The one or more applets 103 may comprise one or more software applications configured to execute on one or more contactless cards, such as a Java® Card applet. However, it is understood that applets 103 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 customer ID 1107 may comprise a unique alphanumeric identifier assigned to a user of the contactless card 101, and the identifier may distinguish the user of the contactless card from other contactless card users. In some examples, the customer ID 1107 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. In some embodiments, the applet 103 may use the customer ID 1107 as input to a cryptographic algorithm with the private key 1108 to generate the encrypted data 108.

[0092] The processor and memory elements of the foregoing exemplary embodiments are described with reference to the contact pad, but the present disclosure is not limited thereto. It is understood that these elements may be implemented outside of the pad 1120 or entirely separate from it, or as further elements in addition to processor 1130 and memory 102 elements located within the contact pad 1120.

[0093] In some examples, the contactless card 101 may comprise one or more antennas 1155. The one or more antennas 1155 may be placed within the contactless card 101 and around the processing circuitry 1125 of the contact pad 1120. For example, the one or more antennas 1155 may be integral with the processing circuitry 1125 and the one or more antennas 1155 may be used with an external booster coil. As another example, the one or more antennas 1155 may be external to the contact pad 1120 and the processing circuitry 1125.

[0094] In an embodiment, the coil of contactless card 101 may act as the secondary of an air core transformer. The terminal may communicate with the contactless card 101 by cutting power or amplitude modulation. The contactless card 101 may infer the data transmitted from the terminal using the gaps in the contactless card's power connection, which may be functionally maintained through one or more capacitors. The contactless card 101 may communicate back by switching a load on the contactless card's coil or load modulation. Load modulation may be detected in the terminal's coil through interference. More generally, using the antennas 1155, processing circuitry 1125, and/or the memory 102, the contactless card 101 provides a communications interface to communicate via NFC, Bluetooth, and/or Wi-Fi communications.

[0095] As explained above, contactless cards 101 may be built on a software platform operable on smart cards or other devices having limited memory, such as JavaCard, and one or more or more applications or applets may be securely executed. Applets may be added to contactless cards to provide a one-time password (OTP) for multifactor authentication (MFA) in various mobile application-based use cases. Applets may be configured to respond to one or more requests, such as near field data exchange requests, from a reader, such as a mobile NFC reader (e.g., the card reader 119 of the device 110), and produce an NDEF message that comprises a cryptographically secure OTP encoded as an NDEF text tag.

[0096] Various embodiments may be implemented using hardware elements, software elements, or a combination of both. Examples of hardware elements may include processors, microprocessors, circuits, circuit elements (e.g., transistors, resistors, capacitors, inductors, and so forth), integrated circuits, application specific integrated circuits (ASIC), programmable logic devices (PLD), digital signal processors (DSP), field programmable gate array (FPGA), logic gates, registers, semiconductor device, chips, microchips, chip sets, and so forth. Examples of software may include software components, programs, applications, computer programs, application programs, system programs, machine programs, operating system software, middleware, firmware, software modules, routines, subroutines, functions, methods, procedures, software interfaces, application program interfaces (API), instruction sets, computing code, computer code, code segments, computer code segments, words, values, symbols, or any combination

thereof. Determining whether an embodiment is implemented using hardware elements and/or software elements may vary in accordance with any number of factors, such as desired computational rate, power levels, heat tolerances, processing cycle budget, input data rates, output data rates, memory resources, data bus speeds and other design or performance constraints.

[0097] One or more aspects of at least one embodiment may be implemented by representative instructions stored on a machine-readable medium which represents various logic within the processor, which when read by a machine causes the machine to fabricate logic to perform the techniques described herein. Such representations, known as "IP cores" may be stored on a tangible, machine readable medium and supplied to various customers or manufacturing facilities to load into the fabrication machines that make the logic or processor. Some embodiments may be implemented, for example, using a machine-readable medium or article which may store an instruction or a set of instructions that, if executed by a machine, may cause the machine to perform a method and/or operations in accordance with the embodiments. Such a machine may include, for example, any suitable processing platform, computing platform, computing device, processing device, computing system, processing system, computer, processor, or the like, and may be implemented using any suitable combination of hardware and/or software. The machine-readable medium or article may include, for example, any suitable type of memory unit, memory device, memory article, memory medium, storage device, storage article, storage medium and/or storage unit, for example, memory, removable or non-removable media, erasable or non-erasable media, writeable or re-writeable media, digital or analog media, hard disk, floppy disk, Compact Disk Read Only Memory (CD-ROM), Compact Disk Recordable (CD-R), Compact Disk Rewriteable (CD-RW), optical disk, magnetic media, magneto-optical media, removable memory cards or disks, various types of Digital Versatile Disk (DVD), a tape, a cassette, or the like. The instructions may include any suitable type of code, such as source code, compiled code, interpreted code, executable code, static code, dynamic code, encrypted code, and the like, implemented using any suitable high-level, low-level, object-oriented, visual, compiled and/or interpreted programming language.

[0098] The foregoing description of example embodiments has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the present disclosure to the precise forms disclosed. Many modifications and variations are possible in light of this disclosure. It is intended that the scope of the present disclosure be limited not by this detailed description, but rather by the claims appended hereto. Future filed applications claiming priority to this application may claim the disclosed subject matter in a different manner, and may generally include any set of one or more limitations as variously disclosed or otherwise demonstrated herein.

CLAIMS

What is claimed is:

1. An apparatus, comprising:

a processor circuit; and

a memory storing instructions which when executed by the processor circuit, cause the processor circuit to:

receive at least one parameter for authorizing a virtual account number for a subaccount associated with a primary account, the at least one parameter comprising an amount parameter associated with the virtual account number;

receive, by an application executing on the processor circuit, authentication credentials for the primary account;

receive, by a card reader of the apparatus, encrypted data from a contactless card associated with the primary account, the encrypted data based on a cryptographic algorithm and a private key;

transmit, by the application, the encrypted data to an authentication server associated with an issuer of the contactless card;

receive, by the application, verification of the encrypted data from the authentication server based on the cryptographic algorithm and the private key;

provide, by the application to the server, the at least one parameter for authorizing the virtual account number; and

receive, by the application, a virtual account number for the subaccount generated by a virtual card number server, the virtual account number restricted to a spending limit based on the amount parameter associated with the virtual account number.

2. The apparatus of claim 1, the memory storing instructions which when executed by the processor circuit, cause the processor circuit to:

provide, by the application, the virtual account number to an application programming interface (API) of a digital wallet service to add the virtual account number to a digital wallet of a user associated with the subaccount.

3. The apparatus of claim 1, wherein the apparatus comprises a first apparatus associated with the subaccount, the at least one parameter received from at least one of: (i) an applet executing in the memory of the contactless card, (ii) the first apparatus, and (iii) a second apparatus associated with the primary account.

4. The apparatus of claim 3, the at least one parameter received from the second apparatus associated with the primary account.

5. The apparatus of claim 4, the at least one parameter received by the instance of the application executing on the processor circuit of the second apparatus responsive to a request generated by the instance of the application executing on the processor circuit of the first apparatus.

6. The apparatus of claim 1, wherein the at least one parameter further comprises a time parameter specifying a time limit for using the virtual account number, a location parameter specifying one or more locations where the virtual number can be used, and a merchant parameter specifying one or more merchants where the virtual account number can be used.

7. The apparatus of claim 1, the memory storing instructions which when executed by the processor circuit, cause the processor circuit to:

output, by the application on a display, a plurality of virtual account numbers provided to a plurality of subaccounts associated with the primary account;

receive selection of one of the plurality of virtual account numbers, the selected one of the plurality of virtual account numbers comprising an inactive virtual account number; and

activate the selected one of the plurality of virtual account numbers, the activating to provide an additional amount of funds to the activated virtual account number.

8. A method, comprising:

receiving, at least one parameter for authorizing a virtual account number for a subaccount associated with a primary account, the at least one parameter comprising an amount parameter associated with the virtual account number;

receiving, by an application executing on a processor circuit of a first device, authentication credentials for the primary account;

receiving, by a card reader of the first device, encrypted data from a communications interface of a contactless card associated with the primary account, the encrypted data generated by an applet executing in a memory of the contactless card using a cryptographic algorithm and a private key stored in the memory of the contactless card;

transmitting, by the application, the encrypted data to an authentication server associated with an issuer of the contactless card;

receiving, by the application, verification of the encrypted data from the authentication server, the authentication server to verify the encrypted data based on the cryptographic algorithm and an instance of the private key stored in a memory of the authentication server;

providing, by the application to the server, the at least one parameter for authorizing the virtual account number; and

receiving, by the application, a virtual account number for the subaccount generated by a virtual card number server, the virtual account number restricted to a spending limit based on the amount parameter associated with the virtual account number.

9. The method of claim 8, further comprising:

providing, by the application, the virtual account number to an application programming interface (API) of a digital wallet service to add the virtual account number to a digital wallet of a user associated with the subaccount.

10. The method of claim 8, wherein the first device is associated with the subaccount, the at least one parameter received from at least one of: (i) the applet executing in the memory of the contactless card, (ii) the first device, and (iii) a second device associated with the primary account, wherein the at least one parameter further comprises a time

parameter specifying a time limit for using the virtual account number, a location parameter specifying one or more locations where the virtual account number can be used, and a merchant parameter specifying one or more merchants where the virtual account number can be used.

11. The method of claim 10, the at least one parameter received from the second device associated with the primary account, the authentication server further configured to:

receive, from an instance of the application executing on a processor circuit of the second device, encrypted data received by the second device from the communications interface of the contactless card associated with the primary account; and

verify the encrypted data received by the second device from the communications interface of the contactless card associated with the primary account.

12. The method of claim 11, the at least one parameter received by the instance of the application executing on the processor circuit of the second device responsive to a request generated by the instance of the application executing on the processor circuit of the first device.

13. The method of claim 8, the applet executing in the memory of the contactless card configured to:

receive an identifier of the first device, the identifier comprising one or more of: (i) a medium access control (MAC) address of the card reader, (ii) a unique identifier of the first device, and (iii) a software fingerprint of the first device generated based on a plurality of applications installed on the first device; and

determine that the identifier of the first device is specified as one of a plurality of devices associated with the primary account.

