(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
07 January 2021 (07.01.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/003137 A1

(51) International Patent Classification:
G06Q 20/34 (2012.01) *G06Q 20/20* (2012.01)
G06Q 20/32 (2012.01) *G06Q 20/40* (2012.01)
G06Q 20/38 (2012.01)

(21) International Application Number:
PCT/US2020/040261

(22) International Filing Date:
30 June 2020 (30.06.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16/503,142 03 July 2019 (03.07.2019) US

(71) Applicant: **CAPITAL ONE SERVICES, LLC** [US/US]; 1680 Capital One Drive, McLean, Virginia 22102 (US).

(72) Inventors: **RULE, Jeffrey**; c/o Capital One Services, LLC, 1680 Capital One Drive, McLean, Virginia 22102 (US). **MORETON, Paul**; c/o Capital One Services, LLC, 1680 Capital One Drive, McLean, Virginia 22102 (US). **LUTZ, Wayne**; c/o Capital One Services, LLC, 1680 Capital One Drive, McLean, Virginia 22102 (US).

(74) Agent: **CARR, Nick** et al.; Kacvinsky Daisak Bluni, PLLC, 2601 Weston Parkway, Suite 103, Cary, North Carolina 27513 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,

(54) Title: CONSTRAINING TRANSACTIONAL CAPABILITIES FOR CONTACTLESS CARDS

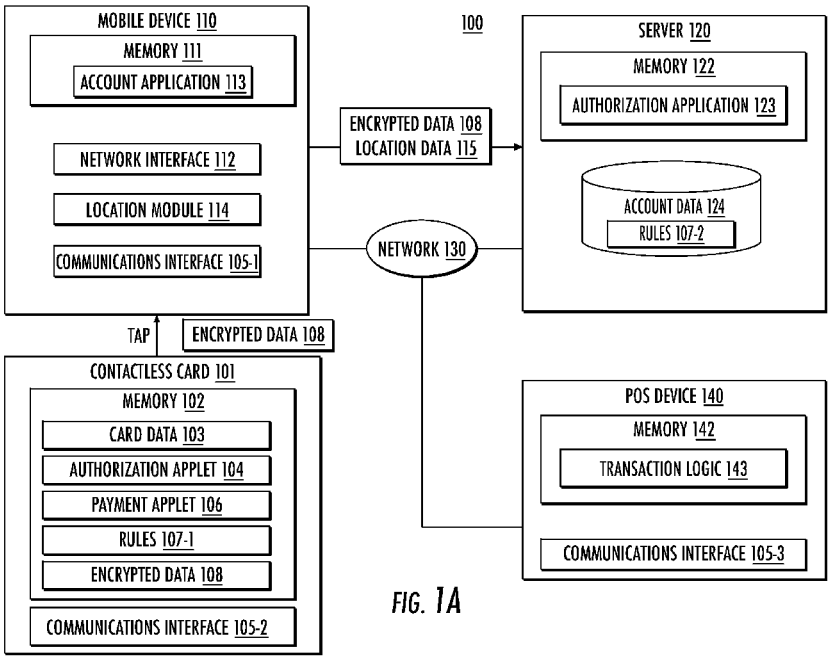


FIG. 1A

(57) **Abstract:** Systems, methods, articles of manufacture, and computer-readable media. A communications interface may receive an indication that a server preauthorized a transaction. The communications interface may receive, from a point of sale device, an indication to pay for the transaction. The contactless card may determine, based on rules stored in the memory, that the location of the mobile device is within one or more locations the contactless card is permitted for use. The contactless card may generate transaction data comprising: indications of an account number and an expiration date of the contactless card, and the indication of the preauthorization. The contactless card may transmit the transaction data to the POS device as payment for the transaction. The server may authorize payment for the transaction using at least a portion of the transaction data based at least in part on identifying the indication of the preauthorization in the transaction data.

WO 2021/003137 A1

[Continued on next page]

OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

CONSTRAINING TRANSACTIONAL CAPABILITIES FOR CONTACTLESS CARDS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Patent Application Serial No. 16/503,142, entitled "CONSTRAINING TRANSACTIONAL CAPABILITIES FOR CONTACTLESS CARDS" filed on July 3, 2019. The contents of the aforementioned patent application are incorporated herein by reference in their entirety.

TECHNICAL FIELD

[0002] Embodiments herein generally relate to contactless cards, and more specifically, to constraining transactional capabilities for contactless cards.

BACKGROUND

[0003] Cardholders (e.g., credit card holders, bank card holders, etc.) often obtain additional physical cards and/or virtual card numbers for trusted individuals, such as family members, employees, and the like. However, doing so may expose security risks. Conventional solutions do not provide the requisite security mechanisms to ensure that the physical cards and/or virtual card numbers are used in accordance with any defined restrictions.

SUMMARY

[0004] Embodiments disclosed herein provide systems, methods, articles of manufacture, and computer-readable media for constraining transactional capabilities of contactless cards. In one example, a communications interface may receive, from a mobile device executing an account application, an indication that a server preauthorized a transaction based on location data describing a location of the mobile device and verification of encrypted data, the encrypted data generated by the contactless card using a cryptographic algorithm and a private key stored in the memory of the contactless card, one or more credentials for an account associated with the contactless card received by the account application. The communications interface may receive, from a point of sale (POS) device, an indication to pay for the transaction using the contactless card. The contactless card may determine, based on one or more rules stored in the memory, that the location of the mobile device is within a threshold distance of one or more locations the contactless card is permitted for use. The contactless card may generate transaction data comprising: (i) indications of an account number and an expiration date of the contactless card, and (ii) the indication of the preauthorization of the transaction by the server. The contactless card may transmit the transaction data to the POS device as payment for the transaction, the server to authorize payment for the transaction using at least a portion of the transaction data based at least in part on identifying the indication of the preauthorization of the transaction by the server in the transaction data.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] Figures 1A-1D illustrate embodiments of a system to constrain transactional capabilities for contactless cards.

[0006] Figures 2A-2B illustrate embodiments of constraining transactional capabilities for contactless cards.

[0007] Figures 3A-3D illustrate embodiments of constraining transactional capabilities for contactless cards.

[0008] Figure 4 illustrates an embodiment of a first logic flow.

[0009] Figure 5 illustrates an embodiment of a second logic flow.

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

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

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

[0013] Figure 9 illustrates an embodiment of a computing architecture.

[0014] Figures 10A-10B illustrate an example contactless card.

DETAILED DESCRIPTION

[0015] Embodiments disclosed herein provide secure techniques to constrain transactional capabilities of contactless cards. Generally, a contactless card may be programmed to include

restrictions on the use of the contactless card. The restrictions may include geographic (or location) restrictions, amount restrictions, and/or time restrictions. When the cardholder attempts to use the contactless card, logic in the contactless card may determine if the attempted use is permitted in light of the restrictions. For example, the contactless card may periodically communicate with a mobile device executing an account management application. The contactless card may periodically receive location data from the account management application, where the location data describes a location of the mobile device (and/or the contactless card). When the cardholder attempts to use the contactless card, the logic in the contactless card may determine whether the received location data is within one or more geographic locations the contactless card is permitted for use. For example, the contactless card may be limited to use in a 5-mile radius from a cardholder's home. If the received location data indicates the mobile device and/or the contactless card are 10 miles away from the home, the contactless card may decline to process the attempted transaction. Similarly, if the location data indicates the mobile device and/or the contactless card are 1 mile away from the home, the contactless card may permit the attempted transaction.

[0016] In some embodiments, the location data may be used as part of a preauthorization process for transactions. For example, the user may tap their contactless card to the mobile device executing the account application to preauthorize a large transaction while shopping for an expensive item, such as a watch. The account application may receive encrypted data generated by the contactless card. The account application may transmit the encrypted data and location data describing the current location of the mobile device to a server. The server may decrypt the encrypted data, thereby validating the encrypted data. The server may further determine that the location data indicates the mobile device and/or the contactless card are within one or more locations the contactless card is permitted for use. Similarly, the server may verify any requested purchase amount and/or time duration for the preauthorization. The server may determine to preauthorize a transaction using the contactless card and transmit an indication of the preauthorization to the account application executing on the mobile device. The indication of preauthorization may be transmitted from the mobile device to the contactless card. When the contactless card determines that the card is being used to pay for a transaction, the contactless card may write the indication of preauthorization to one or more fields of a payment payload that is transmitted to a point of sale (POS) device. The POS device may transmit the payment payload including the indication of preauthorization to the server. The server may authorize payment for the transaction based at least in part on identifying the indication of preauthorization in the payment payload. The server may further verify any data received from the mobile device responsive to a tap of the contactless card at the time of attempted purchase (e.g., requested purchase amount, time, location, etc.). The server may then transmit an indication of the authorization to the POS device.

[0017] Advantageously, embodiments disclosed herein improve the security of all devices and associated data. For example, the preauthorization technique may reduce fraud and/or security risks for the contactless card. As another example, the validation performed by the server provides safeguards to ensure that an authorized user has access to the physical card. Further still, by enforcing rules associated with the use of the physical card and/or virtual account number, the security of the associated account 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 mobile devices 110, a server 120, and one or more point of sale devices 140. 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 105-2, such as a radio frequency identification (RFID) chip, configured to communicate with the communications interface 105-1 of the mobile 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 mobile 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, and the like. The server 120 is representative of any type of computing device, such as a server, workstation, compute cluster, cloud computing platform, virtualized computing system, and the like. The POS devices 140 are representative of any type of device for processing payments, such as card reader devices, smartphones, tablet computers, desktop computers, POS terminals, servers, workstations, laptop computers, and the like.

[0022] As shown, a memory 111 of the mobile device 110 includes an instance of 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, defining restrictions on contactless card 101, communicating location data to the contactless card 101, and communicating with the server 120 for preauthorization. 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. In some embodiments, the user may perform additional authentication (e.g., multi-factor authentication) in addition to providing the authentication credentials. For example, the user may provide, to the account application 113, a one-time passcode received in a text message, the biometric credentials associated with the account, and/or a temporary code generated by an authentication application (not pictured). In some embodiments, the contactless card 101 may generate and transmit encrypted data 108 that is used as an additional

authentication factor. In some embodiments, the account application 113 may transmit an indication to the contactless card 101 specifying that the user has been authenticated using the authentication credentials.

[0023] When the user is authenticated into their account in the account application 113, the account application 113 may receive location data from the location module 114. The location data may generally describe the location of the mobile device 110. The location module 114 may be any device which determines location, such as a global positioning system (GPS) module, Global Navigation Satellite System (GNSS) module, a Galileo module, etc. In some embodiments, the network interface 112 may provide location data that describes the location of the mobile device (e.g., based on cellular network signals, tower locations, etc.). The account application 113 may periodically provide the location data generated to the contactless card 101 via the communications interfaces 105-1, 105-2. As described in greater detail below, the contactless card 101 may use the location data to restrict the transactional capabilities of the contactless card 101. For example, the rules 107-1 of the contactless card 101 may specify one or more locations the contactless card 101 may be used to pay for transactions. If the received location data is not within the one or more locations specified in the rules 107-1 (and/or within a threshold distance of the one or more locations) the contactless card 101 may refrain from generating data and/or transmitting data to the POS device 140 to pay for a transaction.

[0024] In one embodiment, a user may wish to obtain preauthorization for a purchase using the contactless card 101. For example, the user may wish to purchase an expensive item of jewelry using the contactless card 101 while at a jewelry store. To receive preauthorization, the user may generally unlock their mobile device 110 and authenticate in the account application 113. When the user authenticates in the account application 113, the user may access a preauthorization page of the account application 113. In some embodiments, the preauthorization page may be part of a separate application rather a page of the account application 113. In response, the account application 113 may output a notification on the mobile device 110 specifying to tap the contactless card 101 to the mobile device 110, thereby bringing the contactless card 101 sufficiently close to the communications interface 105-1 of the mobile device 110 to enable data transfer (e.g., NFC data transfer, Bluetooth data transfer, etc.) between the communications interface 105-2 of the contactless card 101 and the communications interface 105-1 of the mobile device 110. The authorization applet 104 executing on a processor (not pictured) of the contactless card 101 may then generate and transmit encrypted data 108 to the mobile device 110 via the communications interface 107. The authorization applet 104 of the contactless card 101 may use a cryptographic algorithm to generate a cryptographic payload of encrypted data 108 based at least in part on a private key stored in the memory 102 of the contactless card 101. In such an embodiment, the private key 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 108. Generally, the authorization applet 104 may use any type of cryptographic algorithm and/or system to generate the encrypted data 108, and the use of a specific cryptographic algorithm as an example herein should not be considered limiting of the disclosure. In some embodiments, the authorization applet 104 may perform encryption using a key diversification technique to generate the encrypted data 108. Examples of key diversification techniques are described in United States Patent Application 16/205,119, filed November 29, 2018. The aforementioned patent application is incorporated by reference herein in its entirety. In one embodiment, the authorization applet 104 generates the encrypted data 108 based at least in part on an indication received from the account application 113 specifying that the user has been authenticated into their account using account credentials.

[0025] In some such embodiments, the authorization applet 104 determines whether the most recently received location data is within one or more locations specified in the rules 107-1 as permitted locations to use the contactless card 101. If the location data is within the one or more locations specified in the rules 107-1, the authorization applet 104 may generate the encrypted data 108. If the location data is not within the one or more locations specified in the rules 107-1, to

preserve security, the authorization applet 104 may refrain from generating the encrypted data 108. Furthermore, the authorization applet 104 may apply other rules in the rules 107-1 when determining whether to generate the encrypted data 108. For example, the rules 107-1 may specify a time when the contactless card 101 can be used (e.g., during the hours of 8 AM - 5 PM on weekdays, within 1 year of issuance, etc.). As another example, the rules 107-1 may specify an amount limit for any transaction (or multiple transactions) using the contactless card 101. If the current time is not within the time specified in the rules 107-1, the authorization applet 104 may refrain from generating the encrypted data 108. Similarly, if the user provides a dollar amount for the preauthorization to the account application 113 (which may be transmitted to the contactless card 101) exceeds the dollar amount limit specified in the rules 107-1, the authorization applet 104 may refrain from generating the encrypted data 108.

[0026] Once generated, the authorization applet 104 may transmit the encrypted data 108 to the account application 113 of the mobile device 110, e.g., via NFC. For example, the authorization applet 104 may transmit the encrypted data 108 in an NDEF tag that specifies to an operating system (OS, not pictured) of the mobile device 110 to launch the account application 113 to receive the encrypted data 108. More generally, when communicating with the mobile device 110, data generated by the contactless card 101 may specify to launch the account application 113 (e.g., via an intent attribute). The OS may detect the NFC signal from the contactless card 101, read the data transmitted by the contactless card 101, and launch the account application 113.

[0027] The account application 113 may transmit the encrypted data 108 and the location data 115 generated by the location module 114 to the authorization application 123 of the server 120. The account application 113 may further transmit other data to the server 120, such as the requested amount for preauthorization. The authorization application 123 may attempt to authenticate the received encrypted data 108. For example, the authorization application 123 may attempt to decrypt the encrypted data 108 using a copy of the private key stored in the memory 122 of the server 120. The private key may be identical to the private key stored in the memory 102 of the contactless card 101, where each contactless card 101 is manufactured to include a unique private key (and the server 120 stores a corresponding copy of each unique private key). Therefore, the authorization application 123 may successfully decrypt the encrypted data 108, thereby verifying the encrypted data 108. Although the private key is stated as being stored in the memory 122, the private key 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 108 using the private key and a cryptographic function.

