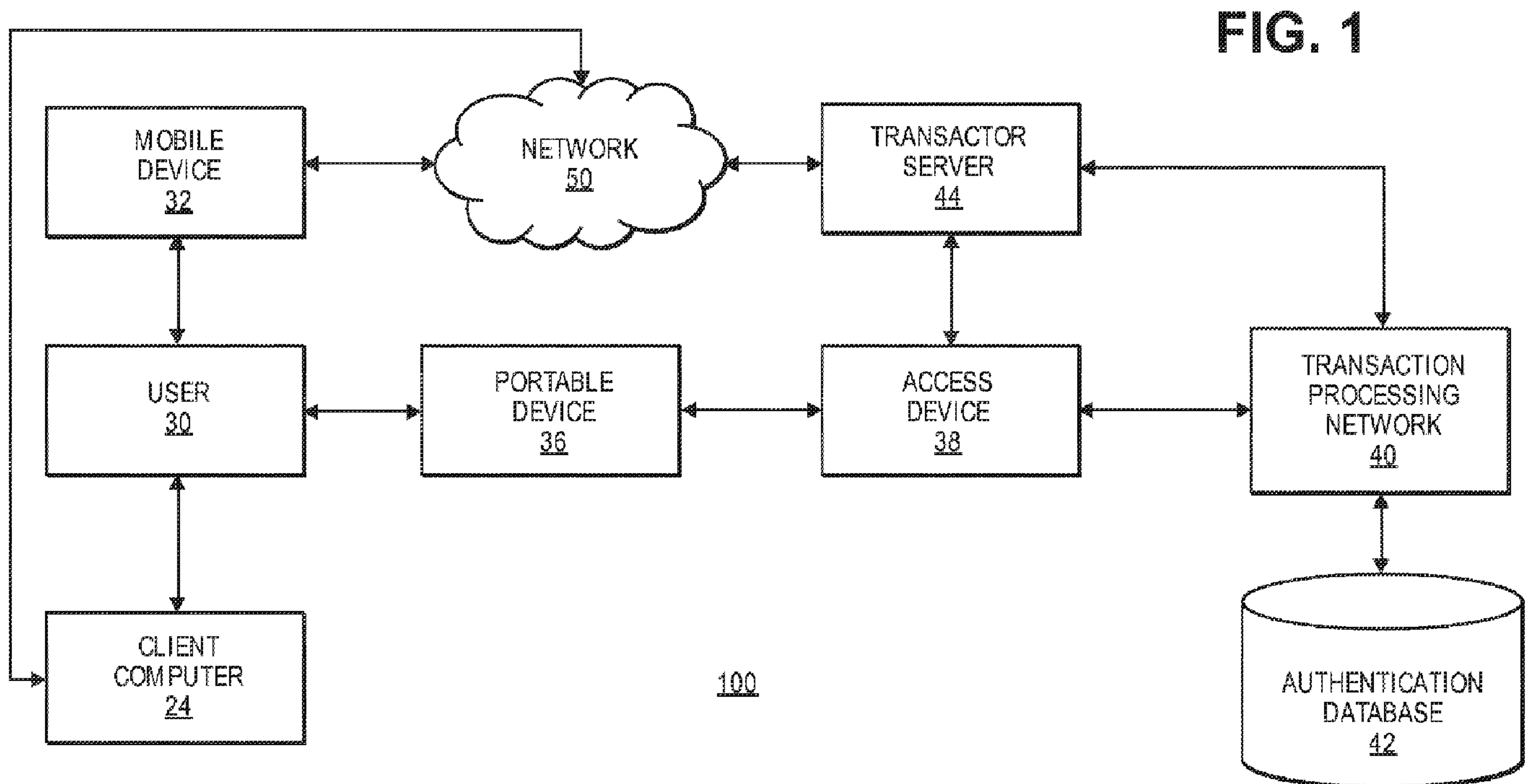




(86) Date de dépôt PCT/PCT Filing Date: 2015/04/29
(87) Date publication PCT/PCT Publication Date: 2015/11/05
(85) Entrée phase nationale/National Entry: 2016/10/17
(86) N° demande PCT/PCT Application No.: US 2015/028365
(87) N° publication PCT/PCT Publication No.: 2015/168334
(30) Priorité/Priority: 2014/05/01 (US61/987,208)

(51) Cl.Int./Int.Cl. *H04L 9/32* (2006.01),
H04W 12/06 (2009.01), *H04W 64/00* (2009.01)
(71) Demandeur/Applicant:
VISA INTERNATIONAL SERVICE ASSOCIATION, US
(72) Inventeur/Inventor:
DIMMICK, JAMES DENE, US
(74) Agent: BERESKIN & PARR LLP/S.E.N.C.R.L.,S.R.L.