14. The method of claim 8, wherein the communication interface of the contactless card is configured to support at least one of near field communication (NFC), Bluetooth, and Wi-Fi, the method further comprising:

outputting, by the application on a display, a plurality of virtual account numbers provided to a plurality of subaccounts associated with the primary account;

receiving selection of one of the plurality of virtual account numbers, the selected one of the plurality of virtual account numbers comprising an inactive virtual account number; and

activating the selected one of the plurality of virtual account numbers, the activating to provide an additional amount of funds to the activated virtual account number.

15. A non-transitory computer-readable storage medium having computer-readable program code embodied therewith, the computer-readable program code executable by a processor circuit of a first device to cause the processor circuit to:

receive at least one parameter for authorizing a virtual account number for a subaccount associated with a primary account, the at least one parameter comprising an amount parameter associated with the virtual account number;

receive, by an application executing on the processor circuit, authentication credentials for the primary account;

receive, by a card reader, encrypted data from a communications interface of a contactless card associated with the primary account, the encrypted data based on a cryptographic algorithm and a private key;

transmit, by the application, the encrypted data to an authentication server associated with an issuer of the contactless card;

receive, by the application, verification of the encrypted data from the authentication server based on the cryptographic algorithm and the private key;

provide, by the application to the server, the at least one parameter for authorizing the virtual account number; and

receive, by the application, a virtual account number for the subaccount generated by a virtual card number server, the virtual account number restricted to a spending limit based on the amount parameter associated with the virtual account number.

16. The non-transitory computer-readable storage medium of claim 15, further comprising computer-readable program code executable by the processor circuit to cause the processor circuit to:

provide, by the application, the virtual account number to an application programming interface (API) of a digital wallet service to add the virtual account number to a digital wallet of a user associated with the subaccount.

17. The non-transitory computer-readable storage medium of claim 15, wherein the first device is associated with the subaccount, the at least one parameter received from at least one of: (i) an applet executing in the contactless card, (ii) the first device, and (iii) a second device associated with the primary account.

18. The non-transitory computer-readable storage medium of claim 17, the at least one parameter received from the second device associated with the primary account, storing instructions which when executed by the authentication server cause the authentication server to:

receive, from an instance of the application executing on a processor circuit of the second device, encrypted data received by the second device from the communications interface of the contactless card associated with the primary account; and

verify the encrypted data received by the second device from the communications interface of the contactless card associated with the primary account.

19. The non-transitory computer-readable storage medium of claim 18, the at least one parameter received by the instance of the application executing on the processor circuit of the second device responsive to a request generated by the instance of the application executing on the processor circuit of the first device.

20. The non-transitory computer-readable storage medium of claim 15, wherein the at least one parameter further comprises a time parameter specifying a time limit for using the virtual account number, a location parameter specifying one or more locations where the virtual number can be used, and a merchant parameter specifying one or more merchants where the virtual account number can be used.

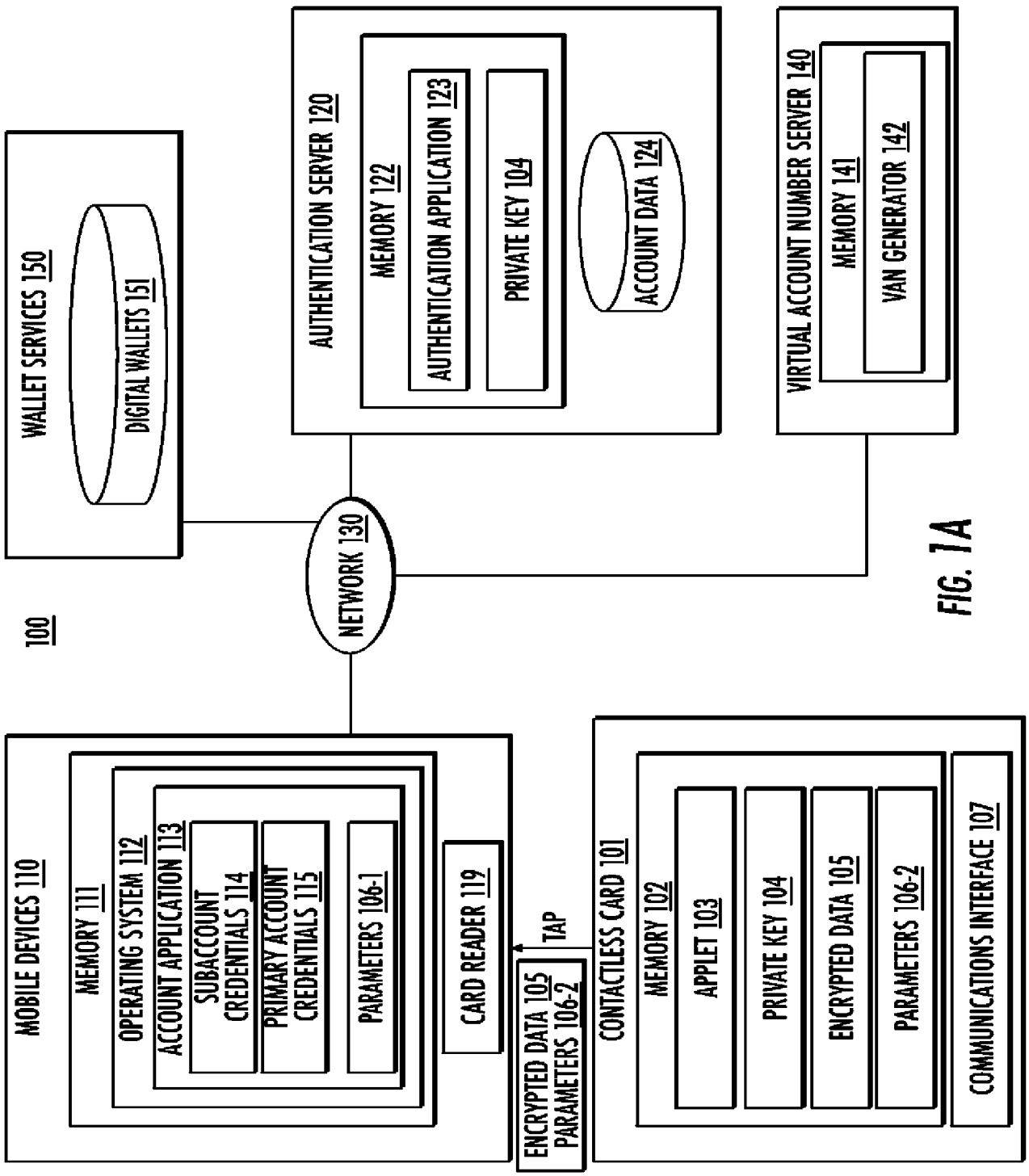
100
WALLET SERVICES 150
DIGITAL WALLETS 151
AUTHENTICATION SERVER 120
MEMORY 122
AUTHENTICATION APPLICATION 123
PRIVATE KEY 104
ACCOUNT DATA 124
VIRTUAL ACCOUNT NUMBER SERVER 140
MEMORY 141
VAN GENERATOR 142
NETWORK 130
MOBILE DEVICES 110
MEMORY 111
OPERATING SYSTEM 112
ACCOUNT APPLICATION 113
SUBACCOUNT CREDENTIALS 114
PRIMARY ACCOUNT CREDENTIALS 115
PARAMETERS 106-1
CARD READER 119
ENCRYPTED DATA 105
PARAMETERS 106-2
TAP
CONTACTLESS CARD 101
MEMORY 102
APPLET 103
PRIVATE KEY 104
ENCRYPTED DATA 105
PARAMETERS 106-2
COMMUNICATIONS INTERFACE 107

FIG. 1A

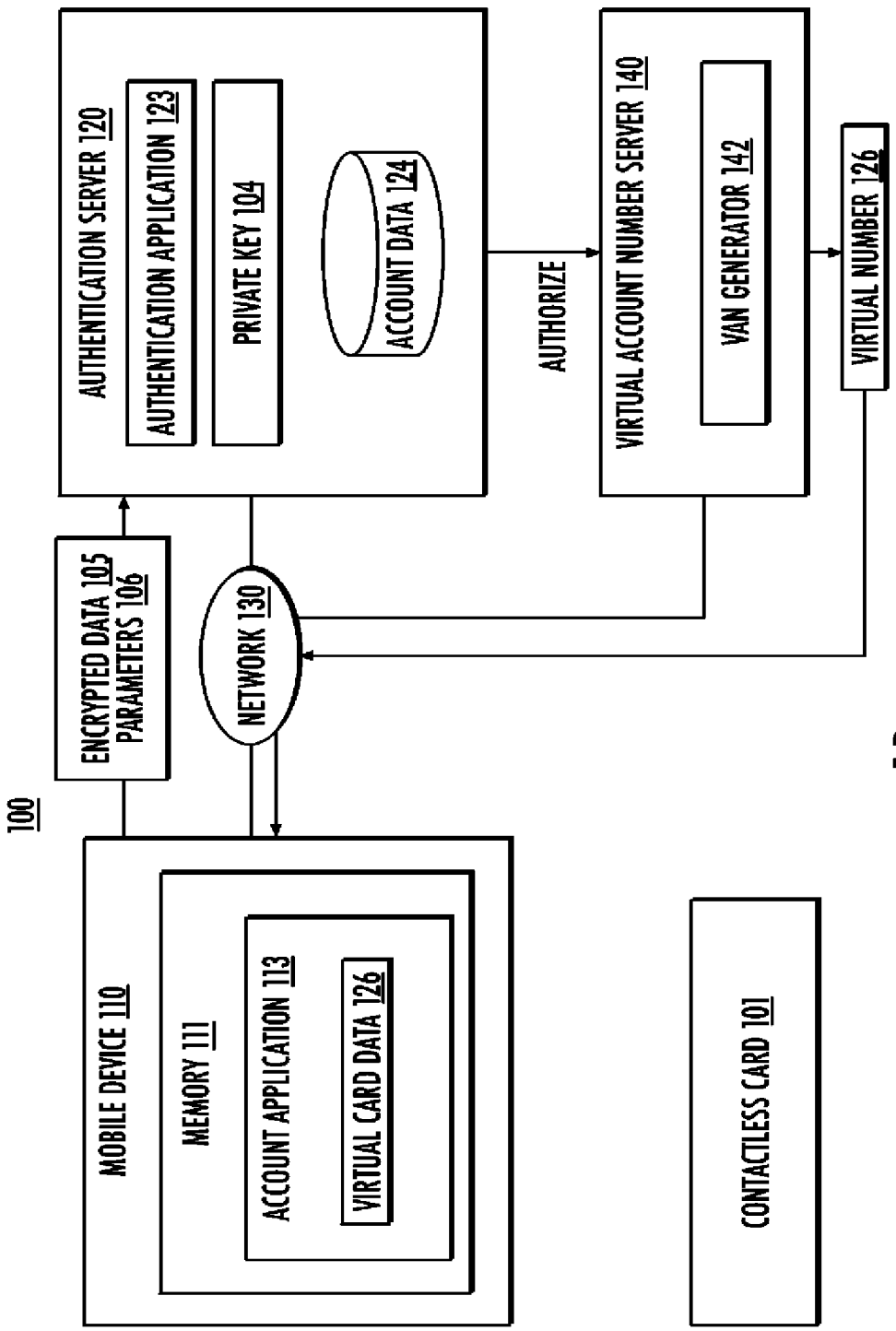
100
MOBILE DEVICE 110
MEMORY 111
ACCOUNT APPLICATION 113
VIRTUAL CARD DATA 126
CONTACTLESS CARD 101
ENCRYPTED DATA 105
PARAMETERS 106
NETWORK 130
AUTHENTICATION SERVER 120
AUTHENTICATION APPLICATION 123
PRIVATE KEY 104
ACCOUNT DATA 124
AUTHORIZE
VIRTUAL ACCOUNT NUMBER SERVER 140
VAN GENERATOR 142
VIRTUAL NUMBER 126