[0028] For example, as stated, the customer identifier associated with the contactless card 101 may be used to generate the encrypted data 108. In such an example, the authorization application 123 may decrypt the encrypted data 108 using the private key of the server 120. If the result of the decryption yields the customer identifier associated with the account in the account data 124, the authorization application 123 verifies the encrypted data 108. If the authorization application 123 is unable to decrypt the encrypted data to yield the expected result (e.g., the customer identifier of the account associated with the contactless card 101), the authorization application 123 does not validate the encrypted data 108. Due to the failed verification, the authorization application 123 may not preauthorize the requested transaction.

[0029] More generally, as part of the preauthorization process, the authorization application 123 may determine whether the location data 115 is within one or more locations specified in the rules 107-2 of the account data 124 for the account as permitted locations to use the contactless card 101. If the location data is within the one or more locations specified in the rules 107-2, the authorization application 123 preauthorize the transaction. If the location data is not within the one or more locations specified in the rules 107-1, to preserve security, the authorization application 123 may refrain from preauthorizing the transaction. Similarly, if a time restriction for using the contactless card 101 in the rules 107-2 is not satisfied by a time associated with the preauthorization request, the authorization application 123 may refrain from preauthorizing the

transaction. Further still, if a transaction amount restriction is not satisfied by the amount associated with the preauthorization request, the authorization application 123 may refrain from preauthorizing the transaction.

[0030] In some embodiments, the authorization application 123 may return a binary indication of preauthorization (e.g., preauthorized and/or not preauthorized) as a preauthorization result. In other embodiments, the authorization application 123 may select a preauthorization level from one or more preauthorization levels as a preauthorization result. For example, the highest level of preauthorization may be selected when the authorization application 123 successfully decrypts the encrypted data 108 and determines that the preauthorization request complies with the restrictions in the rules 107-2. As another example, the second level of preauthorization, less than the highest level of preauthorization, may be selected if the authorization application 123 successfully decrypts the encrypted data 108 and determines that the preauthorization request does not comply with at least one of the restrictions in the rules 107-2. As another example, the third level of preauthorization, less than the highest level of preauthorization, may be selected if the authorization application 123 does not successfully decrypt the encrypted data 108 a and determines that the preauthorization request complies with the restrictions in the rules 107-2. As another example, the lowest level of preauthorization, lower than the highest, second, and third levels of preauthorization, may be selected when the authorization application 123 does not successfully decrypt the encrypted data 108 and determines that the preauthorization request does not comply with at least one of the restrictions in the rules 107-2. Regardless of the type of preauthorization result, in some embodiments, the authorization application 123 may perform additional fraud vector analyses and preauthorize and/or decline to preauthorize the transaction based on the additional analyses.

[0031] As shown in Figure 1B, once the authorization application 123 validates the encrypted data 108 and determines a preauthorization result, the authorization application 123 transmits an indication of the preauthorization 132 to the mobile device 110. The preauthorization result 132 may include an associated timestamp, the received location data 115, the preapproval amount, and any other attribute as metadata. The authorization application 123 may further store the preauthorization result 132 in the account data 124 for the account associated with the contactless card. Once received, the account application 113 may output an indication specifying to tap the contactless card 101 to the mobile device 110. Once tapped, the account application 113 may transmit the indication of preauthorization 132 to the authorization applet 104 of the contactless card 101. In some embodiments, the account application 113 transmits the indication of preauthorization 132 received from the server 120 to the authorization applet 104 of the contactless card 101. In other embodiments, the account application 113 transmits a different indication of preauthorization 132 to the authorization applet 104 of the contactless card 101. The authorization applet 104 may then store the received indication of preauthorization 132 in the memory 102 of the contactless card.

[0032] When the user attempts to make a purchase, the user may bring the contactless card 101 in communications range of the communications interface 105-3 of a POS device 140. For example, the user may tap the contactless card 101 to the POS device 140 to communicate wirelessly and/or insert the contactless card into a card reader communications interface 105-3 of the POS device 140. The transaction logic 144 in the memory 142 of the POS device 140 may then transmit transaction data 145 to the contactless card 101. The transaction data 145 may include an amount value for the transaction, a merchant identifier, location data of the POS device 140, a timestamp, and the like. For example, the transaction data 145 may specify that the user is attempting to purchase a $1,000 ring, include a merchant identifier of the jeweler, and location data for the POS device 140 and/or the jeweler. The payment applet 106 may receive the transaction data 145 and request approval from the authorization applet 104 to provide the card data 103 as payment for the transaction.

[0033] To determine whether to approve the transaction, the authorization applet 104 may determine whether the rules 107-1 are satisfied by the transaction data 145 and/or the location data

received from the mobile device 110 at periodic intervals. For example, if the $1,000 amount of the transaction exceeds a maximum spending amount in the rules 107-1, the authorization applet 104 may decline the approval requested by the payment applet 106. As another example, if the location data received from the mobile device 110 (or the location data in the transaction data 145) is outside the locations specified in the rules 107-1, the authorization applet 104 may decline the approval requested by the payment applet 106. Further still, the authorization applet 104 may determine whether the preauthorization 132 has been received for the transaction. If the preauthorization 132 has been received, the authorization applet 104 may decline the approval requested by the payment applet 106. In some embodiments, the authorization applet 104 determines whether a difference of the timestamp in the transaction data 145 and the timestamp of the preauthorization 132 exceeds a time threshold specified in the rules 107-1. If the difference exceeds the time threshold, the authorization applet 104 may decline the approval requested by the payment applet 106.

[0034] If, however, the authorization applet 104 determines all rules 107-1 are satisfied and/or determines the preauthorization 132 has been received from the server 120, the authorization applet 104 may provide the approval requested by the payment applet 106. Figure 1C depicts an embodiment where the authorization applet 104 provides the approval requested by the payment applet 106 to the payment applet 106. In response, the payment applet 106 may generate transaction data 109 comprising the card data 103 and an indication of the preauthorization 132. The card data 103 may include a card number (or an account number), an expiration date, and/or card verification value (CVV). In some embodiments, the transaction data 109 is an EMV payload. In such embodiments, the card data 103 is inserted into one or more corresponding fields of the EMV payload, and the indication of the preauthorization 132 is stored in one or more other fields of the EMV payload. For example, the card number may be stored in tag (or field) 5A of an EMV payload and the expiration date may be stored in tag 59 of the EMV payload. In some embodiments, the CVV is not included in the EMV payload. In other embodiments, the CVV is included in one or more other tags of the EMV payload. The indication of preauthorization may be stored in any other tag of the EMV payload, such as discretionary data fields and/or padding data fields of an EMV payload.

[0035] Figure 1D illustrates an embodiment where the transaction logic 144 of the POS device 140 transmits transaction data 150 to the server 120 via the network 130 to request approval for the requested transaction. As shown, the transaction data 150 may include the card data 103, the preauthorization 132, location data 132 describing a location of the POS device, and the transaction data 145. In at least one embodiment, the transaction data 150 includes the EMV payload generated by the payment applet 106, which includes the card data 103 and the indication of preauthorization 132 in the respective one or more fields of the EMV payload. In some embodiments, the mobile device 110 may transmit at least a portion of the transaction data 150 to the server 120, e.g., requested purchase amount, location of the mobile device 110, etc.) as part of the request for approval of the transaction.

[0036] Once received, the authorization application 123 may process the transaction data 150 to determine whether to approve and/or reject the transaction. Generally, the authorization application 123 may attempt to identify the indication of preauthorization 132 in the transaction data 150. If the authorization application 123 identifies the indication of preauthorization 132, the authorization application 123 may compare the received indication of preauthorization 132 (or any attribute thereof) to the indication of preauthorization 132 (or any attribute thereof) stored in the account data 124 for the account associated with the contactless card 101. If the authorization application 123 determines that a matching indication of preauthorization 132 exists in the account data 124 for the account associated with the contactless card 101, the authorization application 123 may approve the transaction, as the preauthorization 132 at least in part reflects the prior validation of the encrypted data 108. If the authorization application 123 determines that a matching indication of preauthorization 132 does not exist in the account data 124 for the account associated with the contactless card 101, the authorization application 123 may decline the transaction. In

some embodiments, the authorization application 123 may determine whether the location of the POS device 140 is within a threshold distance of the location data 115 stored as an attribute of the preauthorization 132 in the account data 124. If the location of the POS device 140 is not within the threshold distance of the location data 115, the authorization application 123 may reject the transaction and/or require further processing of the transaction prior to approving the transaction.

[0037] In other embodiments, the authorization application 123 may perform additional processing prior to approving and/or declining the transaction. For example, the authorization application 123 may determine whether the transaction amount exceeds any account limits and/or rules 107-2. Similarly, the authorization application 123 may determine whether the time of the transaction is within any time restrictions for using the contactless card 101 in the rules 107-2. Similarly, the authorization application 123 may determine whether the location data of the POS device 140 is within the locations specified in the rules 107-2. In some embodiments, the authorization application 123 may not receive location data from the POS device 140. In such embodiments, the authorization application 123 may determine the location of the POS device 140 based on the merchant identifier and a location associated with the merchant identifier specified in the entry for the merchant in the account data 124. The authorization application 123 may then determine whether the location is within the locations specified in the rules 107-2. Furthermore, the authorization application 123 may perform additional fraud analysis to determine whether to approve the transaction. The authorization application 123 may then transmit an indication of approval and/or denial of the transaction to the POS device 140. The POS device 140 may then transmit an indication of the approval and/or the denial of the transaction to the contactless card 101. Furthermore, the authorization application 123 may transmit indications of additional details related to the approval and/or denial of the transaction to the POS device 140 (e.g., results of any processing performed by the authorization application 123 for the transaction, such as location analysis, analysis based on the rules 107-2, etc.). The POS device 140 may then transmit the received indications to the contactless card 101.

[0038] Figure 2A is a schematic 200 depicting an example embodiment of using the account application 113 on the mobile device 110 to define rules for using a contactless card 101. As shown, the account application 113 outputs a form including fields 201-204, where field 201 corresponds to an amount field, field 202 corresponds to a location field, field 203 corresponds to a time field, and field 204 corresponds to a merchant category field. As shown, the user has provided example values of $300 in the amount field 201, 10 miles from an office in the location field 202, 10 days in the time field 203, and hardware stores in the merchant field 204. Therefore, by providing the values in the fields 201-204, the user specifies that the contactless card 101 can be used to spend up to $300 for 10 days within 10 miles of the office at hardware stores.

[0039] Figure 2B is a schematic 210 illustrating an embodiment where the user submits the values in the fields 201-203. As shown, the account application 113 may output an indication to tap the contactless card 101 to the mobile device 110. Doing so may cause the authorization applet 104 to generate encrypted data 108. The account application 113 may transmit the encrypted data 108 and values from the fields 201-204 (or indications thereof) to the server 120, which may validate the encrypted data 108 and store the received values (or indications thereof) in the rules 107-2 for the corresponding account in the account data. The server 120 may then transmit an indication of the validation of the encrypted data 108 to the account application 113, which may output another indication to tap the contactless card 101 to the mobile device 110. Once tapped, the account application 113 may transmit the values from the fields 201-204 (or indications thereof) to the contactless card 101, which stores the received values in the rules 107-1.

[0040] Figure 3A is a schematic 300 illustrating an example of tapping the contactless card 101 to preauthorize a transaction. As shown, the account application 113 may output an indication to tap the contactless card 101 to the mobile device 110 to preauthorize a transaction after receiving a fingerprint to authenticate the user's account. The user may initiate a request to preauthorize the transaction in the account application 113 to preserve account security.

[0041] Once the contactless card 101 is tapped to the mobile device 110, the contactless card 101 may generate encrypted data 108 using the private key, the cryptographic algorithm, and the customer identifier. As stated, in some embodiments, the contactless card 101 may determine whether any data received from the mobile device 110 violates one or more rules 107-1. For example, as shown, the user has specified to preapprove a $100 transaction. If the $100 value exceeds a rule in the rules 107-1, the contactless card 101 may refrain from generating the encrypted data 108, thereby ending the preauthorization process. As another example, if location data received from the mobile device 110 is not within the one or more permitted locations specified in the rules 107-1, the contactless card 101 may refrain from generating the encrypted data 108, thereby ending the preauthorization process.

[0042] Once generated, the contactless card 101 may transmit the encrypted data 108 to the account application 113 of the mobile device 110. The account application 113 may transmit the encrypted data 108, location data, and any other data (e.g., requested amount, requested merchant, etc.) to the server 120. The authorization application 123 may then attempt to decrypt the encrypted data 108. If the encrypted data 108 is successfully decrypted to yield the customer ID, the authorization application 123 may then determine whether the location data and any other received data violates any rules in the rules 107-2. For example, if the $100 request exceeds an amount specified in the rules 107-2, the authorization application 123 may refrain from preauthorizing the transaction.

[0043] In the example depicted in Figure 3A, the authorization application 123 preauthorizes the transaction based on decrypting the encrypted data 108 and/or determining that the rules 107-2 are not violated by the request. In response, the authorization application 123 stores an indication of the preauthorization in the account data 124 and transmits an indication of the preauthorization to the account application 113 of the mobile device 110. The stored indication of preauthorization may include one or more attributes, such as the location data received from the mobile device, a timestamp, a transaction amount, etc. The account application 113 may then output another indication to tap the contactless card 101 to the mobile device 110. Doing so may cause the indication of preauthorization to be stored in the memory 102 of the contactless card 101.

[0044] Figure 3B is a schematic 310 depicting an embodiment where the user who has received preauthorization of the transaction in Figure 3A attempts to make a purchase at a POS device 140 using the contactless card 101. As shown, the user may tap the contactless card 101 to the POS device 140 and/or insert the contactless card 101 in the POS device 140. Doing so causes the payment applet 106 to receive transaction data from the POS device 140. The transaction data may describe an amount of the transaction, a time of the transaction, a merchant identifier associated with the POS device 140, and/or a location of the transaction. The payment applet 106 may then request authorization to proceed with the transaction from the authorization applet 104. The authorization applet 104 may determine to approve the transaction based on the indication of preauthorization stored based on the results of Figure 3A. The authorization applet 104 may additionally determine whether the transaction data received from the POS device 140 satisfies the rules 107-2 (e.g., whether the merchant identifier corresponds to a permitted class of merchants, the location data corresponds to a permitted location, the amount is a permitted amount, etc.).

[0045] The authorization applet 104 may then provide an indication of approval and/or an indication of the preauthorization to the payment applet 106. The payment applet 106 may then generate an EMV payload that includes the card data 103 and the indication of preauthorization. The payment applet 106 may then transmit the EMV payload to the POS device 140. The POS device 140 may then transmit the EMV payload to the server 120. The POS device 140 may further transmit other data to the server 120, such as the transaction data, location data, merchant ID, etc. The server 120 may then approve and/or decline the transaction based at least in part on the indication of preauthorization in the EMV payload. If, for example, the server 120 identifies the indication of preauthorization, the server 120 may approve the transaction. If, however, the indication of preauthorization is expected but not detected in the EMV payload, the server 120

may decline the transaction. The server 120 may further approve and/or decline the transaction based on whether the transaction satisfies and/or violates the rules 107-2.