(54) Titre : VERIFICATION DE DONNEES A L'AIDE D'UN DISPOSITIF D'ACCES
(54) Title: DATA VERIFICATION USING ACCESS DEVICE



(57) **Abrégé/Abstract:**

An embodiment of the invention is directed to a method comprising receiving, at a server computer, information for a portable device that includes a mobile device identifier and storing, by the server computer, the information for the portable device that includes the mobile device identifier in a database associated with the server computer. The method further comprising receiving,

(57) Abrégé(suite)/Abstract(continued):

by the server computer, transaction data from an access device for a transaction conducted at the access device, determining, by the server computer, from the transaction data that the transaction is associated with the portable device, determining, by the server computer, a location of the access device, determining, by the server computer, a location of a mobile device associated with the mobile device identifier, determining, by the server computer, that the location of the mobile device matches the location of the access device, and marking, by the server computer, the stored information for the portable device as authentication verified.

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

(19) World Intellectual Property
Organization
International Bureau



(10) International Publication Number
WO 2015/168334 A1

(43) International Publication Date
5 November 2015 (05.11.2015)

(51) International Patent Classification:

H04L 9/32 (2006.01) *H04W 64/00* (2009.01)
H04W 12/06 (2009.01)

(21) International Application Number:

PCT/US2015/028365

(22) International Filing Date:

29 April 2015 (29.04.2015)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

61/987,208 1 May 2014 (01.05.2014) US

(71) Applicant: VISA INTERNATIONAL SERVICE ASSOCIATION [US/US]; P.O. Box 8999, M1-11F, San Francisco, California 94128-8999 (US).

(72) Inventor: DIMMICK, James Dene; 835 Catamaran Street, Apt. 2, Foster City, California 94404 (US).

(74) Agents: PACHECO, Raquel et al.; Kilpatrick Townsend & Stockton LLP, Two Embarcadero Center, 8th Floor, San Francisco, California 94111 (US).