FIG. 1B

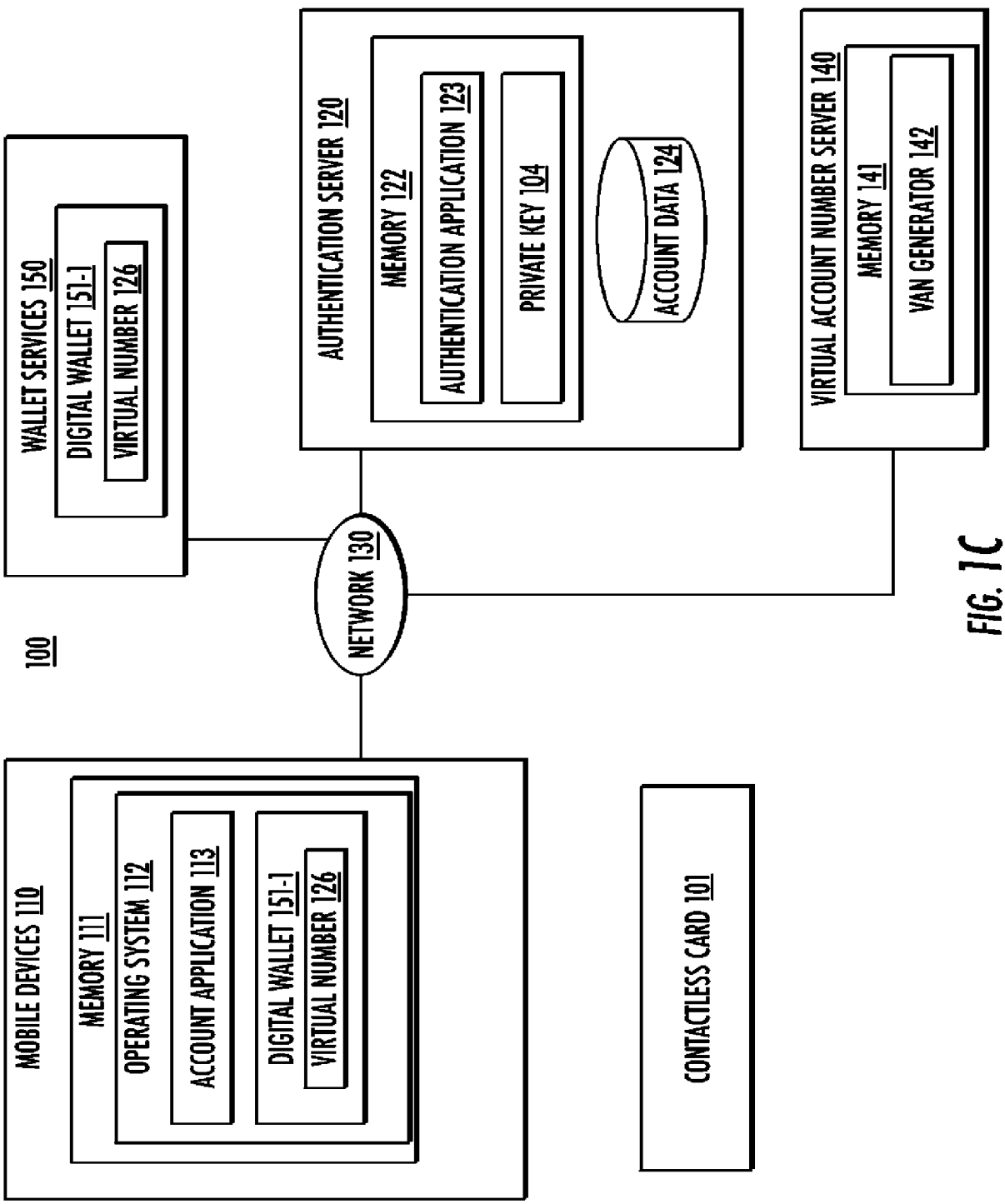
100
MOBILE DEVICES 110
MEMORY 111
OPERATING SYSTEM 112
ACCOUNT APPLICATION 113
DIGITAL WALLET 151-1
VIRTUAL NUMBER 126
CONTACTLESS CARD 101
NETWORK 130
WALLET SERVICES 150
DIGITAL WALLET 151-1
VIRTUAL NUMBER 126
AUTHENTICATION SERVER 120
MEMORY 122
AUTHENTICATION APPLICATION 123
PRIVATE KEY 104
ACCOUNT DATA 124
VIRTUAL ACCOUNT NUMBER SERVER 140
MEMORY 141
VAN GENERATOR 142

FIG. 1C

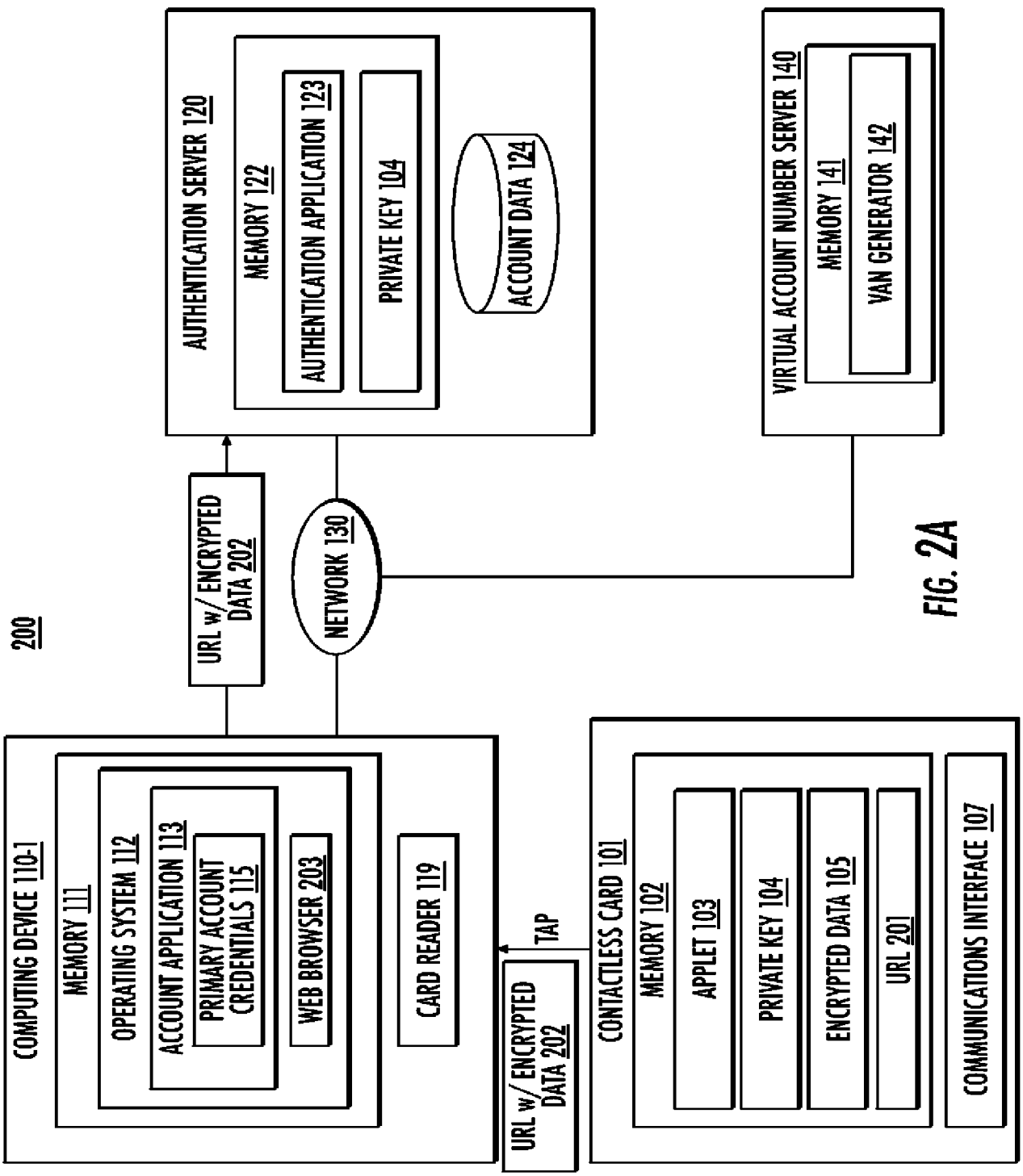
200
COMPUTING DEVICE 110-1
MEMORY 111
OPERATING SYSTEM 112
ACCOUNT APPLICATION 113
PRIMARY ACCOUNT CREDENTIALS 115
WEB BROWSER 203
CARD READER 119
URL w/ ENCRYPTED DATA 202
TAP
CONTACTLESS CARD 101
MEMORY 102
APPLET 103
PRIVATE KEY 104
ENCRYPTED DATA 105
URL 201
COMMUNICATIONS INTERFACE 107
URL w/ ENCRYPTED DATA 202
NETWORK 130
AUTHENTICATION SERVER 120
MEMORY 122
AUTHENTICATION APPLICATION 123
PRIVATE KEY 104
ACCOUNT DATA 124
VIRTUAL ACCOUNT NUMBER SERVER 140
MEMORY 141
VAN GENERATOR 142