[0046] Figure 3C is a schematic 320 illustrating an embodiment where the POS device 140 outputs an indication that the server 120 denied the transaction. For example, the server 120 may determine that the location of the POS device 140 and/or the corresponding merchant is outside the geographical regions specified in the rules 107-2 where the contactless card 101 can be used. As another example, the authorization application 123 may determine that the location of the POS device 140 and/or the corresponding merchant is not within a threshold distance of the location data stored as an attribute of the preauthorization 132 in the account data 124. For example, if the location data of the POS device 140 and/or the merchant is 5 miles from the location data in the preauthorization 132, the server 120 may deny the transaction because the user is no longer within a threshold distance (e.g., 100 feet) of the location where the preauthorization was requested. The server 120 may transmit an indication of the denial to the POS device 140, which may output the same for display to the user.

[0047] Figure 3D is a schematic 330 illustrating an embodiment where the POS device 140 outputs an indication that the server 120 approved the transaction based on the preauthorization flag in the EMV payload. As stated, the server 120 may approve the transaction based at least in part on whether the expected indication of preauthorization is present in the EMV payload, and matches a corresponding indication stored in the account data 124 when the transaction was preauthorized. As stated, however, the server 120 may authorize the transaction based on additional factors, such as the rules 107-2 and/or other fraud prevention analyses. Once approved, the server 120 may transmit an indication of the approval to the POS device 140, which may output the same for display to the user.

[0048] Figure 4 illustrates an embodiment of a logic flow 400. The logic flow 400 may be representative of some or all of the operations executed by one or more embodiments described herein. For example, the logic flow 400 may include some or all of the operations to preauthorize a transaction. Embodiments are not limited in this context.

[0049] As shown, the logic flow 400 begins at block 405, where the authorization applet 104 generates encrypted data 108 using a private key, input data (e.g., a customer identifier), and a cryptographic algorithm. The authorization applet 104 may transmit the encrypted data 108 to the account application 113 executing on a mobile device 110. In one embodiment, the authorization applet 104 generates the encrypted data 108 responsive to a user requesting preauthorization after the user has provided authentication credentials for their account in the account application 113. At block 410, the account application 113 transmits the encrypted data 108 and location data received from the location module 114 to the server 120 via the network 130. As stated, the location data received from the location module 114 may describe the location of the mobile device 110. In some embodiments, the account application 113 may transmit additional data to the server 120, such as a requested amount for the preauthorization, a merchant for the preauthorization, a duration for the preauthorization, and/or a merchant category for the preauthorization.

[0050] At block 420, the authorization application 123 may preauthorize the transaction based at least in part on the received location data and/or decrypting the encrypted data 108. For example, the authorization application 123 may determine whether the received location data is within one or more permitted locations to use the contactless card 101 specified in the rules 107-2. The authorization application 123 may further attempt to decrypt the encrypted data 108 using the private key associated with the contactless card 101. In one embodiment, the authorization application 123 may preauthorize the transaction based on decrypting the encrypted data 108 and determining that the location data is within the one or more locations for using the contactless card 101 specified in the rules 107-2. In another embodiment, the authorization application 123 may preauthorize the transaction based on decrypting the encrypted data 108 or determining that the location data is within the one or more locations for using the contactless card 101 specified in the rules 107-2. In some embodiments, the authorization application 123 may additionally determine whether the preauthorization request satisfies the rules 107-2, e.g., whether the requested amount,

merchant, duration, and/or merchant category satisfy one or more corresponding rules in the rules 107-2. As stated, in some embodiments, the authorization application 123 may select a level of preauthorization from a plurality of levels of preauthorization. In other embodiments, the authorization application 123 may return a binary preauthorization result (e.g., preauthorized and/or not preauthorized). The authorization application 123 may then store an indication of the preauthorization in the account data 124 for the account. As stated, the stored indication of the preauthorization may include attributes such as the level of preauthorization, the time of the preauthorization, the location data received from the mobile device, etc.

[0051] At block 430, the account application 113 of the mobile device 110 may receive an indication of the preauthorization from the server 120. The account application 113 may then transmit the indication of preauthorization to the contactless card 101 which stores the indication of preauthorization in the memory 102. At block 440, the authorization applet 104 may receive a request to approve a transaction from the payment applet 106. Generally, the payment applet 106 may receive transaction data from a POS device 140 indicating attributes such as a transaction amount, merchant ID, location data, timestamp, etc.

[0052] At block 450, the authorization applet 104 approves the request from the payment applet based at least in part on the preauthorization by the server 120 and/or the location of the mobile device 110 (and/or the POS device 140). The authorization applet 104 may approve and/or decline the request based at least in part on the presence of the indication of preauthorization stored in the memory 102. For example, the authorization applet 104 may determine if the location associated with the indication of preauthorization is within a threshold distance of the latest location data received from the mobile device 110 and/or location data received from the POS device 140. Additionally and/or alternatively, the authorization applet 104 may determine whether the transaction amount and/or the time received from the POS device 140 violate amount and/or time rules in the rules 107-2. Additionally and/or alternatively, the authorization applet 104 may determine whether the merchant ID received from the POS device 140 violates merchant and/or merchant category rules in the rules 107-2.

[0053] At block 460, the payment applet 106 generates an EMV payload comprising transaction data and an indication of the preauthorization. The transaction data may include the card number, expiration date, and CVV value of the contactless card 101. The payment applet 106 may transmit the EMV payload to the POS device 140. At block 470, the POS device transmits the EMV payload and transaction data to the server 120 to request approval of payment for the transaction using the contactless card 101. The transaction data may include a transaction amount, merchant identifier, and/or location data of the POS device 140. In some embodiments, the account application 113 may also transmit data (e.g., requested amount, location information, time information) to the server 120 for approval. At block 480, the authorization application 123 of the server 120 approves payment for the transaction using the contactless card 101 based at least in part on the indication of the preauthorization in the EMV payload. For example, the authorization application 123 may determine that the location data in the stored indication of preauthorization in the account data 124 is within a threshold distance of the location of the POS device 140. Additionally and/or alternatively, the authorization application 123 may determine that the attributes of the transaction do not violate any rules 107-2 for using the contactless card 101. At block 490, the authorization application 123 transmits an indication of approval of the transaction to the POS device 140, which may output an indication of approval and further process the transaction.

[0054] Figure 5 illustrates an embodiment of a logic flow 500. The logic flow 500 may be representative of some or all of the operations executed by one or more embodiments described herein. For example, the logic flow 500 may include some or all of the operations performed by the authorization application 123 to preauthorize a transaction. Embodiments are not limited in this context.

[0055] As shown, the logic flow 500 begins at block 510, where the authorization application 123 determines whether the location data received from the mobile device 110 is within one or

more locations specified in the rules 107-2 as being permitted to use the contactless card 101. In some embodiments, the authorization application 123 determines whether the location data is within a threshold distance of the one or more locations specified in the rules 107-2. At block 520, the authorization application 123 attempts to decrypt the encrypted data 108 generated by the contactless card 101, e.g., using a copy of the private key associated with the contactless card 101. At block 530, the authorization application 123 determines whether multi-factor authentication has been completed for the account. For example, the authorization application 123 may determine to preauthorize transactions based at least in part on whether multi-factor authentication was used to authenticate the user in their account in the account application 113.

[0056] At block 540, the authorization application 123 may select one or more levels of preauthorization for the transaction based at least in part on the result of the attempted decryption of the encrypted data 108 and/or whether the location data received from the mobile device 110 is within one or more locations specified in the rules 107-2. Additionally and/or alternatively, the authorization application 123 may select the preauthorization levels based on whether multi-factor authentication was completed and/or whether any rules 107-2 are violated by the requested preauthorization. At block 550, the authorization application 123 may store an indication of the selected level of preauthorization. In some embodiments, the level of preauthorization is a binary preauthorization (e.g., preauthorized and/or not preauthorized). In one embodiment, the indication of preauthorization comprises a unique identifier for the preauthorization. The indication of preauthorization may further include the location data received from the mobile device, the requested preauthorization amount, and/or a timestamp.

[0057] At block 560, the authorization application 123 may transmit an indication of the preauthorization to the mobile device 110. The transmitted indication may be the same as the indication stored in the account data 124 and/or a different indication. For example, the authorization application 123 may transmit the unique identifier of the preauthorization. At block 570, the account application 113 transmits the indication of preauthorization received from the authorization application 123 to the contactless card 101. The contactless card 101 may then store the received indication of preauthorization to include in EMV payloads generated by the contactless card 101 to pay for transactions via a POS device 140. Doing so allows the authorization application 123 to identify the indication of preauthorization in the EMV payloads and compare the received indication (or attributes thereof) to the indication of preauthorization stored in the account data 124 (or attributes thereof).

[0058] 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 performed by the authorization application 123 to constrain the transactional capabilities of a contactless card. Embodiments are not limited in this context. For example, the authorization applet 104 may perform some or all of the operations of the logic flow 600 when determining whether to generate encrypted data 108 and/or approve a request from the payment applet 106 to pay for a transaction using the contactless card.

[0059] As shown, the logic flow 600 begins at block 610, where the authorization application 123 may determine whether location data received from the mobile device 110 is within one or more permitted locations to use the contactless card 101 (and/or within a threshold distance thereof). As stated, the permitted locations to use the contactless card 101 may be stored in the rules 107-2. At block 620, the authorization application 123 may determine whether location data provided by the POS device 140 is within one or more permitted locations to use the contactless card 101. Additionally and/or alternatively, the authorization application 123 may determine whether the location data provided by the POS device 140 is within a predefined distance of the location data received from the mobile device 110 as part of a preauthorization request.

[0060] At block 630, the authorization application 123 may determine whether a transaction amount for a requested transaction is below a maximum amount specified in the rules 107-1 and/or the rules 107-2 for using the contactless card. At block 640, the authorization application 123 may

determine whether a time of the transaction is within one or more periods of time the contactless card 101 is permitted for use (e.g., based on the rules 107-2 and/or the rules 107-2). At block 650, the authorization application 123 may determine whether a merchant associated with the transaction is a permitted use of the contactless card 101. As stated, the 107-2 may specify permitted merchant identifiers and/or merchant categories. If the merchant identifier associated with the transaction is not a permitted merchant identifier and/or not within a permitted merchant category, the server 120 and/or the contactless card 101 may restrict use of the contactless card 101. At block 660, the authorization application 123 may determine whether an indication of preauthorization is stored in the EMV payload received from the POS device 140. In some embodiments, the authorization application 123 may compare the indication of preauthorization (or an attribute thereof) to one or more stored indications of preauthorization for the account in the account data. Furthermore, the authorization application 123 may determine whether any rules associated with the indication of preauthorization are violated. For example, the preauthorization may be limited in time, distance (e.g., relative to the location data received from the mobile device 110 when the preauthorization was processed), etc.

[0061] At block 670, the authorization application 123 may approve the transaction based at least in part on determining all rules 107-2 are satisfied and/or identifying the indication of preauthorization in the EMV payload. At block 680, the authorization application 123 may decline the transaction based at least in part on determining at least one rule 107-2 is not satisfied and/or failing to identify the indication of preauthorization in the EMV payload. Similarly, if the location data associated with the indication of preauthorization is not within a threshold distance of the POS device 140 providing the EMV payload, the authorization application 123 may decline the transaction.

[0062] 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 constrain the transactional capabilities of a contactless card. Embodiments are not limited in this context.

[0063] As shown, the logic flow 700 begins at block 705, where the location module 114 of an unlocked mobile device 110 provides location data to the account application 113. The account application 113 may, in turn, transmit the location data to the contactless card 101. At block 710, the payment applet 106 of the contactless card 101 may receive transaction data (e.g., a transaction amount, merchant ID, location data, etc.) from a POS device 140. At block 720, the payment applet 106 requests approval for the transaction from the authorization applet 104. At block 730, the authorization applet 104 determines that the rules 107-1 are satisfied by the transaction data, including the transaction amount, location of the POS device 140, and/or the merchant ID. At block 740, the authorization applet 104 determines that a valid indication of preauthorization is stored in the memory 102. For example, the authorization applet 104 may determine that a time associated with the preauthorization is within a time threshold specified in the rules 107-1. As another example, the authorization applet 104 may determine that the location data associated with the indication of preauthorization is within a threshold distance of the location data of the POS device 140.

[0064] At block 750, the authorization applet 104 provides the approval to the payment applet 106 based at least in part on the determinations made at blocks 730 and 740. At block 760, the payment applet 106 generates an EMV payload comprising the account number, expiration date, CVV, and indication of preauthorization. The payment applet 106 may then transmit the EMV payload to the POS device 140. At block 770, the POS device 140 transmits the EMV payload, transaction data, and location data of the POS device 140 to the authorization application 123 of the server 120.

[0065] At block 780, the authorization application 123 approves the transaction based at least in part on detecting the indication of preauthorization in the EMV payload and/or the location data received from the POS device 140. For example, the authorization application 123 may determine whether location data provided by the POS device 140 is within one or more permitted locations

to use the contactless card 101. Additionally and/or alternatively, the authorization application 123 may determine whether the location data provided by the POS device 140 is within a predefined distance of the location data of the indication of preauthorization stored in the account data 124. The authorization application 123 may then transmit an indication of approval. At block 790, the POS device 140 may process the transaction responsive to receiving the indication of approval from the authorization application 123.

[0066] 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 to determine multi-factor authentication has been performed for an account. Embodiments are not limited in this context.

[0067] As shown, the logic flow 800 begins at block 810, where the account application 113 optionally receives valid login credentials (e.g., a username and password) for an account. At block 820, the account application 113 optionally receives biometric credentials (e.g., iris scan, fingerprints, Face ID, etc.) for the account. At block 830, the account application 113 optionally receives a one-time passcode transmitted by the server 120 to the phone number of the mobile device 110 in a text message. At block 840, the account application 113 optionally receives encrypted data 108 generated by the contactless card 101 and transmits the encrypted data 108 to the server 120. The server 120 may decrypt the encrypted data 108 to verify the encrypted data 108 and transmit an indication of the verification to the account application 113. At block 850, the account application 113 optionally receive a passcode generated by a different application and provided by the user as input to the account application 113. At block 860, the account application 113 may determine multi-factor authentication for the account has occurred based on at least two of the authentication factors in blocks 810-850. For example, if the login credentials are received at block 810 and the biometric credentials are received at 820, the account application 113 may determine multi-factor authentication for the account has been completed. The account application 113 may transmit an indication of the multi-factor authentication for the account to the server 120.

[0068] Figure 9 illustrates an embodiment of an exemplary computing architecture 900 comprising a computing system 902 that may be suitable for implementing various embodiments as previously described. In various embodiments, the computing architecture 900 may comprise or be implemented as part of an electronic device. In some embodiments, the computing architecture 900 may be representative, for example, of a system that implements one or more components of the system 100. In some embodiments, computing system 902 may be representative, for example, of the contactless card 101, mobile devices 110, server 120, and/or the POS devices 140 of the system 100. The embodiments are not limited in this context. More generally, the computing architecture 900 is configured to implement all logic, applications, systems, methods, apparatuses, and functionality described herein with reference to Figures 1-8.

[0069] 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 900. 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.

[0070] The computing system 902 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 902.

[0071] As shown in Figure 9, the computing system 902 comprises a processor 904, a system memory 906 and a system bus 908. The processor 904 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 904.