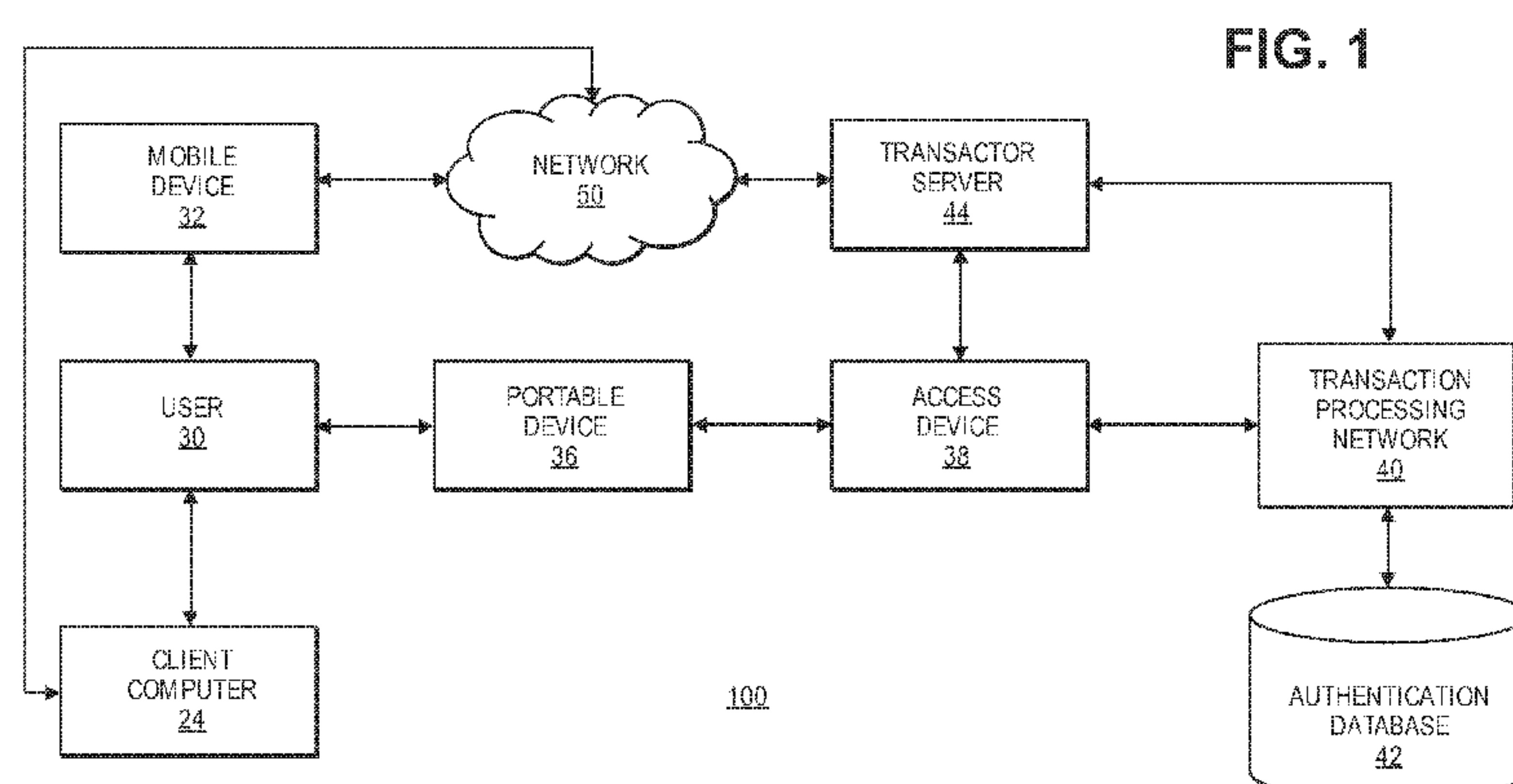
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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))

(54) Title: DATA VERIFICATION USING ACCESS DEVICE



(57) Abstract: An embodiment of the invention is directed to a method comprising receiving, at a server computer, information for a portable device that includes a mobile device identifier and storing, by the server computer, the information for the portable device that includes the mobile device identifier in a database associated with the server computer. The method further comprising receiving, by the server computer, transaction data from an access device for a transaction conducted at the access device, determining, by the server computer, from the transaction data that the transaction is associated with the portable device, determining, by the server computer, a location of the access device, determining, by the server computer, a location of a mobile device associated with the mobile device identifier, determining, by the server computer, that the location of the mobile device matches the location of the access device, and marking, by the server computer, the stored information for the portable device as authentication verified.

WO 2015/168334 A1

DATA VERIFICATION USING ACCESS DEVICE

5

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application is a non-provisional of and claims priority to U.S. provisional application no. 61/987,208, filed on May 1, 2014, which is herein incorporated by
10 reference in its entirety for all purposes.

BACKGROUND

[0002] In conventional physical or proximity transactions, there are many ways to verify that a user utilizing a portable device to make a transaction is indeed the user
15 authorized to use that portable device. For example, a user may use a portable device that has been securely issued by their bank, such as a credit card with a mag stripe or a debit card with a contactless chip, to interact with an access device at a merchant to make a payment. The data from the mag stripe and a physical
signature (for example) can be used to authenticate the user as the authorized user
20 of the portable device. Or the contactless chip on the portable device can exchange data with the access device to provide further authentication and security. This data can additionally be sent to an authorization server such as at a payment processing network or issuer to compare it with stored data to authenticate the user or portable device.

25 **[0003]** Remote transactions are becoming more and more common place. There are a number of security and usability issues with remote transactions that do not exist in physical or proximity transactions. For example, a user may use his portable device, such a credit card with a mag stripe or a debit card with a contactless chip, to make a purchase at a merchant via the merchant's website. Instead of swiping the
30 card at an access device so that the mag stripe or chip on the card can interact with the access device to exchange information, the user simply inputs his account number and expiration date (for example). Since there is no physical or proximity

interaction with the portable device, traditional means of providing authentication and additional security are not effective.