FIG. 2A

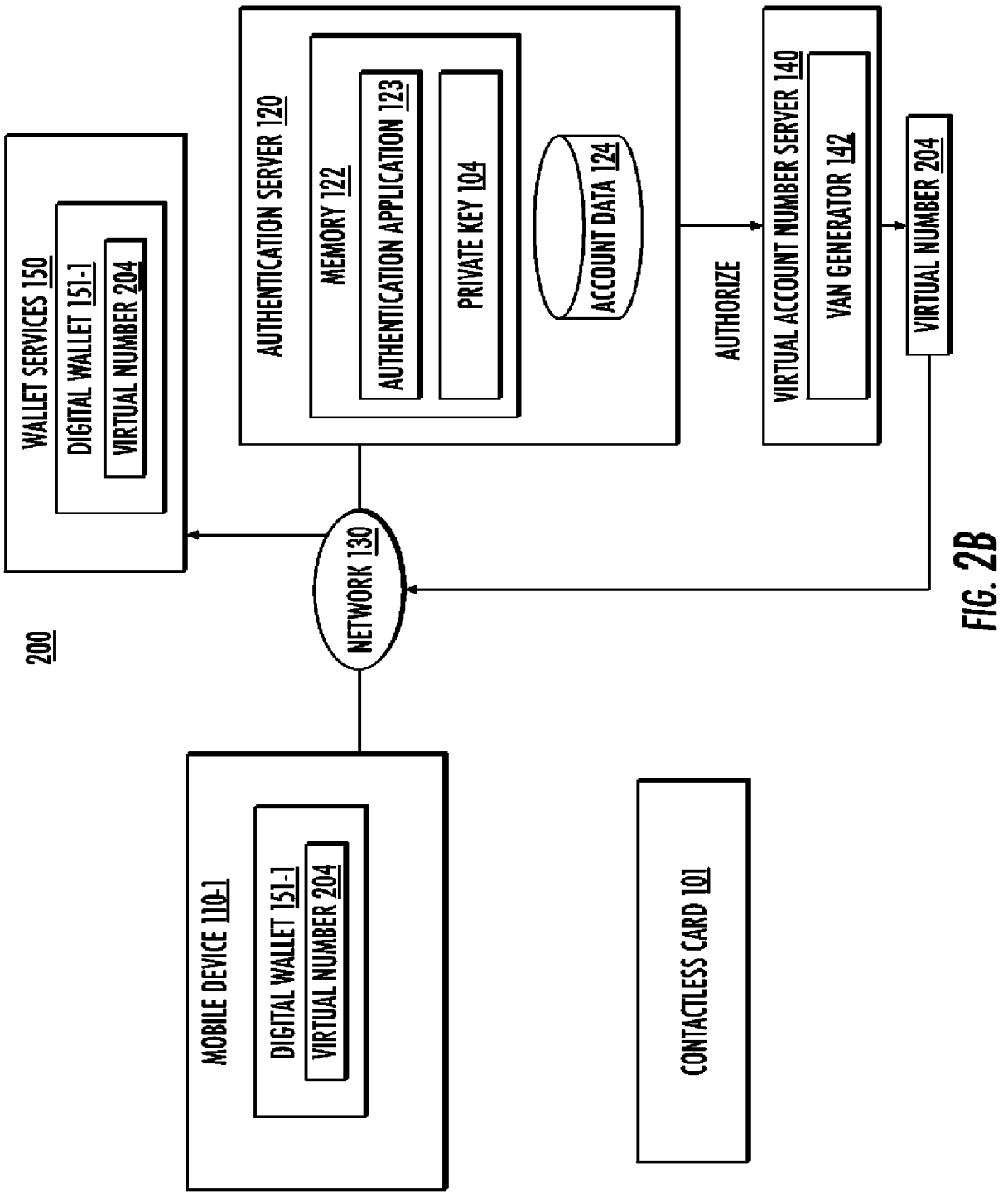
200
WALLET SERVICES 150
DIGITAL WALLET 151-1
VIRTUAL NUMBER 204
AUTHENTICATION SERVER 120
MEMORY 122
AUTHENTICATION APPLICATION 123
PRIVATE KEY 104
ACCOUNT DATA 124
AUTHORIZE
VIRTUAL ACCOUNT NUMBER SERVER 140
VAN GENERATOR 142
VIRTUAL NUMBER 204
NETWORK 130
MOBILE DEVICE 110-1
DIGITAL WALLET 151-1
VIRTUAL NUMBER 204
CONTACTLESS CARD 101

FIG. 2B

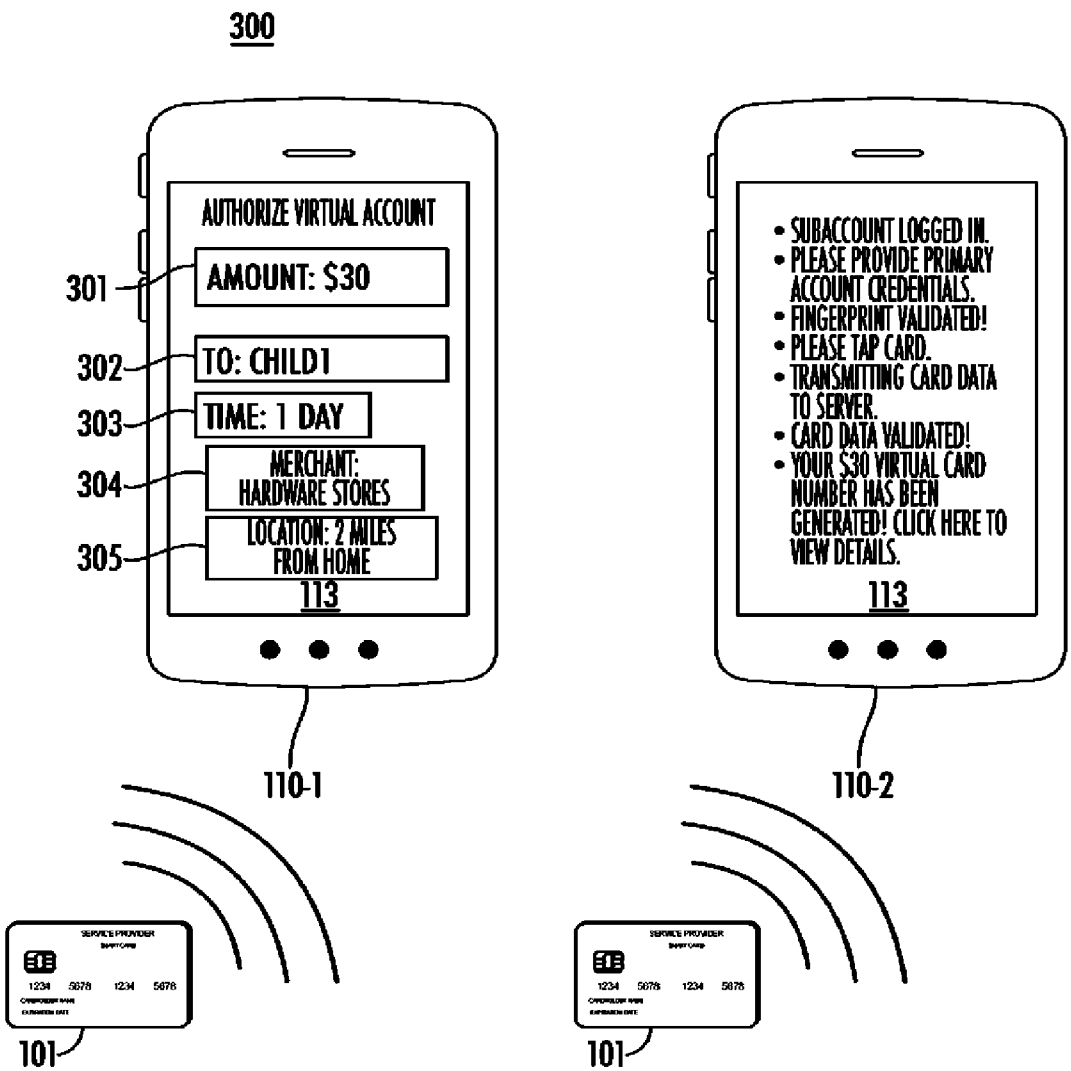
300
AUTHORIZE VIRTUAL ACCOUNT
AMOUNT: $30
TO: CHILD1
TIME: 1 DAY
MERCHANT: HARDWARE STORES
LOCATION: 2 MILES FROM HOME
113
301
302
303
304
305
110-1
101
• SUBACCOUNT LOGGED IN.
• PLEASE PROVIDE PRIMARY ACCOUNT CREDENTIALS.
• FINGERPRINT VALIDATED!
• PLEASE TAP CARD.
• TRANSMITTING CARD DATA TO SERVER.
• CARD DATA VALIDATED!
• YOUR $30 VIRTUAL CARD NUMBER HAS BEEN GENERATED! CLICK HERE TO VIEW DETAILS.
113
110-2
101