[0072] The system bus 908 provides an interface for system components including, but not limited to, the system memory 906 to the processor 904. The system bus 908 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 908 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.

[0073] The system memory 906 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 9, the system memory 906 can include non-volatile memory 910 and/or volatile memory 912. A basic input/output system (BIOS) can be stored in the non-volatile memory 910.

[0074] The computing system 902 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) 914, a magnetic floppy disk drive (FDD) 916 to read from or write to a removable magnetic disk 918, and an optical disk drive 920 to read from or write to a removable optical disk 922 (e.g., a CD-ROM or DVD). The HDD 914, FDD 916 and optical disk drive 920 can be connected to the system bus 908 by a HDD interface 924, an FDD interface 926 and an optical drive interface 928, respectively. The HDD interface 924 for external drive implementations can include at least one or both of Universal Serial Bus (USB) and IEEE 1394 interface technologies. The computing system 902 is generally is configured to implement all logic, systems, methods, apparatuses, and functionality described herein with reference to Figures 1-8.

[0075] 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 910, 912, including an operating system 930, one or more application programs 932, other program modules 934, and

program data 936. In one embodiment, the one or more application programs 932, other program modules 934, and program data 936 can include, for example, the various applications and/or components of the system 100, e.g., the card data 103, authorization applet 104, payment applet 106, rules 107, encrypted data 108, account application 113, the authorization application 123, account data 124, and/or the transaction logic 144.

[0076] A user can enter commands and information into the computing system 902 through one or more wire/wireless input devices, for example, a keyboard 938 and a pointing device, such as a mouse 940. 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 904 through an input device interface 942 that is coupled to the system bus 908, 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.

[0077] A monitor 944 or other type of display device is also connected to the system bus 908 via an interface, such as a video adaptor 946. The monitor 944 may be internal or external to the computing system 902. In addition to the monitor 944, a computer typically includes other peripheral output devices, such as speakers, printers, and so forth.

[0078] The computing system 902 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 948. The remote computer 948 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 902, although, for purposes of brevity, only a memory/storage device 950 is illustrated. The logical connections depicted include wire/wireless connectivity to a local area network (LAN) 952 and/or larger networks, for example, a wide area network (WAN) 954. 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 952 and the WAN 954.

[0079] When used in a LAN networking environment, the computing system 902 is connected to the LAN 952 through a wire and/or wireless communication network interface or adaptor 956. The adaptor 956 can facilitate wire and/or wireless communications to the LAN 952, which may also include a wireless access point disposed thereon for communicating with the wireless functionality of the adaptor 956. The network interface 112 of the mobile device 110 is an example of the adaptor 956.

[0080] When used in a WAN networking environment, the computing system 902 can include a modem 958, or is connected to a communications server on the WAN 954, or has other means for establishing communications over the WAN 954, such as by way of the Internet. The modem 958, which can be internal or external and a wire and/or wireless device, connects to the system bus 908 via the input device interface 942. In a networked environment, program modules depicted relative to the computing system 902, or portions thereof, can be stored in the remote memory/storage device 950. 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.

[0081] The computing system 902 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).

[0082] Figure 10A 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 1002 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 1010, 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.

[0083] The contactless card 101 may also include identification information 1015 displayed on the front and/or back of the card, and a contact pad 1020. The contact pad 1020 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. 10A. These components may be located behind the contact pad 1020 or elsewhere on the substrate 1010. 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. 10A).

[0084] As illustrated in FIG. 10B, the contact pad 1020 of contactless card 101 may include processing circuitry 1025 for storing and processing information, including a microprocessor 1030 and the memory 102. It is understood that the processing circuitry 1025 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.

[0085] 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.

[0086] The memory 102 may be configured to store the card data 103, one or more applets (including the authorization applet 104, the payment applet 106, and any other applet), a private key 1008, the encrypted data 108, the rules 107-1, and one or more customer (or user) identifiers (IDs) 1007. 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 1007 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 1007 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 authorization applet 104 (or a different applet)

may use the customer ID 1007 as input to a cryptographic algorithm with the private key 1008 to generate the encrypted data 108.

[0087] 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 1020 or entirely separate from it, or as further elements in addition to processor 1030 and memory 102 elements located within the contact pad 1020.

[0088] In some examples, the contactless card 101 may comprise one or more antennas 1055. The one or more antennas 1055 may be placed within the contactless card 101 and around the processing circuitry 1025 of the contact pad 1020. For example, the one or more antennas 1055 may be integral with the processing circuitry 1025 and the one or more antennas 1055 may be used with an external booster coil. As another example, the one or more antennas 1055 may be external to the contact pad 1020 and the processing circuitry 1025.

[0089] 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 1055, processing circuitry 1025, and/or the memory 102, the contactless card 101 provides a communications interface to communicate via NFC, Bluetooth, and/or Wi-Fi communications.

[0090] 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 communications interface 105-1 of the device 110), and produce an NDEF message that comprises a cryptographically secure OTP encoded as an NDEF text tag.

[0091] 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.

[0092] 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.

[0093] 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. A contactless card, comprising:

a processor circuit;

a communications interface; and

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

receive, via the communications interface from a mobile device executing an account application, an indication that a server preauthorized a transaction based on location data describing a location of the mobile device and verification of encrypted data, the encrypted data generated by the contactless card using a cryptographic algorithm and a private key stored in the memory of the contactless card, the indication further specifying that one or more credentials for an account associated with the contactless card have received by the account application;

receive, via the communications interface from a point of sale (POS) device, an indication to pay for the transaction using the contactless card;

determine, based on one or more rules stored in the memory, that the location of the mobile device is within a threshold distance of one or more locations the contactless card is permitted for use;

generate transaction data comprising: (i) indications of an account number and an expiration date of the contactless card, and (ii) the indication of the preauthorization of the transaction by the server;

transmit the transaction data to the POS device as payment for the transaction; and

receive, from the POS device, an indication that the server authorized payment for the transaction using at least a portion of the transaction data and based at least in part on identifying the indication of the preauthorization of the transaction by the server in the transaction data.

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

write the indication of the preauthorization of the transaction by the server to a first field of an EMV payload; and

write an indication of the location data, the indication of the account number, the indication of the expiration date, and an indication of a card verification value (CVV) to one or more other fields of the EMV payload.

3. The contactless card of claim 2, wherein the memory stores an authorization applet and a payment applet, wherein the authorization applet determines that the location of the mobile device is within the threshold distance of the one or more locations the contactless card is permitted for use, wherein the authorization applet receives the indication of the preauthorization of the transaction by the server from the mobile device, wherein the authorization applet generates the encrypted data based on a customer ID associated with the contactless card, wherein the payment applet generates the EMV payload and transmits the EMV payload to the POS device responsive to receiving approval from the authorization applet, the authorization applet to provide approval to the payment applet based on the received indication of the preauthorization of the transaction by the server from the mobile device and the determination that the location of the mobile device is within the threshold distance of the one or more locations the contactless card is permitted for use.

4. The contactless card of claim 3, the memory storing instructions which when executed by the processor circuit cause the processor circuit to:

receive, via the communications interface from the account application executing on the mobile device, an indication that multi-factor authentication for the account has been completed using the mobile device, the multi-factor authentication based on at least two of: (i) a login and

password for the account, (ii) a one-time password transmitted to a phone number associated with the account, (iii) biometric credentials associated with the account, (iv) a temporary code generated by an authentication application, and (v) data generated by the contactless card.

5. The contactless card of claim 3, the POS device to transmit the EMV payload and location data describing a location of the POS device to the server, the memory storing instructions which when executed by the processor circuit cause the processor circuit to:

prior to transmitting an indication of approval for the transaction to the POS device:

receive an indication specifying that the server determined that the location of the mobile device is within the threshold distance of the location data describing the location of the POS device; and

receive an indication specifying that the server verified that the transaction has been preauthorized based on the indication of the preauthorization of the transaction by the server in the first field of the EMV payload.

6. The contactless card of claim 3, the memory storing instructions which when executed by the processor circuit cause the processor circuit to:

receive, by the authorization applet via the communications interface from the mobile device, updated location data describing an updated location of the mobile device, the updated location different than the location;

determine, by the authorization applet based on the one or more rules stored in the memory, that the location of the mobile device is not within the threshold distance of one or more of the locations the contactless card is permitted for use;

receive, by the payment applet from a second POS device, indication to pay for a second transaction using the contactless card;

request, by the payment applet, approval from the authorization applet to pay for the second transaction;

deny, by the authorization applet, approval to pay for the second transaction based on the determination that the location of the mobile device is not within the threshold distance of one or more of the locations the contactless card is permitted for use; and

transmit, by the payment applet to the second POS device, an indication denying payment for the second transaction using the contactless card based on the denial by the authorization applet.

7. The contactless card of claim 1, wherein the indication of the preauthorization of the transaction by the server in the transaction data comprises a different indication of the preauthorization of the transaction by the server, wherein the communications interface of the contactless card is configured to support at least one of near field communication (NFC), Bluetooth, and Wi-Fi, the memory storing instructions which when executed by the processor circuit cause the processor circuit to:

receive a current time associated with the transaction;

determine, based on the one or more rules stored in the memory, that the current time is within an amount of time permitted to use the contactless card;

receive, from the POS device, an indication of an amount of the transaction; and

determine, based the on one or more rules stored in the memory, that the amount of the transaction is less than a maximum spend amount associated with the contactless card.

8. A non-transitory computer-readable storage medium storing instructions which when executed by a processor cause the processor to:

verify, by a server, encrypted data generated by a contactless card using a cryptographic algorithm and a private key, the encrypted data received by the server from a mobile device executing an account application, one or more credentials for an account associated with the contactless card received by the account application;

determine, by the server based on one or more rules associated with the account, that location data received from the mobile device is within a threshold distance of one or more locations the contactless card is permitted for use;

preauthorize, by the server, a transaction using the contactless card based on the verification of the encrypted data and the determination that the mobile device is within the threshold distance of the one or more locations the contactless card is permitted for use;

transmit, by the server to the account application executing on the mobile device, an indication of the preauthorization for the transaction;

receive, by the server from a point of sale (POS) device, transaction data comprising: (i) indications of an account number and an expiration date of the contactless card, and (ii) the indication of the preauthorization of the transaction by the server; and

approve the transaction by the server based at least in part on identifying the indication of the preauthorization of the transaction by the server in the transaction data.

9. The non-transitory computer-readable storage medium of claim 8, the transaction data comprising an EMV payload, the non-transitory computer-readable storage medium storing instructions which when executed by the processor cause the processor to:

identify, by the server, the indication of the preauthorization of the transaction by the server in a first field of the EMV payload; and

identify the indication of the account number, the indication of the expiration date, and an indication of a card verification value (CVV) in one or more other fields of the EMV payload.

10. The non-transitory computer-readable storage medium of claim 9, storing instructions which when executed by the processor cause the processor to:

store, by the server, the indication of the preauthorization; and

compare, by the server, the stored indication of the preauthorization of the transaction by the server to the indication of the preauthorization of the transaction by the server in the first field of the EMV payload.

11. The non-transitory computer-readable storage medium of claim 10, the preauthorization comprising one or more levels of preauthorization, the levels of preauthorization based on: (i) the server decrypting the encrypted data using a copy of the private key and the cryptographic algorithm, and (ii) determining that location data received from the mobile device is within the threshold distance of one or more locations the contactless card is permitted for use.

12. The non-transitory computer-readable storage medium of claim 11, the POS device to transmit the EMV payload and location data describing a location of the POS device to the server, the non-transitory computer-readable storage medium storing instructions which when executed by the processor cause the processor to, prior to transmitting an indication of approval for the transaction to the POS device:

determine, by the server, that the location of the mobile device is within the threshold distance the location of the POS device.

13. The non-transitory computer-readable storage medium of claim 11, storing instructions which when executed by the processor cause the processor to:

receive, by the server, a current time associated with the transaction; and

determine, by the server based on the one or more rules associated with the account, that the current time is within an amount of time permitted to use the contactless card.

14. The non-transitory computer-readable storage medium of claim 8, wherein a communications interface of the contactless card is configured to support at least one of near field communication (NFC), Bluetooth, and Wi-Fi, storing instructions which when executed by the processor cause the processor to:

receive, by the server from the POS device, an indication of an amount of the transaction; and

determine, by the server based on the one or more rules associated with the account, that the amount of the transaction is less than a maximum spend amount associated with the contactless card.

15. A method, comprising:

verifying, by a server, encrypted data generated by a contactless card using a cryptographic algorithm and a private key, the encrypted data received by the server from a

mobile device executing an account application, one or more credentials for an account associated with the contactless card received by the account application;

determining, by the server based on one or more rules associated with the account, that location data received from the mobile device is within a threshold distance of one or more locations the contactless card is permitted for use;

preauthorizing, by the server, a transaction using the contactless card based on the verification of the encrypted data and the determination that the mobile device is within the threshold distance of the one or more locations the contactless card is permitted for use;

transmitting, by the server to the account application executing on the mobile device, an indication of the preauthorization for the transaction;

receiving, by the server from a point of sale (POS) device, transaction data comprising: (i) indications of an account number and an expiration date of the contactless card, and (ii) the indication of the preauthorization of the transaction by the server; and

approving the transaction by the server based at least in part on identifying the indication of the preauthorization of the transaction by the server in the transaction data.

16. The method of claim 15, the transaction data comprising an EMV payload, the method further comprising:

identifying, by the server, the indication of the preauthorization of the transaction by the server in a first field of the EMV payload; and

identifying the indication of the account number, the indication of the expiration date, and an indication of a card verification value (CVV) in one or more other fields of the EMV payload.

17. The method of claim 16, further comprising:

storing, by the server, the indication of the preauthorization; and

comparing, by the server, the stored indication of the preauthorization of the transaction by the server to the indication of the preauthorization of the transaction by the server in the first field of the EMV payload.

18. The method of claim 17, the preauthorization comprising one or more levels of preauthorization, the levels of preauthorization based on: (i) the server decrypting the encrypted data using a copy of the private key and the cryptographic algorithm, and (ii) determining that location data received from the mobile device is within the threshold distance of one or more locations the contactless card is permitted for use.

19. The method of claim 17, wherein the POS device transmits the EMV payload and location data describing a location of the POS device to the server, the method further comprising prior to transmitting an indication of approval for the transaction to the POS device:

determining, by the server, that the location of the mobile device is within the threshold distance the location of the POS device.

20. The method of claim 15, wherein a communications 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 prior to approving the transaction:

receiving, by the server, a current time associated with the transaction;

determining, by the server based on the one or more rules associated with the account, that the current time is within an amount of time permitted to use the contactless card;

receiving, by the server from the POS device, an indication of an amount of the transaction; and

determining, by the server based on the one or more rules associated with the account, that the amount of the transaction is less than a maximum spend amount associated with the contactless card.