[0004] There are some solutions that have emerged to address issues of authentication in remote transactions. One example is 3D Secure which allows entities such as Visa, MasterCard, and American Express to provide additional means to authenticate a portable device. For example, a password based method may be used which requires a user to register a password and then to input the password during each remote purchase transaction. This can be burdensome to the user whose payment experience may be interrupted to setup and register a password, and then to remember and enter the password for every remote transaction. Such a solution can also be expensive for a merchant or other entity to implement and maintain. Moreover, this solution can introduce other security issues. For example, password based solutions typically require a pop-up window to appear during the user's payment transaction. It may be difficult for the user to distinguish between a legitimate pop up window and a fraudulent phishing site. An inline frame may be used instead of a pop-up to reduce user confusion, but this may make it even harder for a user to verify that the inline frame is genuine. In addition, a user may not be allowed to proceed with a payment until they have registered a 3D Secure password. If a user does not want to risk providing the information during the purchase (or cannot remember the password), the user may have to cancel the transaction. Furthermore, many mobile browsers may not support inline frames or pop-ups and thus, the security feature may not work correctly on many mobile devices.

[0005] A more secure and effective way to authenticate users and portable devices is needed.

BRIEF SUMMARY

[0006] Embodiments of the invention are directed to systems, apparatuses, and methods to authenticate users and portable devices.

[0007] One embodiment of the invention is directed to a method comprising receiving, at a server computer, information for a portable device that includes a mobile device identifier, and storing, by the server computer, the information for the

portable device that includes the mobile device identifier in a database associated with the server computer. The method further comprising receiving, by the server computer, transaction data from an access device for a transaction conducted at the access device, determining, by the server computer, from the transaction data that the transaction is associated with the portable device, determining, by the server computer, a location of the access device, determining, by the server computer, a location of a mobile device associated with the mobile device identifier, determining, by the server computer, that the location of the mobile device matches the location of the access device, and marking, by the server computer, the stored information for the portable device as authentication verified.

[0008] Another embodiment of the invention is directed to a server computer comprising a processor and a non-transitory computer readable medium coupled with the processor. The computer readable medium comprising instructions executable by the processor, the instructions comprising receiving information for a portable device that includes a mobile device identifier and storing the information for the portable device that includes the mobile device identifier in a database associated with the server computer. The instructions further comprising receiving transaction data from an access device for a transaction conducted at the access device, determining from the transaction data that the transaction is associated with the portable device, determining a location of the access device, determining a location of a mobile device associated with the mobile device identifier, determining that the location of the mobile device matches the location of the access device, and marking the stored information for the portable device as authentication verified.

[0009] Another embodiments of the invention is directed to a computer apparatus comprising a processor and a non-transitory computer readable medium coupled with the processor. The computer readable medium comprising instructions executable by the processor, the instructions comprising sending information for a portable device that includes a mobile device identifier, to a server computer wherein the server computer stores the information for the portable device that includes the mobile device identifier in a database associated with the server computer, receiving transaction data for a transaction conducted using the portable device, and sending the transaction data to a server computer wherein the server computer determines a location of an access device associated with the mobile device identifier, determines

a location of the mobile device associated with the mobile device identifier, determines that the location of the mobile device identifier matches the location of the access device, and marks stored information in the authentication database as authentication verified.

5 **[0010]** These and other embodiments of the invention are further described below.

BRIEF DESCRIPTION

[0011] FIG. 1 shows a block diagram of a system according to embodiments of the invention.

10 **[0012]** FIG. 2 shows a block diagram of an exemplary database according to embodiments of the invention.

[0013] FIG. 3 shows a block diagram of an exemplary server computer according to embodiments of the invention.

15 **[0014]** FIG. 4 shows a flowchart of a method according to embodiments of the invention.

[0015] FIG. 5 shows a flowchart of a method according to embodiments of the invention.

[0016] FIG. 6 shows a flowchart of a method according to embodiments of the invention.

20 **[0017]** FIG. 7 shows an exemplary device according to embodiments of the invention.