FIG. 3A

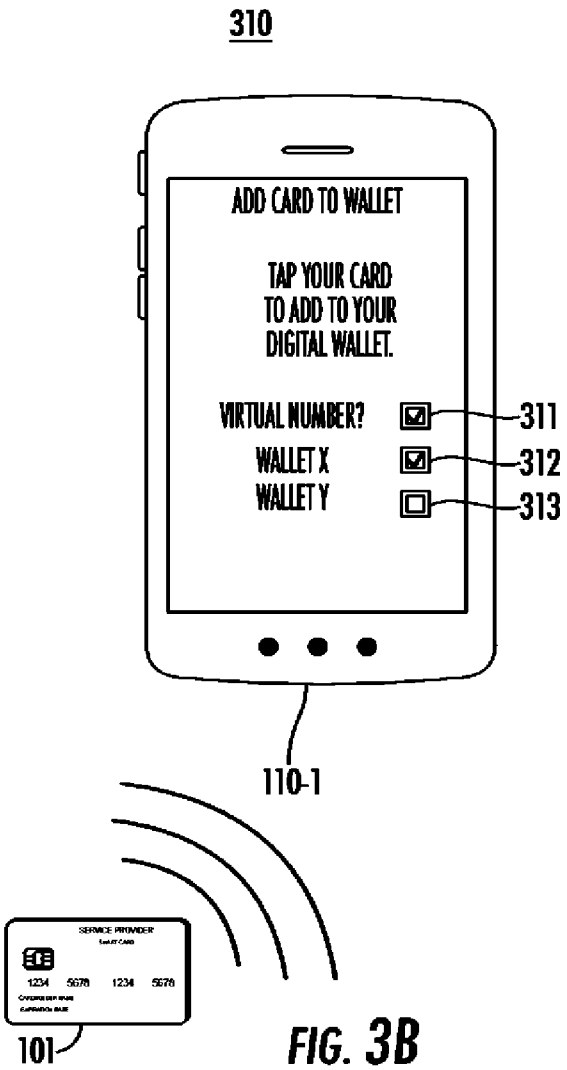
310
ADD CARD TO WALLET
TAP YOUR CARD TO ADD TO YOUR DIGITAL WALLET.
VIRTUAL NUMBER?
WALLET X
WALLET Y
311
312
313
110-1
SERVICE PROVIDER
1234 5678 1234 5678
101

FIG. 3B

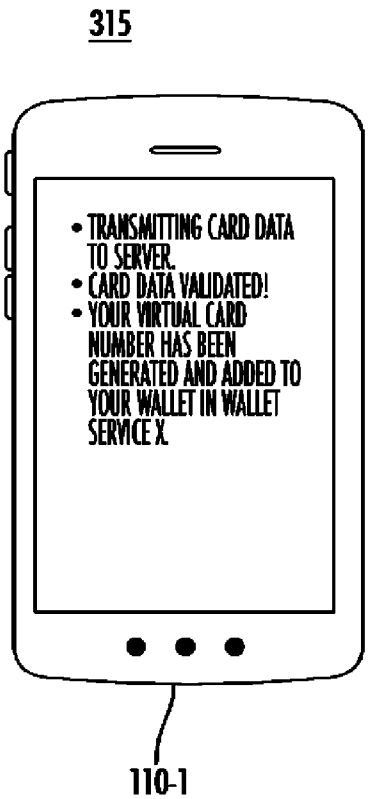
315
• TRANSMITTING CARD DATA TO SERVER.
• CARD DATA VALIDATED!
• YOUR VIRTUAL CARD NUMBER HAS BEEN GENERATED AND ADDED TO YOUR WALLET IN WALLET SERVICE X.
110-1

FIG. 3C

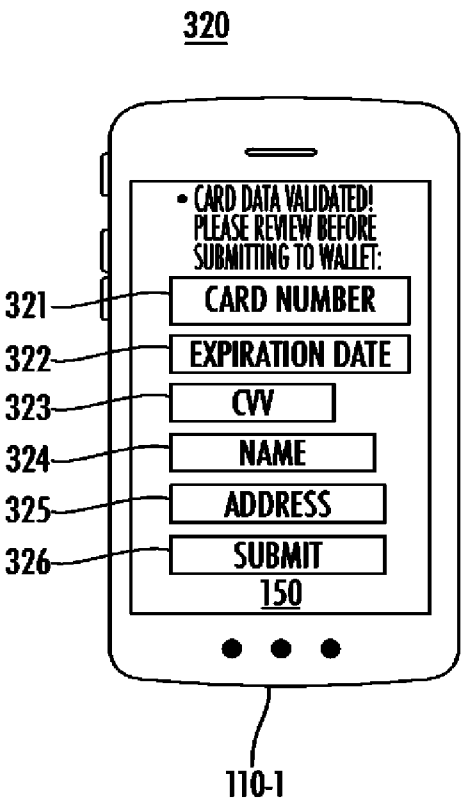
320
• CARD DATA VALIDATED! PLEASE REVIEW BEFORE SUBMITTING TO WALLET:
321
CARD NUMBER
322
EXPIRATION DATE
323
CVV
324
NAME
325
ADDRESS
326
SUBMIT
150
110-1

FIG. 3D

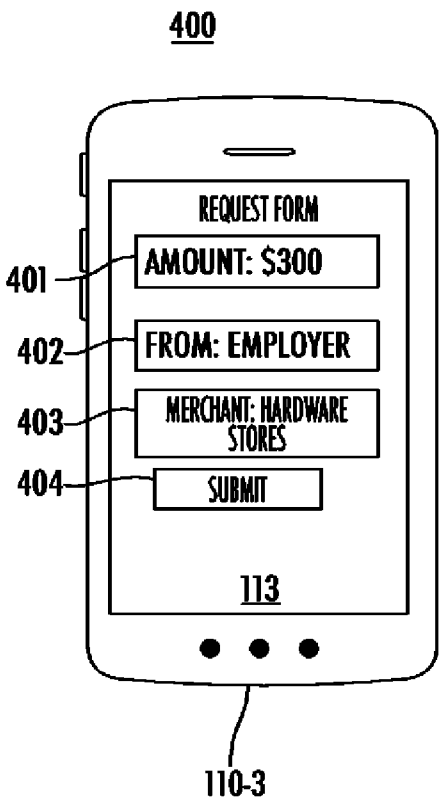
400
REQUEST FORM
AMOUNT: $300
FROM: EMPLOYER
MERCHANT: HARDWARE STORES
SUBMIT
113
401
402
403
404
110-3

FIG. 4

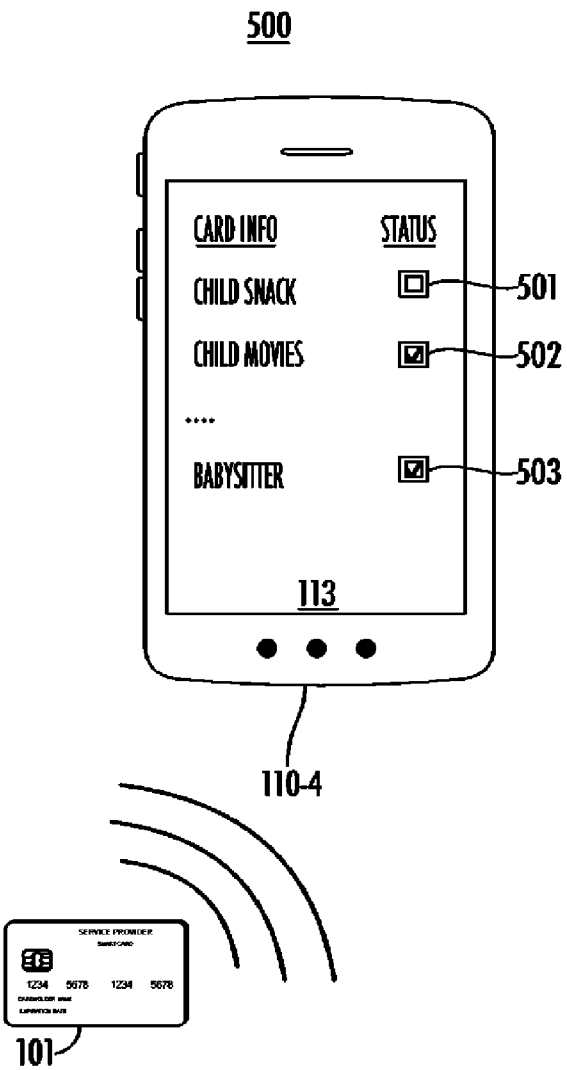
500
CARD INFO
STATUS
CHILD SNACK
CHILD MOVIES
....
BABYSITTER
113
501
502
503
110-4
101