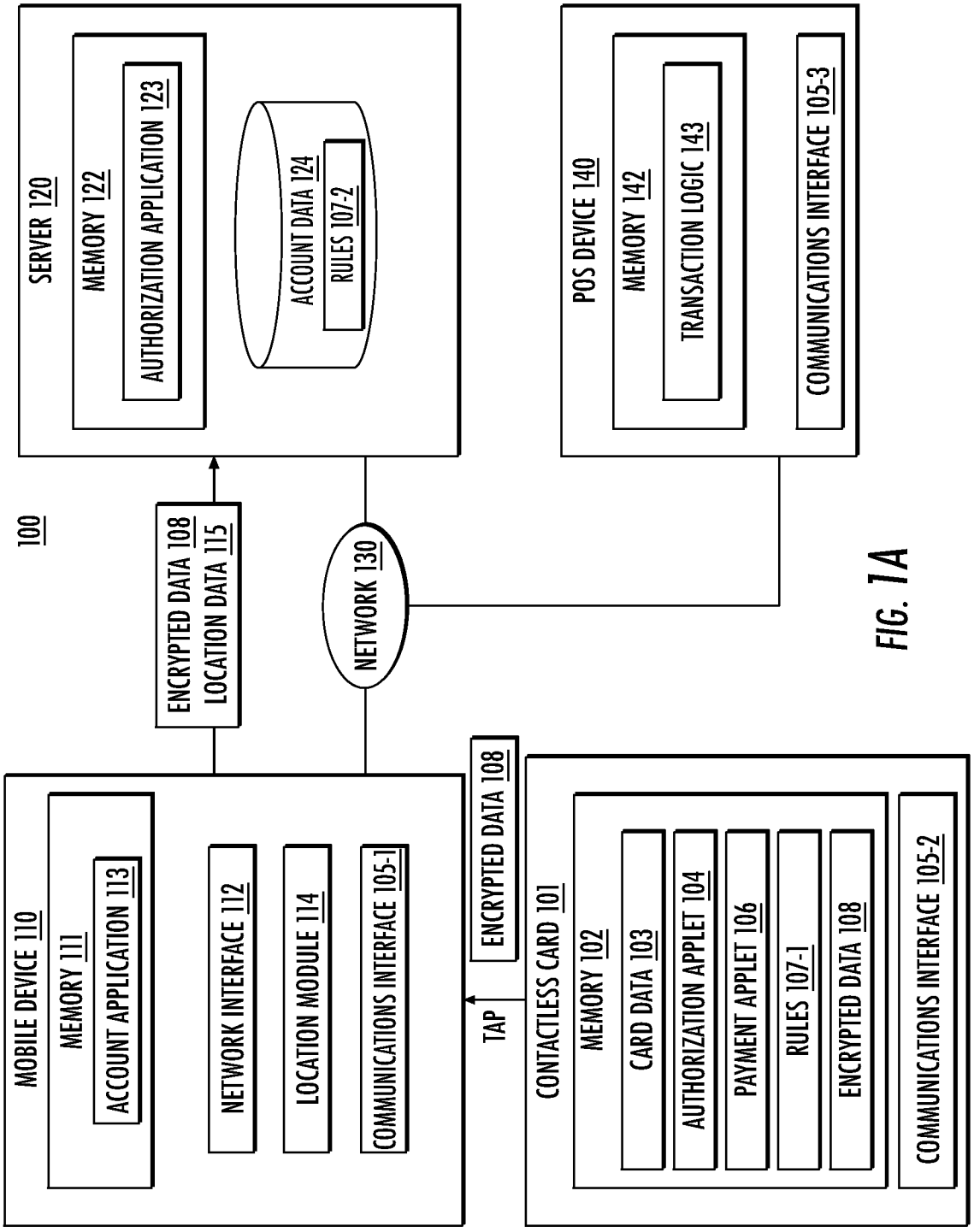

100
SERVER 120
MEMORY 122
AUTHORIZATION APPLICATION 123
ACCOUNT DATA 124
RULES 107-2
POS DEVICE 140
MEMORY 142
TRANSACTION LOGIC 143
COMMUNICATIONS INTERFACE 105-3
ENCRYPTED DATA 108
LOCATION DATA 115
NETWORK 130
MOBILE DEVICE 110
MEMORY 111
ACCOUNT APPLICATION 113
NETWORK INTERFACE 112
LOCATION MODULE 114
COMMUNICATIONS INTERFACE 105-1
TAP
ENCRYPTED DATA 108
CONTACTLESS CARD 101
MEMORY 102
CARD DATA 103
AUTHORIZATION APPLET 104
PAYMENT APPLET 106
RULES 107-1
ENCRYPTED DATA 108
COMMUNICATIONS INTERFACE 105-2

FIG. 1A

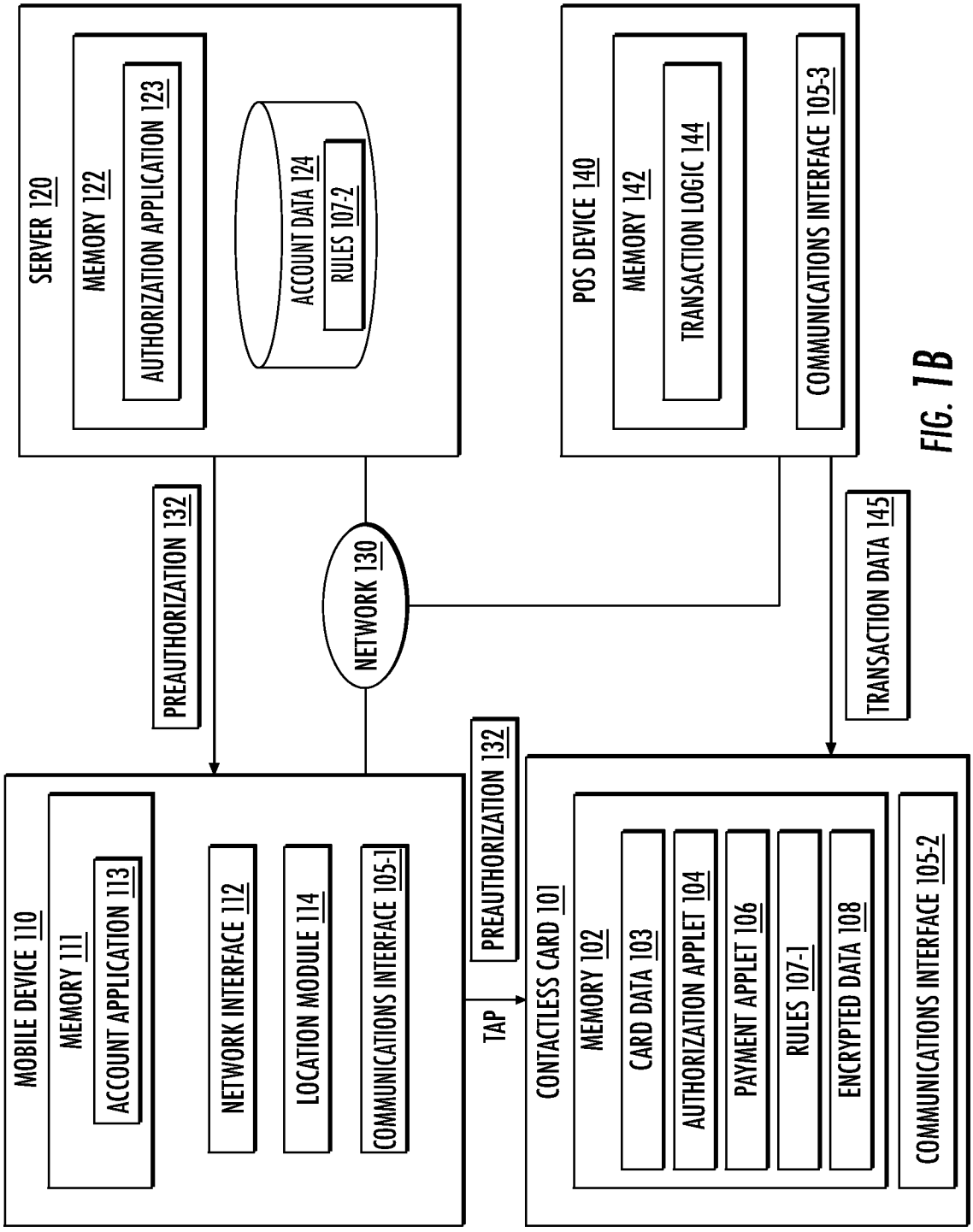

SERVER 120
MEMORY 122
AUTHORIZATION APPLICATION 123
ACCOUNT DATA 124
RULES 107-2
POS DEVICE 140
MEMORY 142
TRANSACTION LOGIC 144
COMMUNICATIONS INTERFACE 105-3
PREAUTHORIZATION 132
NETWORK 130
TRANSACTION DATA 145
MOBILE DEVICE 110
MEMORY 111
ACCOUNT APPLICATION 113
NETWORK INTERFACE 112
LOCATION MODULE 114
COMMUNICATIONS INTERFACE 105-1
PREAUTHORIZATION 132
TAP
CONTACTLESS CARD 101
MEMORY 102
CARD DATA 103
AUTHORIZATION APPLET 104
PAYMENT APPLET 106
RULES 107-1
ENCRYPTED DATA 108
COMMUNICATIONS INTERFACE 105-2

FIG. 1B

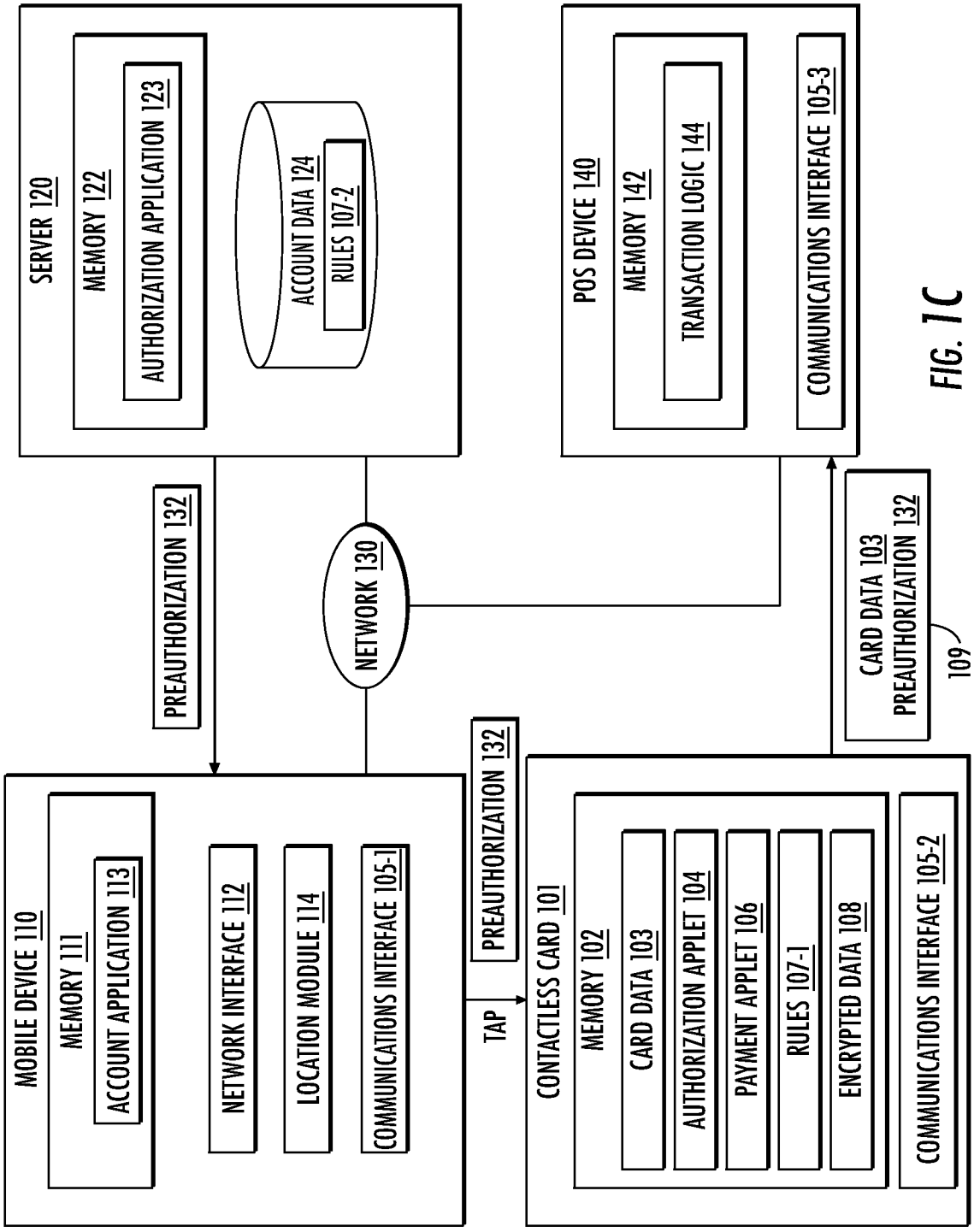

SERVER 120
MEMORY 122
AUTHORIZATION APPLICATION 123
ACCOUNT DATA 124
RULES 107-2
POS DEVICE 140
MEMORY 142
TRANSACTION LOGIC 144
COMMUNICATIONS INTERFACE 105-3
PREAUTHORIZATION 132
NETWORK 130
CARD DATA 103
PREAUTHORIZATION 132
109
MOBILE DEVICE 110
MEMORY 111
ACCOUNT APPLICATION 113
NETWORK INTERFACE 112
LOCATION MODULE 114
COMMUNICATIONS INTERFACE 105-1
PREAUTHORIZATION 132
TAP
CONTACTLESS CARD 101
MEMORY 102
CARD DATA 103
AUTHORIZATION APPLET 104
PAYMENT APPLET 106
RULES 107-1
ENCRYPTED DATA 108
COMMUNICATIONS INTERFACE 105-2