[0018] FIG. 8 shows an exemplary computer system according to embodiments of the invention.

DETAILED DESCRIPTION

25 **[0019]** Embodiments of the invention are directed to systems, apparatuses, and methods to authenticate portable devices. For example, a user may provide information to register a portable device for authentication of remote transactions (e.g., primary account number (PAN), expiry date for the portable device, a card verification value (CVV), etc.). The user may also provide a mobile device identifier
30 (e.g., a mobile phone number). The user may provide this information to a

transactor (e.g., merchant) during a remote, physical, or proximity transaction or a user may utilize an electronic wallet (e.g., Amazon wallet, Google wallet, etc.) and provide information in the electronic wallet.

[0020] The information provided by the user may be sent to a transaction processing network. The transaction processing network may store the information in an authentication database and indicate that the stored information is not yet authentication verified. The next time the user conducts a physical or proximity transaction at an access device associated with a transactor/merchant, the access device or transactor server associated with the access device may send transaction data to a transaction processing network. The transaction processing network may determine from the transaction data that the transaction is associated with a portable device that has been registered to be authentication verified but that is not yet authentication verified. The transaction processing network may determine that the location of the access device and the location of a mobile device associated with the mobile device identifier match and thus, verify that the information associated with the portable device is authentic. The transaction processing network may mark the stored information for the portable device as authentication verified. The next time the user conducts a remote transaction using the portable device, the system can confirm that the portable device is authentication verified and utilize a CAVV, digital certificate, or other means during the transaction to provide additional security for the remote transaction.

[0021] Other embodiments of the invention allow for using messages sent to a user's mobile device and using tokens to verify authentication of the portable device.

[0022] Embodiments of the invention provide novel ways to authenticate a portable device for remote transactions where conventional methods are not effective. In contrast to conventional systems for authenticating remote transactions, such as password based 3D Secure solutions, embodiments of the invention do not require a cumbersome process by the user, or implementation and maintenance of an expensive system for the merchant or other entities in the system. By matching up transaction data and location information from a physical or proximity transaction with stored registration information for a portable device (for example), embodiments of the invention provide for a more secure and efficient systems for authenticating a

portable device and providing security means for remote transactions, without imposing burdensome methods on users, merchants, and other entities involved in remote transactions.

[0023] I. Exemplary System

5 **[0024]** FIG. 1 shows an exemplary system 100 according to embodiments of the invention. Although some of the entities and components in FIG. 1 may be depicted as separate, in some instances, one or more of the components may be combined into a single device or location (and vice versa). Similarly, although certain functionality may be described as being performed by a single entity or component
10 within the system, the functionality may in some instances be performed by multiple components and/or entities (and vice versa). Moreover, for simplicity, only one user, one mobile device, one client computer, one portable device, one access device, etc. are shown in FIG. 1. It is understood that the system 100 may comprise multiple users, mobile devices, client computers, portable devices, access device, etc.
15 Communication between entities and components may comprise the exchange of data or information using electronic messages and any suitable electronic communication medium and method, as described below.

[0025] The system 100 includes a user 30. The user 30 may be an individual, or an organization such as a business, that is capable of conducting transactions such
20 as purchasing goods or services, transferring money, etc. The user 30 may use a portable device 36 to conduct a transaction. For example, a portable device 36 may be a payment card such as a credit card, debit card, or a prepaid card, used to conduct a transaction, such as to provide payment information to a merchant.

[0026] The portable device 36 may be in any suitable form. For example suitable
25 portable devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, magnetic stripe cards, keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of portable devices include cellular phones, personal digital assistants (PDAs), pagers, payment cards, security
30 cards, access cards, smart media, transponders, 2-D barcodes, an electronic or digital wallet, and the like. Portable devices may also include wearable devices such as smart watches, fitness bands, ankle bracelets, rings earrings, etc. If the portable

device is in the form of a debit, credit, or smartcard, the portable device may also optionally have features such as magnetic stripes and/or computer chips. Such devices can operate in either a contact (e.g., physical) or contactless (e.g., proximity) mode.