FIG. 5

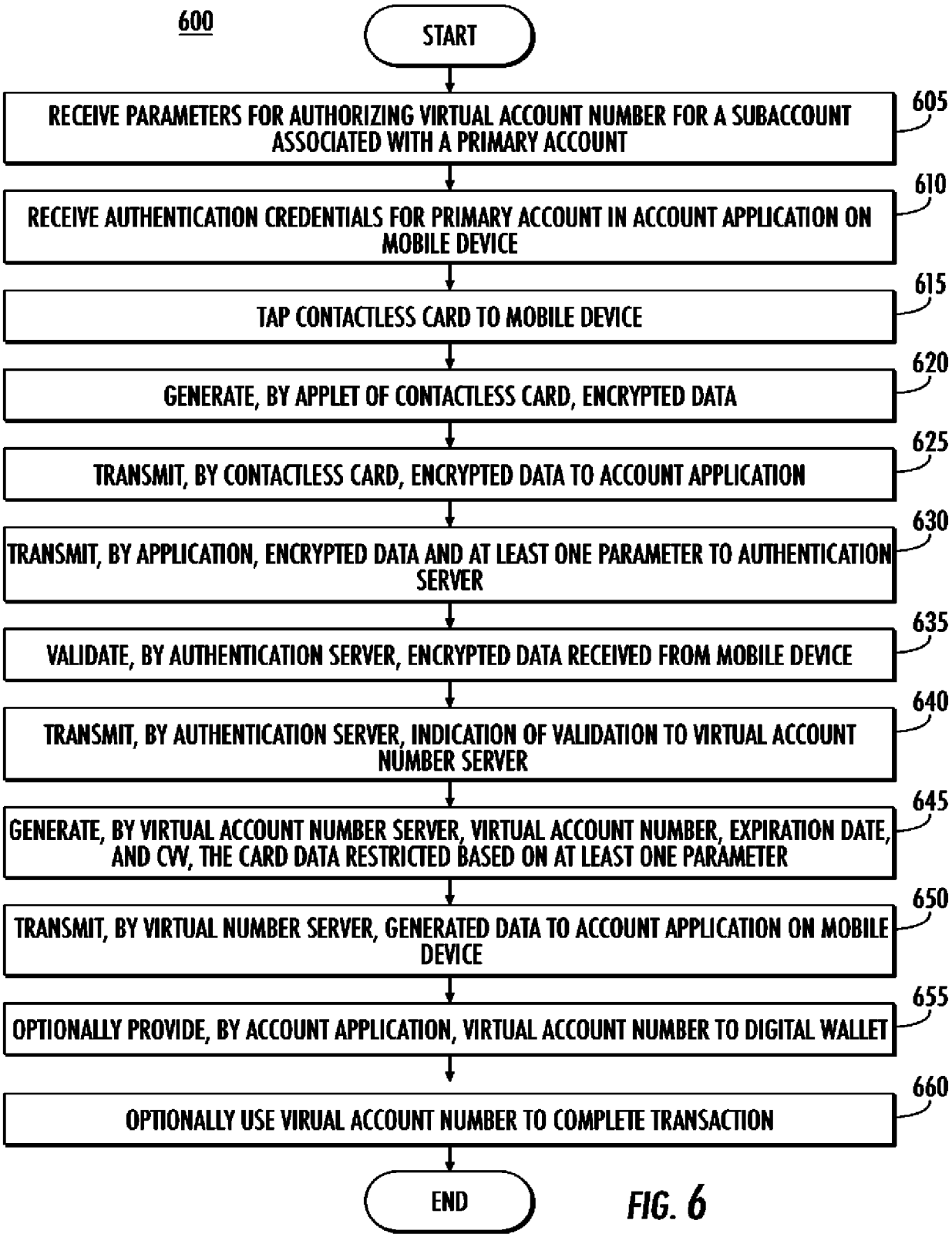
600
START
RECEIVE PARAMETERS FOR AUTHORIZING VIRTUAL ACCOUNT NUMBER FOR A SUBACCOUNT ASSOCIATED WITH A PRIMARY ACCOUNT
605
RECEIVE AUTHENTICATION CREDENTIALS FOR PRIMARY ACCOUNT IN ACCOUNT APPLICATION ON MOBILE DEVICE
610
TAP CONTACTLESS CARD TO MOBILE DEVICE
615
GENERATE, BY APPLET OF CONTACTLESS CARD, ENCRYPTED DATA
620
TRANSMIT, BY CONTACTLESS CARD, ENCRYPTED DATA TO ACCOUNT APPLICATION
625
TRANSMIT, BY APPLICATION, ENCRYPTED DATA AND AT LEAST ONE PARAMETER TO AUTHENTICATION SERVER
630
VALIDATE, BY AUTHENTICATION SERVER, ENCRYPTED DATA RECEIVED FROM MOBILE DEVICE
635
TRANSMIT, BY AUTHENTICATION SERVER, INDICATION OF VALIDATION TO VIRTUAL ACCOUNT NUMBER SERVER
640
GENERATE, BY VIRTUAL ACCOUNT NUMBER SERVER, VIRTUAL ACCOUNT NUMBER, EXPIRATION DATE, AND CVV, THE CARD DATA RESTRICTED BASED ON AT LEAST ONE PARAMETER
645
TRANSMIT, BY VIRTUAL NUMBER SERVER, GENERATED DATA TO ACCOUNT APPLICATION ON MOBILE DEVICE
650
OPTIONALLY PROVIDE, BY ACCOUNT APPLICATION, VIRTUAL ACCOUNT NUMBER TO DIGITAL WALLET
655
OPTIONALLY USE VIRUAL ACCOUNT NUMBER TO COMPLETE TRANSACTION
660
END

FIG. 6

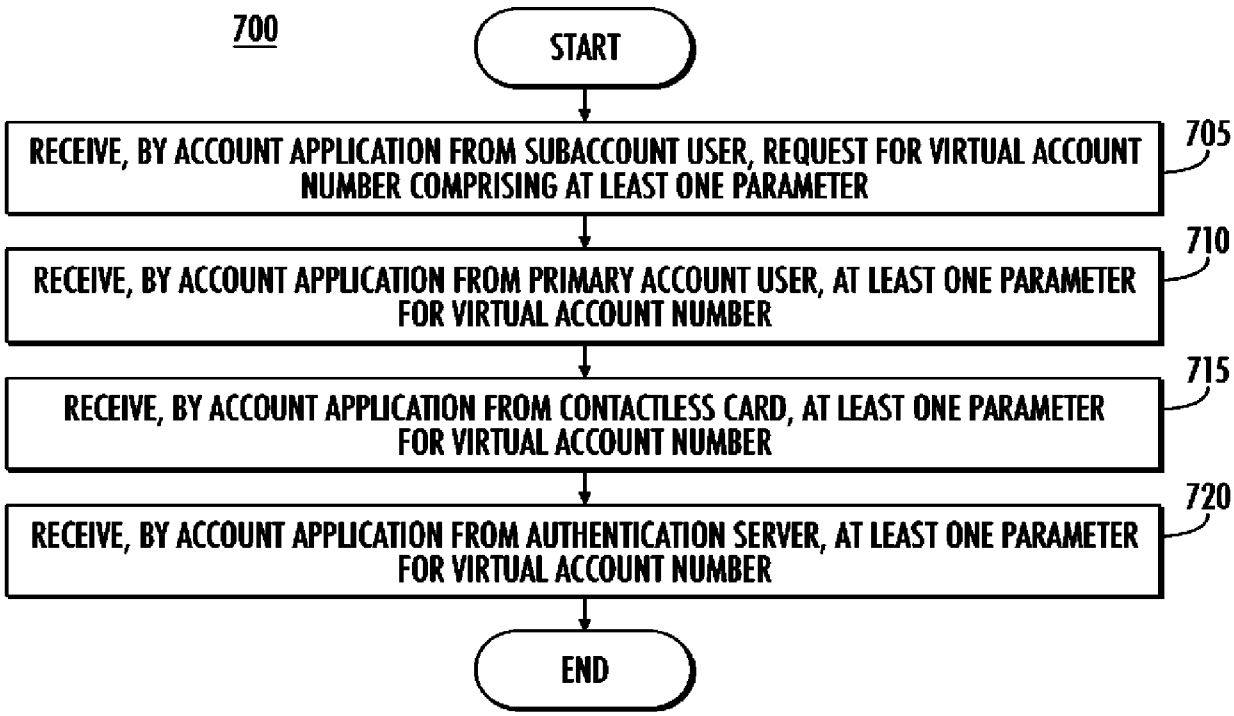
700
START
RECEIVE, BY ACCOUNT APPLICATION FROM SUBACCOUNT USER, REQUEST FOR VIRTUAL ACCOUNT NUMBER COMPRISING AT LEAST ONE PARAMETER
705
RECEIVE, BY ACCOUNT APPLICATION FROM PRIMARY ACCOUNT USER, AT LEAST ONE PARAMETER FOR VIRTUAL ACCOUNT NUMBER
710
RECEIVE, BY ACCOUNT APPLICATION FROM CONTACTLESS CARD, AT LEAST ONE PARAMETER FOR VIRTUAL ACCOUNT NUMBER
715
RECEIVE, BY ACCOUNT APPLICATION FROM AUTHENTICATION SERVER, AT LEAST ONE PARAMETER FOR VIRTUAL ACCOUNT NUMBER
720
END

FIG. 7

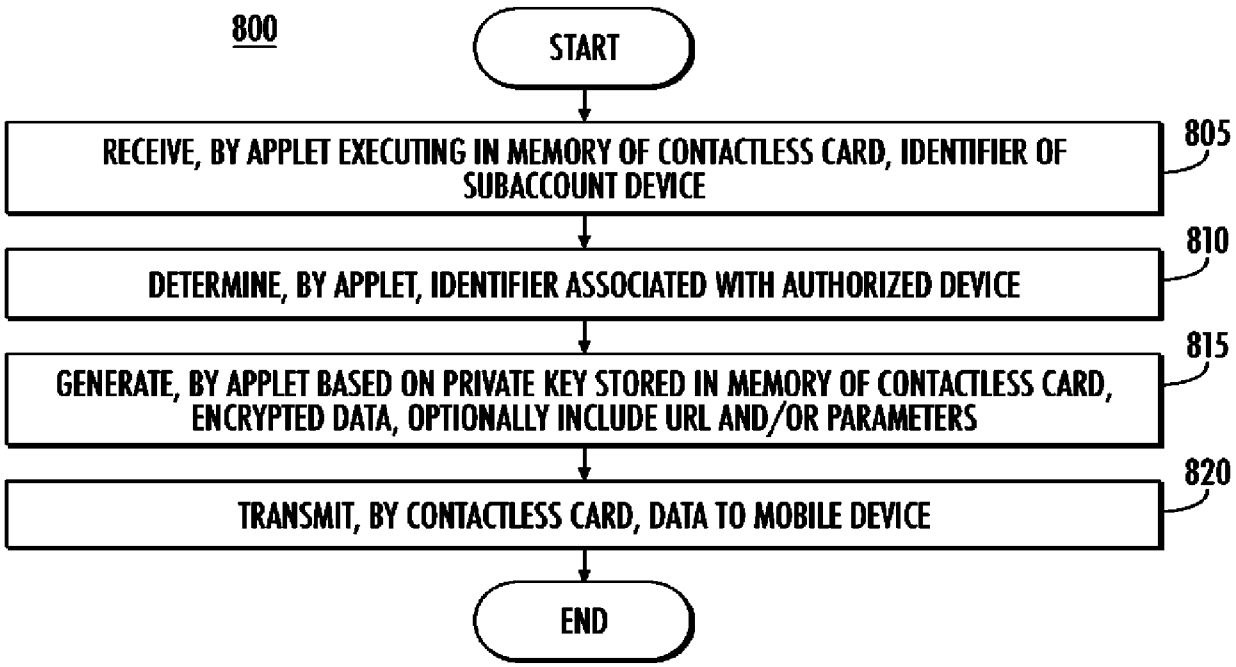
800
START
RECEIVE, BY APPLET EXECUTING IN MEMORY OF CONTACTLESS CARD, IDENTIFIER OF SUBACCOUNT DEVICE
805
DETERMINE, BY APPLET, IDENTIFIER ASSOCIATED WITH AUTHORIZED DEVICE
810
GENERATE, BY APPLET BASED ON PRIVATE KEY STORED IN MEMORY OF CONTACTLESS CARD, ENCRYPTED DATA, OPTIONALLY INCLUDE URL AND/OR PARAMETERS
815
TRANSMIT, BY CONTACTLESS CARD, DATA TO MOBILE DEVICE
820
END