FIG. 1C

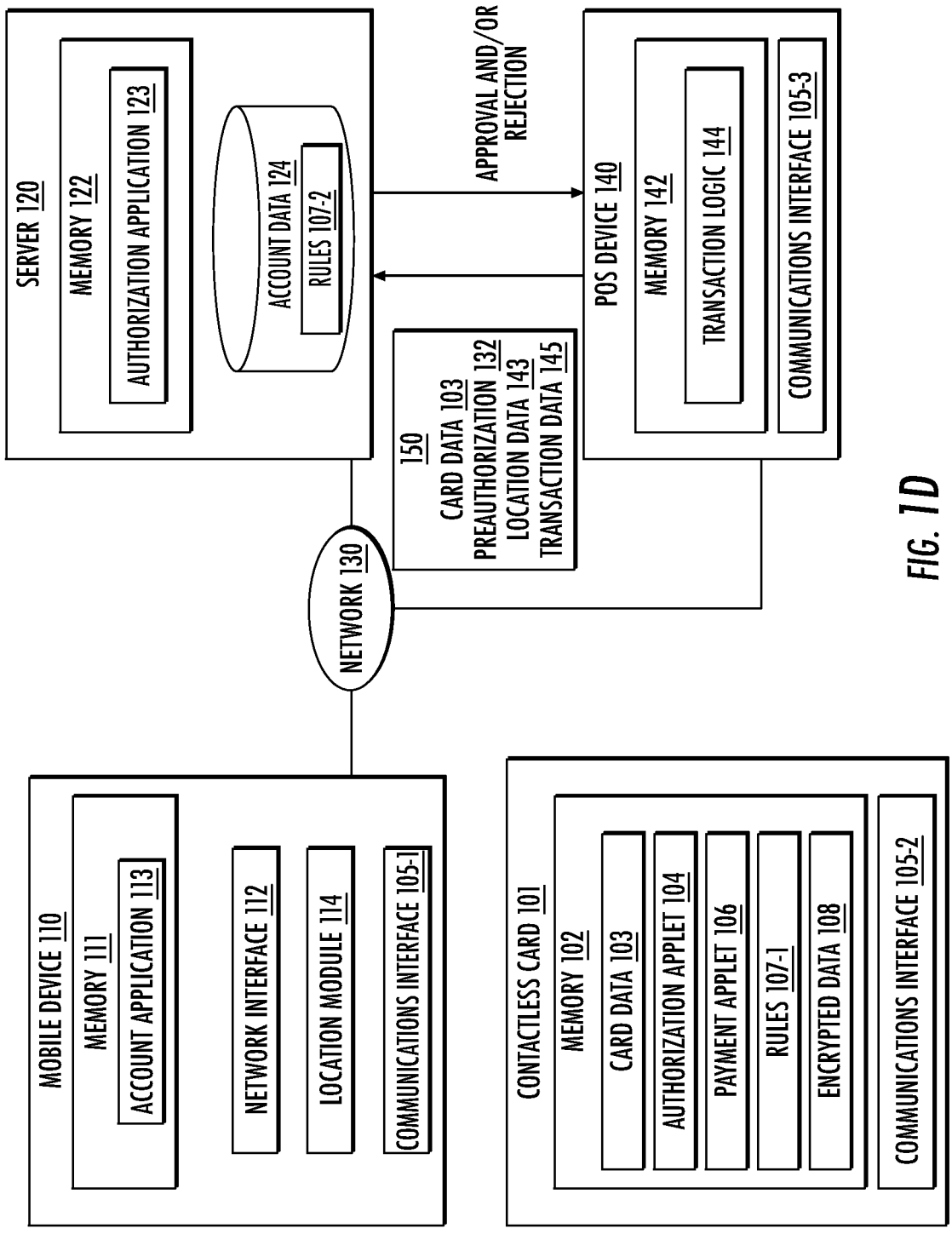

SERVER 120
MEMORY 122
AUTHORIZATION APPLICATION 123
ACCOUNT DATA 124
RULES 107-2
APPROVAL AND/OR REJECTION
POS DEVICE 140
MEMORY 142
TRANSACTION LOGIC 144
COMMUNICATIONS INTERFACE 105-3
150
CARD DATA 103
PREAUTHORIZATION 132
LOCATION DATA 143
TRANSACTION DATA 145
NETWORK 130
MOBILE DEVICE 110
MEMORY 111
ACCOUNT APPLICATION 113
NETWORK INTERFACE 112
LOCATION MODULE 114
COMMUNICATIONS INTERFACE 105-1
CONTACTLESS CARD 101
MEMORY 102
CARD DATA 103
AUTHORIZATION APPLET 104
PAYMENT APPLET 106
RULES 107-1
ENCRYPTED DATA 108
COMMUNICATIONS INTERFACE 105-2

FIG. 1D

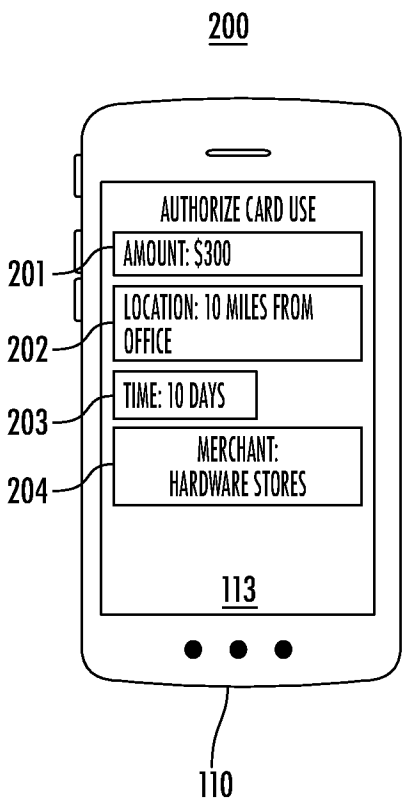

200
AUTHORIZE CARD USE
AMOUNT: $300
LOCATION: 10 MILES FROM OFFICE
TIME: 10 DAYS
MERCHANT: HARDWARE STORES
201
202
203
204
113
110

FIG. 2A

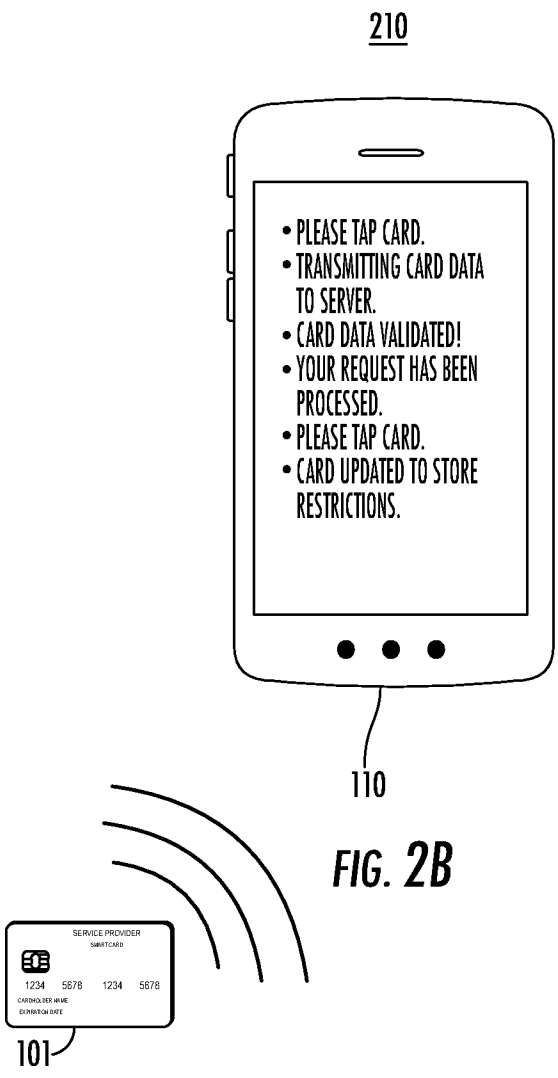

210
• PLEASE TAP CARD.
• TRANSMITTING CARD DATA TO SERVER.
• CARD DATA VALIDATED!
• YOUR REQUEST HAS BEEN PROCESSED.
• PLEASE TAP CARD.
• CARD UPDATED TO STORE RESTRICTIONS.
110
SERVICE PROVIDER
SMARTCARD
1234 5678 1234 5678
CARDHOLDER NAME
EXPIRATION DATE
101

FIG. 2B

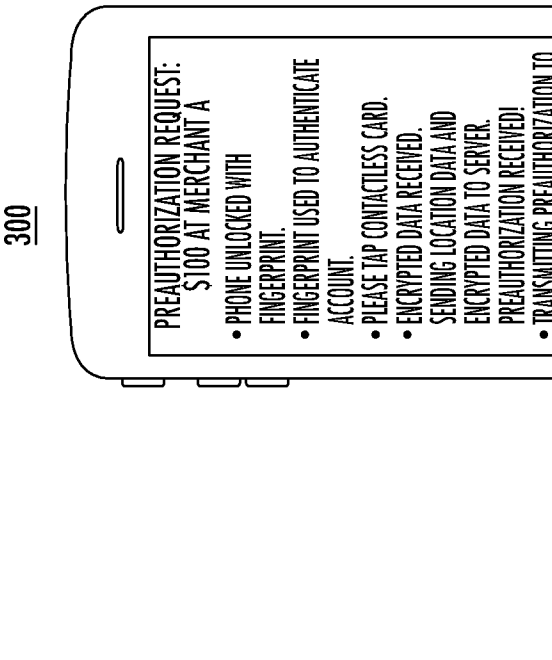

300
PREAUTHORIZATION REQUEST:
$100 AT MERCHANT A
• PHONE UNLOCKED WITH FINGERPRINT.
• FINGERPRINT USED TO AUTHENTICATE ACCOUNT.
• PLEASE TAP CONTACTLESS CARD.
• ENCRYPTED DATA RECEIVED. SENDING LOCATION DATA AND ENCRYPTED DATA TO SERVER. PREAUTHORIZATION RECEIVED!
• TRANSMITTING PREAUTHORIZATION TO CONTACTLESS CARD.
113
110
101
SERVICE PROVIDER
SMART CARD
1234 5678 1234 5678
CARDHOLDER NAME
EXPIRATION DATE

FIG. 3A

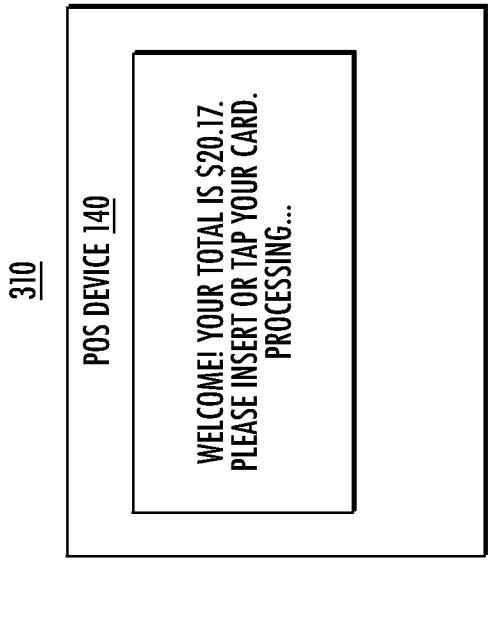

310
POS DEVICE 140
WELCOME! YOUR TOTAL IS $20.17.
PLEASE INSERT OR TAP YOUR CARD.
PROCESSING...
101
SERVICE PROVIDER
SMART CARD
1234 5678 1234 5678
CARDHOLDER NAME
EXPIRATION DATE

FIG. 3B

330

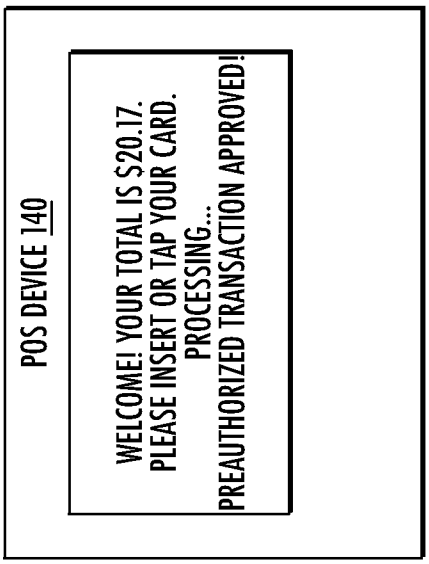


FIG. 3D

320

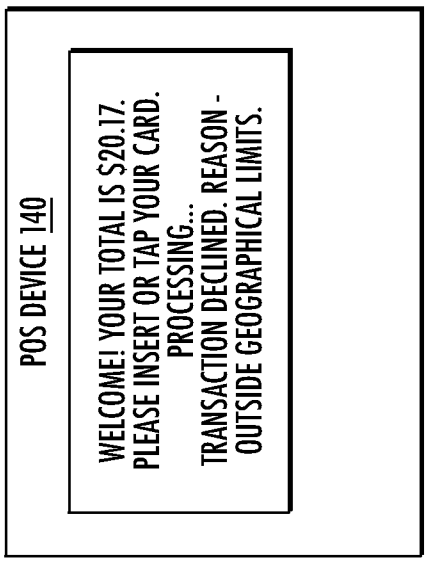


FIG. 3C

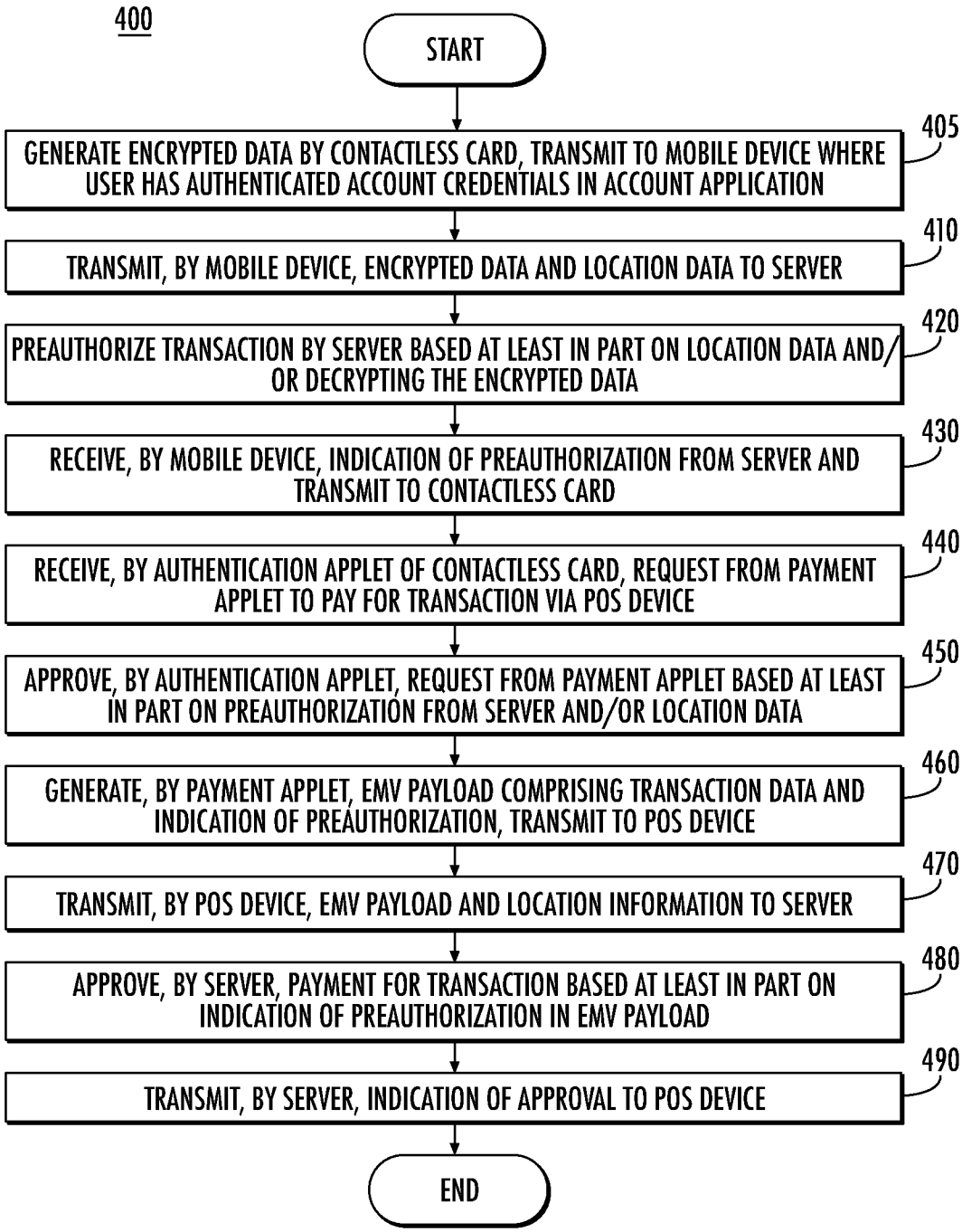

400
START
GENERATE ENCRYPTED DATA BY CONTACTLESS CARD, TRANSMIT TO MOBILE DEVICE WHERE USER HAS AUTHENTICATED ACCOUNT CREDENTIALS IN ACCOUNT APPLICATION
405
TRANSMIT, BY MOBILE DEVICE, ENCRYPTED DATA AND LOCATION DATA TO SERVER
410
PREAUTHORIZE TRANSACTION BY SERVER BASED AT LEAST IN PART ON LOCATION DATA AND/OR DECRYPTING THE ENCRYPTED DATA
420
RECEIVE, BY MOBILE DEVICE, INDICATION OF PREAUTHORIZATION FROM SERVER AND TRANSMIT TO CONTACTLESS CARD
430
RECEIVE, BY AUTHENTICATION APPLET OF CONTACTLESS CARD, REQUEST FROM PAYMENT APPLET TO PAY FOR TRANSACTION VIA POS DEVICE
440
APPROVE, BY AUTHENTICATION APPLET, REQUEST FROM PAYMENT APPLET BASED AT LEAST IN PART ON PREAUTHORIZATION FROM SERVER AND/OR LOCATION DATA
450
GENERATE, BY PAYMENT APPLET, EMV PAYLOAD COMPRISING TRANSACTION DATA AND INDICATION OF PREAUTHORIZATION, TRANSMIT TO POS DEVICE
460
TRANSMIT, BY POS DEVICE, EMV PAYLOAD AND LOCATION INFORMATION TO SERVER
470
APPROVE, BY SERVER, PAYMENT FOR TRANSACTION BASED AT LEAST IN PART ON INDICATION OF PREAUTHORIZATION IN EMV PAYLOAD
480
TRANSMIT, BY SERVER, INDICATION OF APPROVAL TO POS DEVICE
490
END