- 5 **[0027]** A portable device 36 in the form of a card may comprise a plastic substrate. In some embodiments, a contactless element for interfacing with an access device 38 may be present on, or embedded within, the plastic substrate. Portable device information such as an account number, expiration date, and/or a user name may be printed or embossed on the card. A magnetic stripe may also be on the plastic
- 10 substrate. In some embodiments, the portable device 36 may comprise a microprocessor and/or memory chips with user data stored in them. In some embodiments, both a magnetic stripe and a contactless element may be in the portable device 36. In some embodiments, either a magnetic stripe or a contactless element may be present in the portable device 36.
- 15 **[0028]** A user 30 may operate a mobile device 32 to communicate with a transactor server 44. The mobile device 32 may be may comprise any electronic device that may be transported and operated by a user, which may also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network
- 20 (e.g. 3G, 4G or similar networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network (e.g., network 50) such as the Internet or a private network.

- [0029]** Examples of mobile devices include mobile phones (e.g. cellular phones), PDAs, tablet computers, net books, laptop computers, personal music players, hand-
- 25 held specialized readers, etc. A mobile device 32 may comprise any suitable hardware and software for performing such functions, and may also include multiple devices or components (e.g. when a device has remote access to a network by tethering to another device - i.e. using the other device as a modem – both devices taken together may be considered a single mobile device). A mobile device 32 may
- 30 also comprise a verification token in the form of, for instance, a secured hardware or software component within the mobile device 32 and/or one or more external components that may be coupled to the mobile device 32.

[0030] The mobile device 32 may also be used as a portable device in some embodiments of the invention. For example, the mobile device 32 may contain technology to be used to conduct transactions, such as at an access device 38 to make a payment by placing the device near the access device 38. Portable device
5 information can be transferred to the access device via short range communication technology such as NFC (Near Field Communication) technology. The mobile device 32 may utilize an electronic wallet or digital wallet to conduct such a transaction. An electronic wallet or digital wallet can store user profile information, payment information, bank account information, and/or the like and can be used in a
10 variety of transactions, such as but not limited to eCommerce, social networks, money transfer/ personal payments, mobile commerce, proximity payments, gaming, and/or the like for retail purchases, digital goods purchases, utility payments, purchasing games or gaming credits from gaming websites, transferring funds between users, and/or the like. An electronic wallet may comprise any suitable
15 software that provides front end functionality of the electronic wallet to the user 30. For example, the electronic wallet may be embodied as a software application downloadable by a computer apparatus or mobile device 32 (e.g., a mobile phone). In some instances, the electronic wallet may provide a user interface (such as a series of menus or other elements) that allows the user 30 to manage his electronic
20 wallet(s). In some embodiments, the electronic wallet may store data in a computer readable memory for later use, such as user 30 preferences or identifiers associated with funding sources added to the electronic wallet.

[0031] The client computer 34 may be a personal computer or the like. The user 30 may use the client computer 34 to conduct transactions such as conducting a
25 payment transaction on a transactor (e.g., merchant) website via a network 50 (e.g., the internet) and a transactor server 44.

[0032] The transactor server 44 may be a server computer associated with a transactor such as a merchant. A transactor may refer to an entity that engages in transactions and can sell goods or services to a user. The terms “transactor” and
30 “merchant” may be used interchangeably throughout this application.

[0033] As used herein, a server computer is typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a

minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server.

[0034] The access device 38 may be any suitable device for communicating with a transaction processing network 40, and for interacting with a portable device 36 or mobile device 32. An access device 38 may be in any suitable form. Some examples of access devices include POS devices, cellular phones, PDAs, personal computers (PCs), tablet PCs, hand-held specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, Websites, and the like.

An access device 38 may use any suitable contact or contactless mode of operation to send or receive data from, or associated with, a portable device 36 and/or a user mobile device 32. In some embodiments, where an access device 38 may comprise a POS terminal, any suitable POS terminal may be used and may include a reader, a processor, and a computer-readable medium. A reader may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include radio frequency (RF) antennas, optical scanners, bar code readers, or magnetic stripe readers to interact with a portable device 36 and/or mobile device 32. The access device 38 may generally be located in any suitable location. For example, in a physical or proximity transaction situation, the access device 38 may be located at the location of a transactor/merchant. In a remote transaction situation the access device 38 may be a computer, such a transactor server 44 (e.g., a merchant server computer), accessible by a user 30 using a website or application over a network 50 such as the internet or an application on a mobile device or client computer. In physical or proximity transactions, the access device 38 may be coupled with a transactor server 44.