FIG. 8

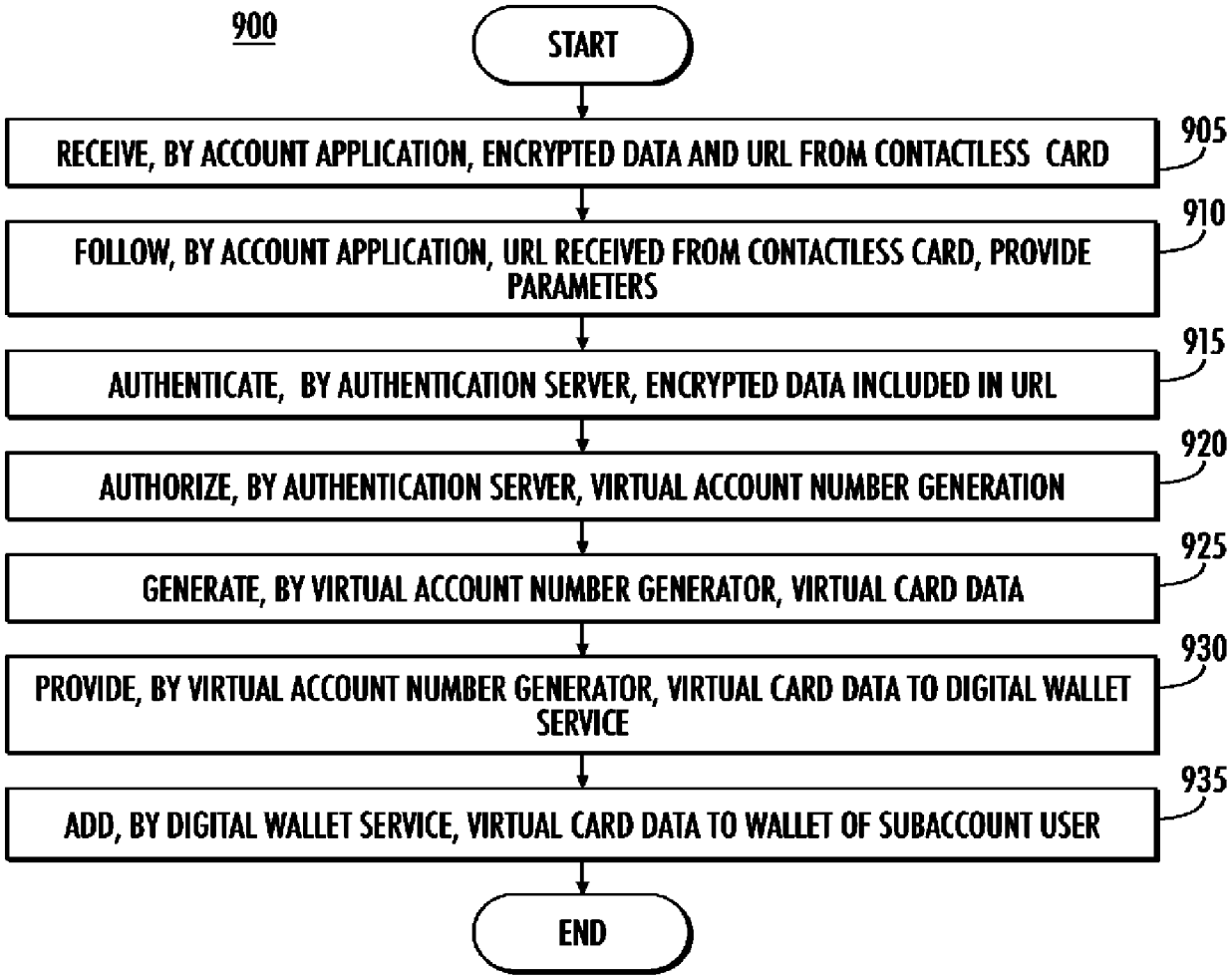
900
START
RECEIVE, BY ACCOUNT APPLICATION, ENCRYPTED DATA AND URL FROM CONTACTLESS CARD
905
FOLLOW, BY ACCOUNT APPLICATION, URL RECEIVED FROM CONTACTLESS CARD, PROVIDE PARAMETERS
910
AUTHENTICATE, BY AUTHENTICATION SERVER, ENCRYPTED DATA INCLUDED IN URL
915
AUTHORIZE, BY AUTHENTICATION SERVER, VIRTUAL ACCOUNT NUMBER GENERATION
920
GENERATE, BY VIRTUAL ACCOUNT NUMBER GENERATOR, VIRTUAL CARD DATA
925
PROVIDE, BY VIRTUAL ACCOUNT NUMBER GENERATOR, VIRTUAL CARD DATA TO DIGITAL WALLET SERVICE
930
ADD, BY DIGITAL WALLET SERVICE, VIRTUAL CARD DATA TO WALLET OF SUBACCOUNT USER
935
END

FIG. 9

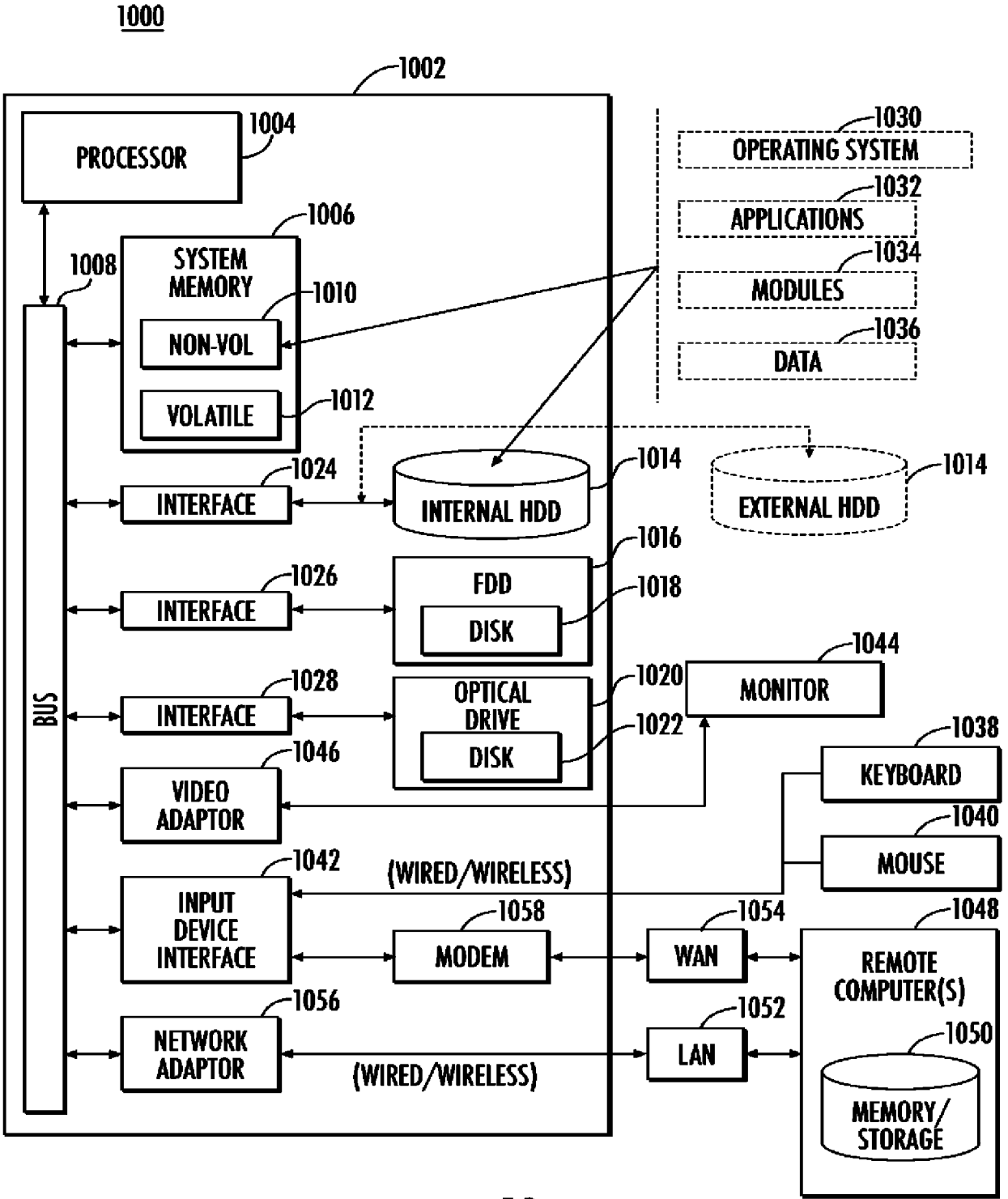
1000
1002
PROCESSOR
1004
SYSTEM MEMORY
1006
1008
1010
NON-VOL
VOLATILE
1012
BUS
1024
INTERFACE
INTERNAL HDD
1014
EXTERNAL HDD
1014
1026
INTERFACE
FDD
1016
DISK
1018
1028
INTERFACE
OPTICAL DRIVE
1020
DISK
1022
1046
VIDEO ADAPTOR
1042
INPUT DEVICE INTERFACE
(WIRED/WIRELESS)
1058
MODEM
1056
NETWORK ADAPTOR
(WIRED/WIRELESS)
1030
OPERATING SYSTEM
1032
APPLICATIONS
1034
MODULES
1036
DATA
1044
MONITOR
1038
KEYBOARD
1040
MOUSE
1054
WAN
1052
LAN
1048
REMOTE COMPUTER(S)
1050
MEMORY/ STORAGE