FIG. 4

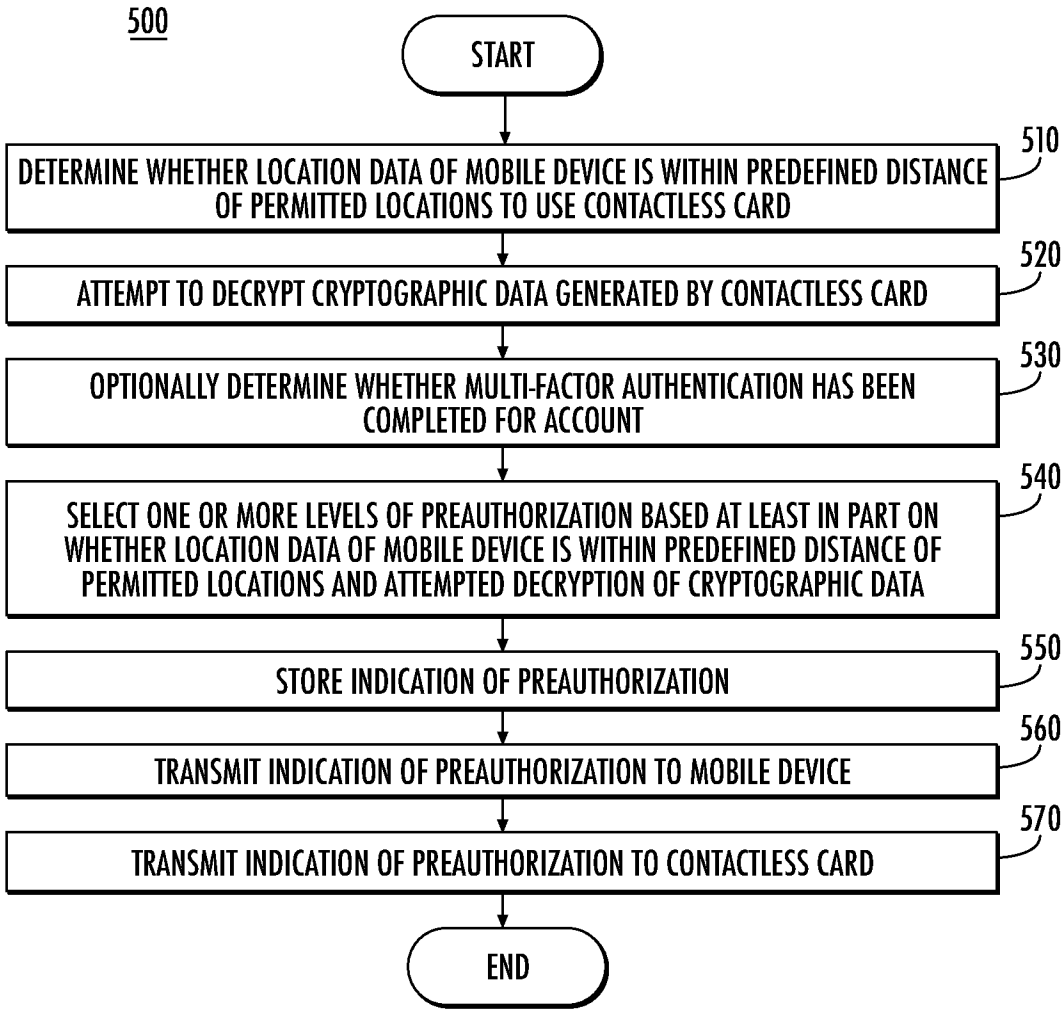

500
START
DETERMINE WHETHER LOCATION DATA OF MOBILE DEVICE IS WITHIN PREDEFINED DISTANCE OF PERMITTED LOCATIONS TO USE CONTACTLESS CARD
510
ATTEMPT TO DECRYPT CRYPTOGRAPHIC DATA GENERATED BY CONTACTLESS CARD
520
OPTIONALLY DETERMINE WHETHER MULTI-FACTOR AUTHENTICATION HAS BEEN COMPLETED FOR ACCOUNT
530
SELECT ONE OR MORE LEVELS OF PREAUTHORIZATION BASED AT LEAST IN PART ON WHETHER LOCATION DATA OF MOBILE DEVICE IS WITHIN PREDEFINED DISTANCE OF PERMITTED LOCATIONS AND ATTEMPTED DECRYPTION OF CRYPTOGRAPHIC DATA
540
STORE INDICATION OF PREAUTHORIZATION
550
TRANSMIT INDICATION OF PREAUTHORIZATION TO MOBILE DEVICE
560
TRANSMIT INDICATION OF PREAUTHORIZATION TO CONTACTLESS CARD
570
END

FIG. 5

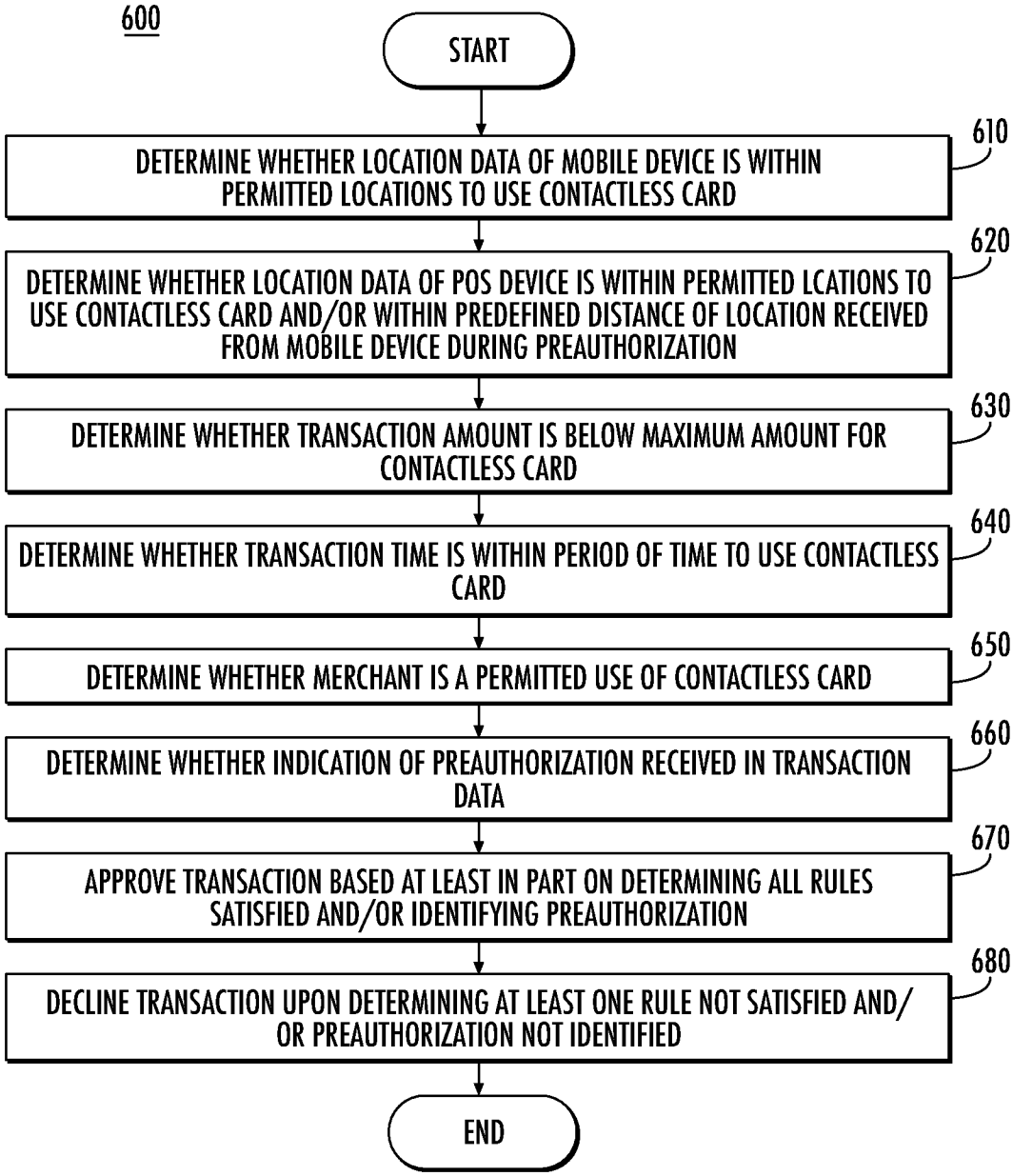

600
START
DETERMINE WHETHER LOCATION DATA OF MOBILE DEVICE IS WITHIN PERMITTED LOCATIONS TO USE CONTACTLESS CARD
610
DETERMINE WHETHER LOCATION DATA OF POS DEVICE IS WITHIN PERMITTED LCATIONS TO USE CONTACTLESS CARD AND/OR WITHIN PREDEFINED DISTANCE OF LOCATION RECEIVED FROM MOBILE DEVICE DURING PREAUTHORIZATION
620
DETERMINE WHETHER TRANSACTION AMOUNT IS BELOW MAXIMUM AMOUNT FOR CONTACTLESS CARD
630
DETERMINE WHETHER TRANSACTION TIME IS WITHIN PERIOD OF TIME TO USE CONTACTLESS CARD
640
DETERMINE WHETHER MERCHANT IS A PERMITTED USE OF CONTACTLESS CARD
650
DETERMINE WHETHER INDICATION OF PREAUTHORIZATION RECEIVED IN TRANSACTION DATA
660
APPROVE TRANSACTION BASED AT LEAST IN PART ON DETERMINING ALL RULES SATISFIED AND/OR IDENTIFYING PREAUTHORIZATION
670
DECLINE TRANSACTION UPON DETERMINING AT LEAST ONE RULE NOT SATISFIED AND/OR PREAUTHORIZATION NOT IDENTIFIED
680
END

FIG. 6

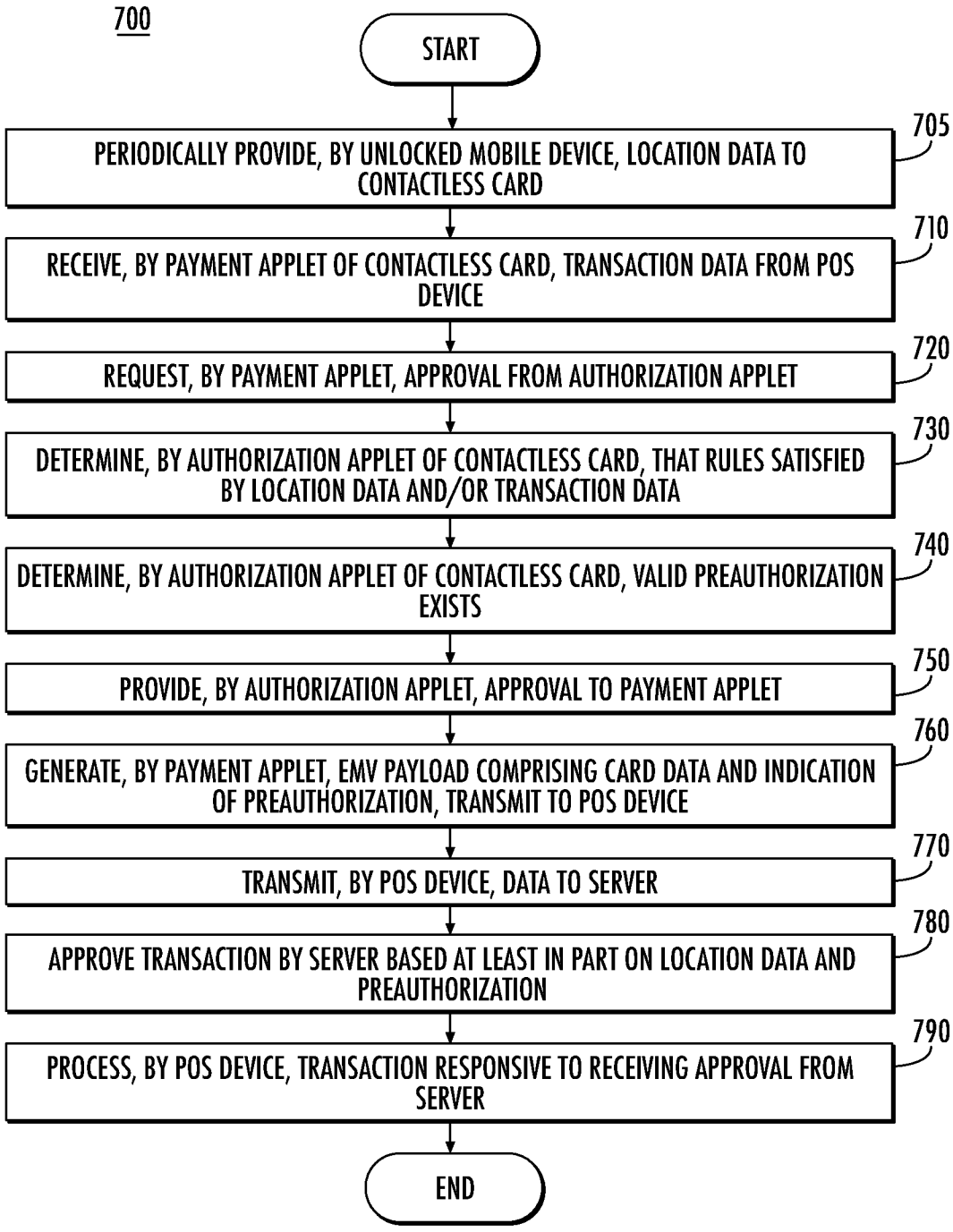

700
START
PERIODICALLY PROVIDE, BY UNLOCKED MOBILE DEVICE, LOCATION DATA TO CONTACTLESS CARD
705
RECEIVE, BY PAYMENT APPLET OF CONTACTLESS CARD, TRANSACTION DATA FROM POS DEVICE
710
REQUEST, BY PAYMENT APPLET, APPROVAL FROM AUTHORIZATION APPLET
720
DETERMINE, BY AUTHORIZATION APPLET OF CONTACTLESS CARD, THAT RULES SATISFIED BY LOCATION DATA AND/OR TRANSACTION DATA
730
DETERMINE, BY AUTHORIZATION APPLET OF CONTACTLESS CARD, VALID PREAUTHORIZATION EXISTS
740
PROVIDE, BY AUTHORIZATION APPLET, APPROVAL TO PAYMENT APPLET
750
GENERATE, BY PAYMENT APPLET, EMV PAYLOAD COMPRISING CARD DATA AND INDICATION OF PREAUTHORIZATION, TRANSMIT TO POS DEVICE
760
TRANSMIT, BY POS DEVICE, DATA TO SERVER
770
APPROVE TRANSACTION BY SERVER BASED AT LEAST IN PART ON LOCATION DATA AND PREAUTHORIZATION
780
PROCESS, BY POS DEVICE, TRANSACTION RESPONSIVE TO RECEIVING APPROVAL FROM SERVER
790
END