FIG. 10

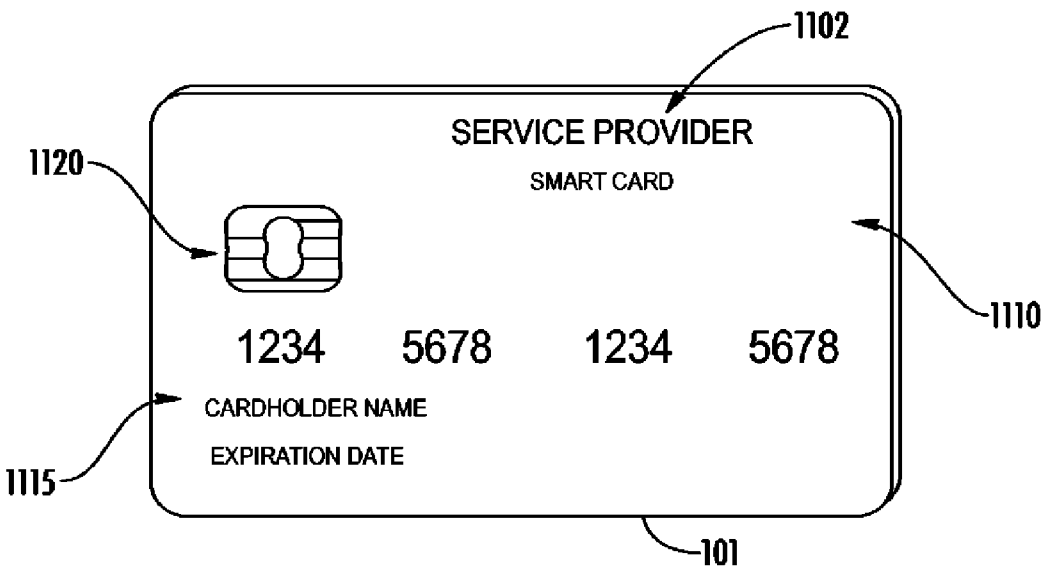
1102
SERVICE PROVIDER
SMART CARD
1120
1110
1234 5678 1234 5678
CARDHOLDER NAME
EXPIRATION DATE
1115
101

FIG. 11A

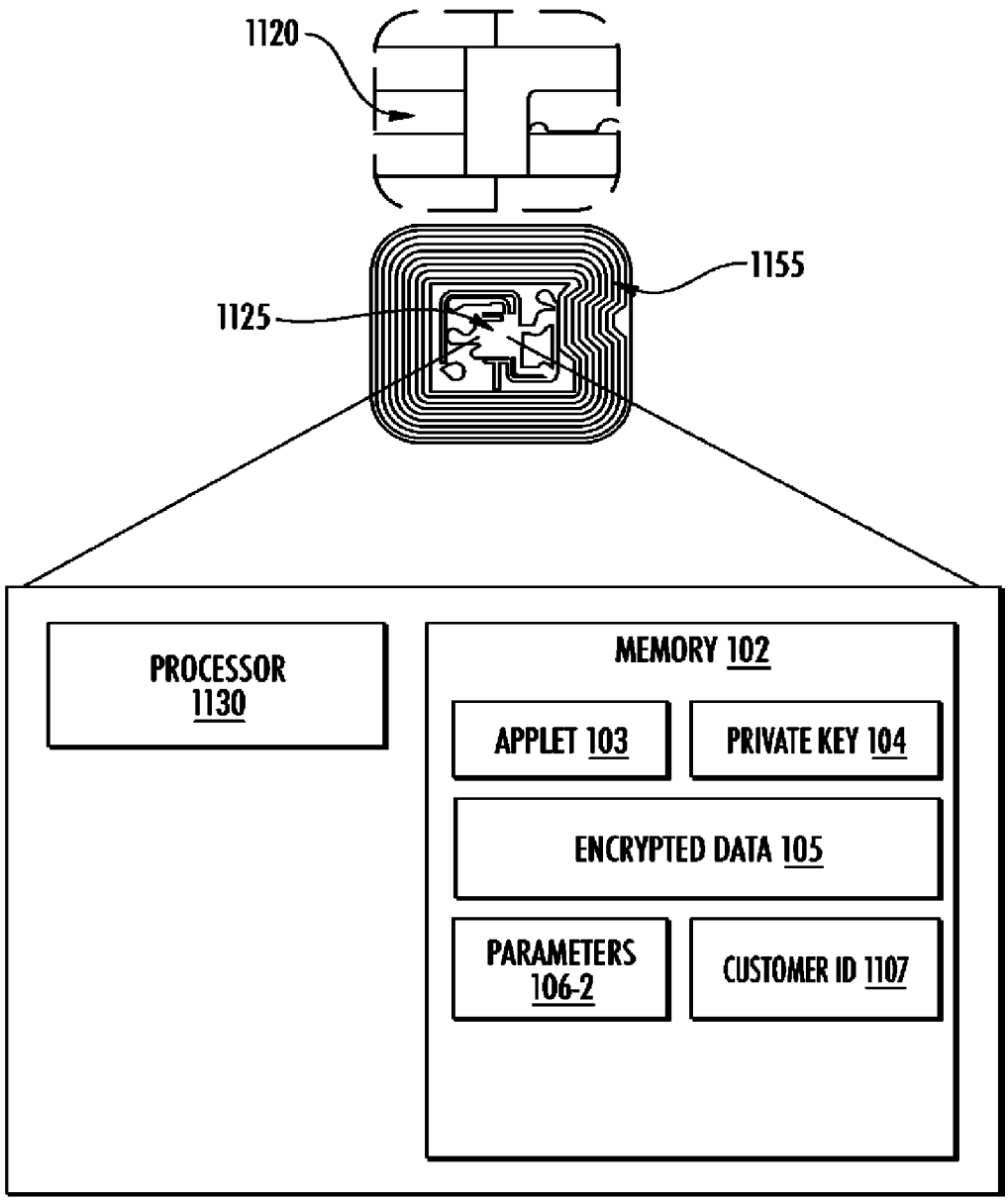
1120
1155
1125
PROCESSOR
1130
MEMORY 102
APPLET 103
PRIVATE KEY 104
ENCRYPTED DATA 105
PARAMETERS
106-2
CUSTOMER ID 1107

FIG. 11B

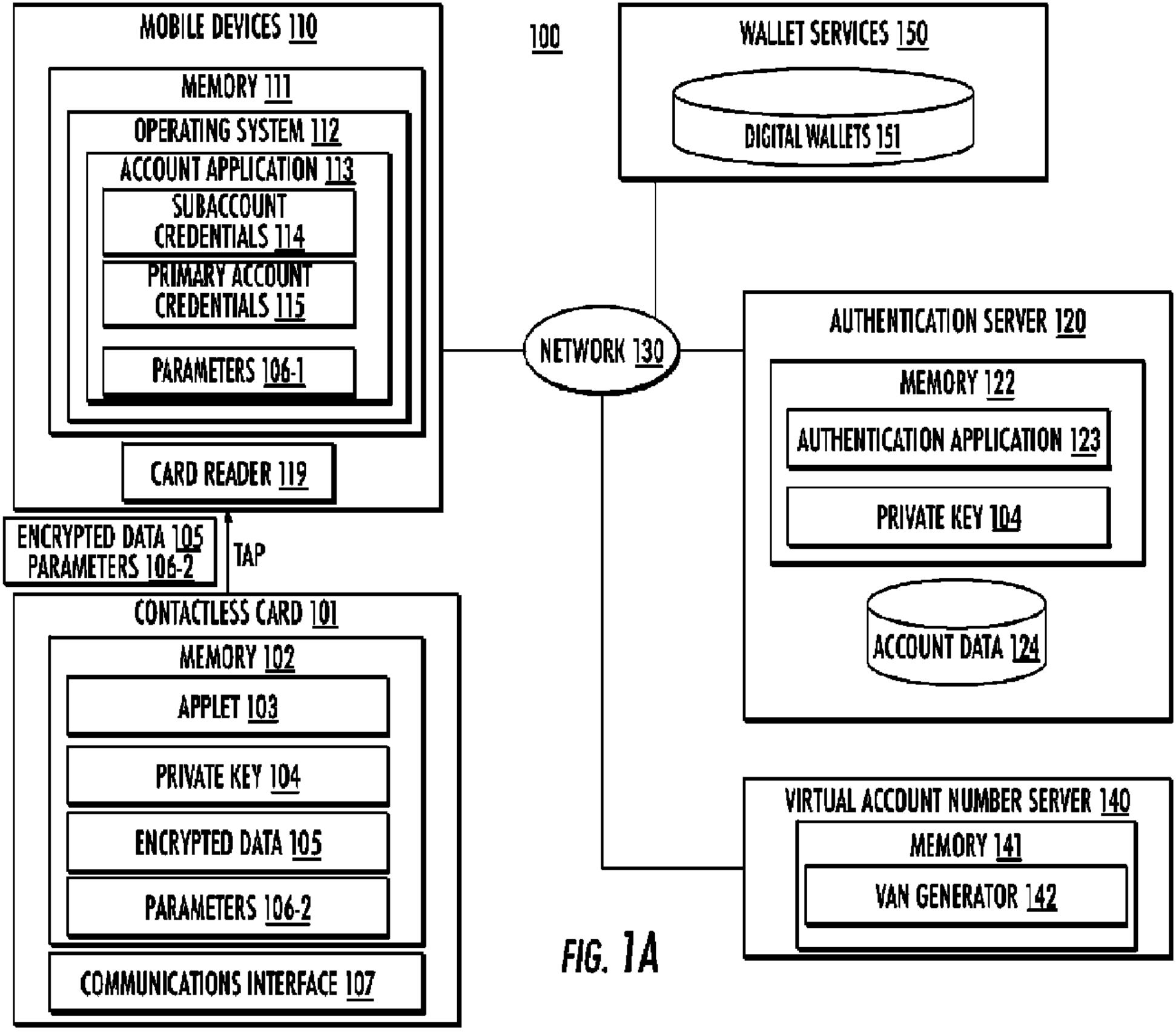
MOBILE DEVICES 110
100
WALLET SERVICES 150
MEMORY 111
DIGITAL WALLETS 151
OPERATING SYSTEM 112
ACCOUNT APPLICATION 113
SUBACCOUNT CREDENTIALS 114
PRIMARY ACCOUNT CREDENTIALS 115
PARAMETERS 106-1
NETWORK 130
AUTHENTICATION SERVER 120
MEMORY 122
AUTHENTICATION APPLICATION 123
PRIVATE KEY 104
CARD READER 119
ACCOUNT DATA 124
ENCRYPTED DATA 105
PARAMETERS 106-2
TAP
CONTACTLESS CARD 101
MEMORY 102
APPLET 103
PRIVATE KEY 104
ENCRYPTED DATA 105
PARAMETERS 106-2
VIRTUAL ACCOUNT NUMBER SERVER 140
MEMORY 141
VAN GENERATOR 142
COMMUNICATIONS INTERFACE 107

FIG. 1A