FIG. 7

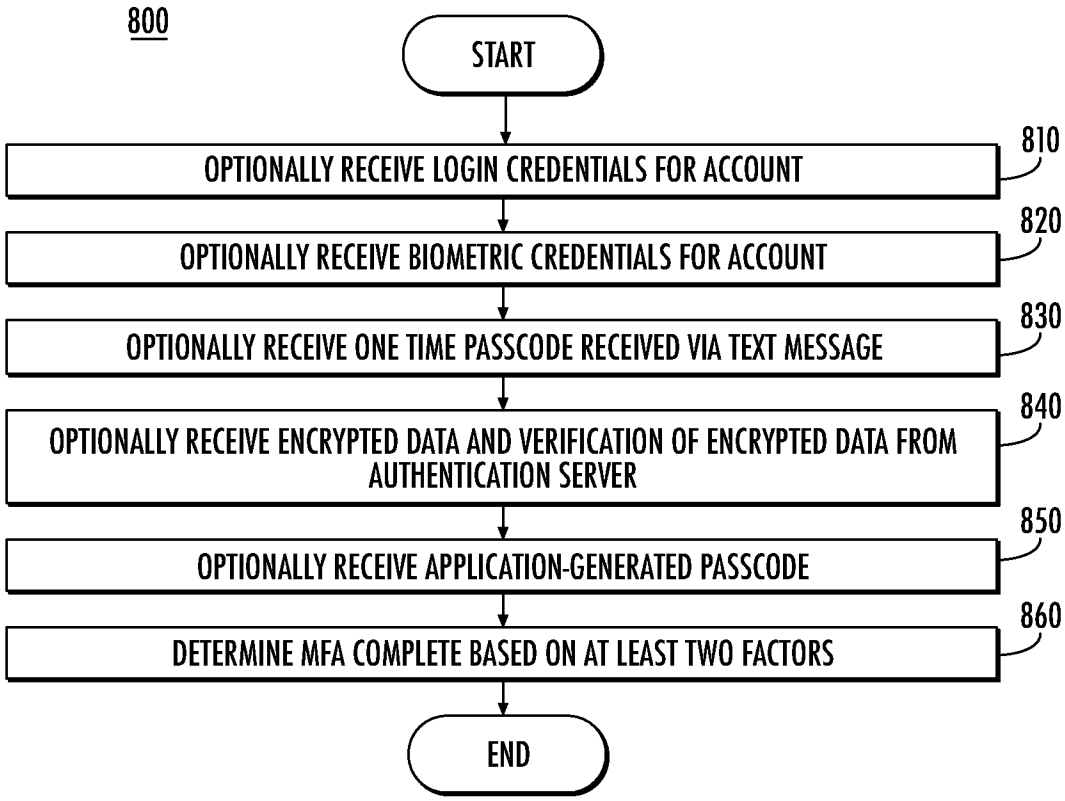

800
START
OPTIONALLY RECEIVE LOGIN CREDENTIALS FOR ACCOUNT
810
OPTIONALLY RECEIVE BIOMETRIC CREDENTIALS FOR ACCOUNT
820
OPTIONALLY RECEIVE ONE TIME PASSCODE RECEIVED VIA TEXT MESSAGE
830
OPTIONALLY RECEIVE ENCRYPTED DATA AND VERIFICATION OF ENCRYPTED DATA FROM AUTHENTICATION SERVER
840
OPTIONALLY RECEIVE APPLICATION-GENERATED PASSCODE
850
DETERMINE MFA COMPLETE BASED ON AT LEAST TWO FACTORS
860
END

FIG. 8

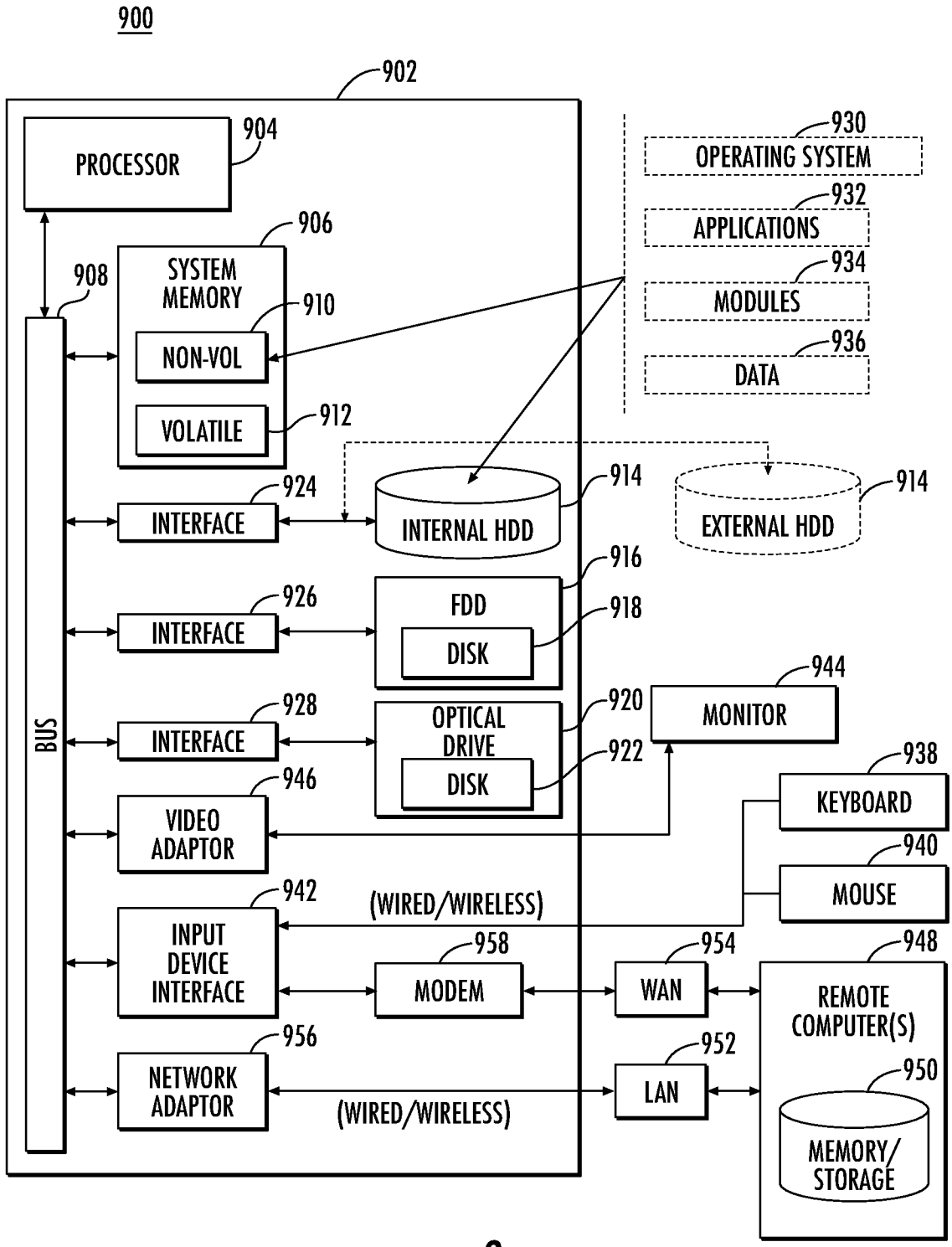

900
902
PROCESSOR
904
SYSTEM MEMORY
906
908
910
NON-VOL
VOLATILE
912
BUS
930
OPERATING SYSTEM
932
APPLICATIONS
934
MODULES
936
DATA
INTERFACE
924
INTERNAL HDD
914
EXTERNAL HDD
914
INTERFACE
926
FDD
916
DISK
918
INTERFACE
928
OPTICAL DRIVE
920
DISK
922
MONITOR
944
KEYBOARD
938
MOUSE
940
VIDEO ADAPTOR
946
(WIRED/WIRELESS)
INPUT DEVICE INTERFACE
942
MODEM
958
WAN
954
REMOTE COMPUTER(S)
948
NETWORK ADAPTOR
956
(WIRED/WIRELESS)
LAN
952
MEMORY/ STORAGE
950

FIG. 9

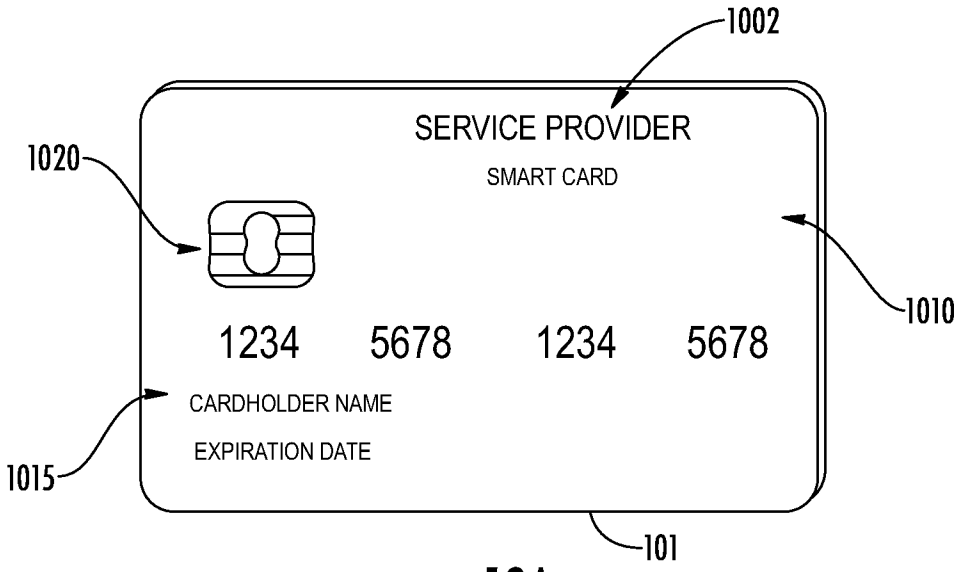

1002
SERVICE PROVIDER
SMART CARD
1020
1010
1234 5678 1234 5678
CARDHOLDER NAME
EXPIRATION DATE
1015
101

FIG. 10A

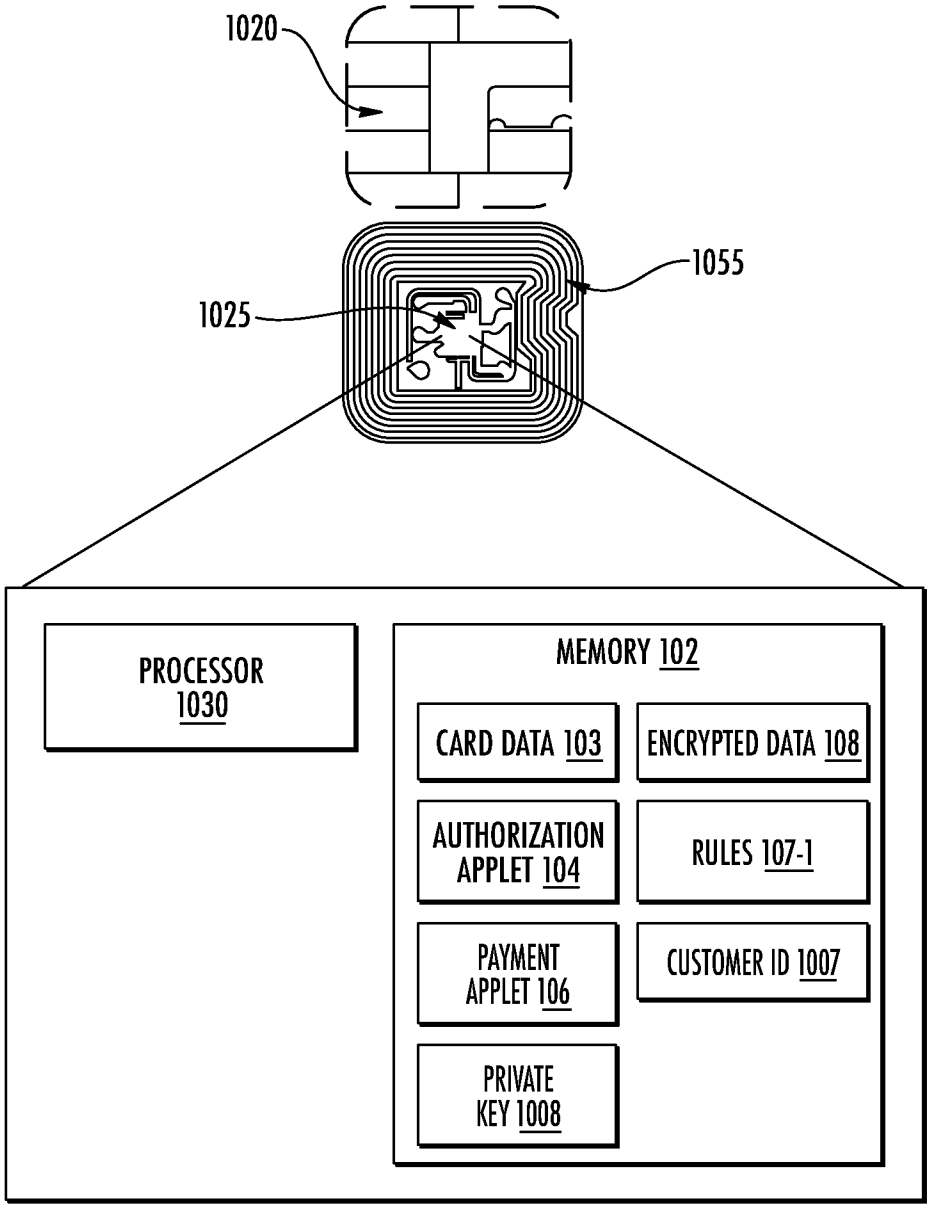

1020
1055
1025
PROCESSOR 1030
MEMORY 102
CARD DATA 103
ENCRYPTED DATA 108
AUTHORIZATION APPLET 104
RULES 107-1
PAYMENT APPLET 106
CUSTOMER ID 1007
PRIVATE KEY 1008

FIG. 10B