[0035] The transaction processing network 40 may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. For example, the transaction processing network 40 may comprise a server computer, coupled to a network interface (e.g. by an external communication interface), and a database(s) of information. The server computer may comprise a processor and a non-transitory computer readable medium coupled with the processor. The non-transitory

computer readable medium may comprise instructions executable by the processor, the instructions comprising functionality described herein.

[0036] An exemplary server computer 400 is shown in FIG. 3. The exemplary server computer 400 is illustrated as comprising a plurality of hardware and software modules (401-413). It should be appreciated that this is provided for illustration purposes only, and each of the modules and associated functionality may be provided and/or performed by the same or different components. Exemplary server 400 may for example, perform some of the relevant functions and steps described herein with reference to the transaction processing network 40 through the use of any suitable combination of software instructions and/or hardware configurations. It should be noted that although FIG. 3 illustrates all of the modules located on a single device, the disclosure is not meant to be so limited. Moreover, a system for implementing the functionality described herein may have additional components or less than all of these components. Additionally, some modules may be located on other devices such as a remote server or other local devices that are functionally connected to the server computer component(s).

[0037] The exemplary server computer 400 is shown as comprising data processor 401, network interface 403, and computer readable medium 413. The computer readable medium may comprise a number of modules (405-411). The data management module 405 may be configured to manage data received by and transmitted from the transaction processing network 40 (e.g., data from an authorization request message, and authorization response message, data related to a mobile device, data related to a portable device, etc.). The location determination and comparison module 407 may be configured to determine location information for various components of the system 100 and compare locations of various components in the system 100 to determine if they are near each other in location. The authorization module 409 may be configured to perform transaction authorization functions (e.g., authorize a payment transaction, etc.). The clearing and settlement module 411 may be configured to perform transaction clearing and settlement functions.

[0038] An exemplary transaction processing network 40 may include VisaNet™ etc. Transaction processing networks such as VisaNet™ are able to process credit

card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services. The Transaction processing network 40 may use any suitable wired or wireless network, including the Internet. Although many of the data processing functions and features of some embodiments may be present in the transaction processing network 40 (and a server computer therein), it should be understood that such functions and features could be present in other components such as an issuer computer, and need not be present in the transaction processing network 40, or a server computer therein.

[0039] The transaction processing network 40 may be coupled with an authentication database 42. The authentication database 42 may store authentication information for portable consumer devices. FIG. 2 shows an exemplary layout of authentication database 42. The authentication database 42 may have a number of fields such as the identifier field and fields shown as references numbers 221-229. For example, reference number 221 may be a unique identifier. An example of a unique identifier may be a primary account number (PAN) such as a sixteen digit PAN (e.g., 4003 3385 5518 2312). The other fields 222-229 may store further information associated with each unique identifier. For example, the authentication database 42 may store account numbers (e.g., primary account number (PANs)), mobile phone numbers, CVVs, Cardholder Authentication Verification Values (CAVV), digital certificates, tokens, other identification information, etc. Identification information may include any suitable information associated with an account (e.g. a payment account and/or portable device associated with the account). Such information may be directly related to the account or may be derived from information related to the account. Examples of account information may include a PAN, user name, expiration date, CVV (card verification value), dCVV (dynamic card verification value), CVV2 (card verification value 2), CVC3 card verification values, etc. CVV2 is generally understood to be a static verification value associated with a portable/payment device. CVV2 values are generally visible to a user (e.g., a consumer), whereas CVV and dCVV values are typically embedded in memory or authorization request messages and are not

readily known to the user (although they are known to the issuer and transaction processor).

[0040] The entities represented in FIG. 1 may communicate using any suitable communications mediums and methods. Suitable communications channels may be present directly between two entities such as a transaction processing network and a transactor (e.g., merchant) or issuer computer, or may include a number of different entities. Any suitable communications protocols may be used for generating a communications channel. A communication channel may in some instance comprise a secure communication channel, which may be established in any known manner, including the use of mutual authentication and a session key and establishment of an SSL session. However, any method of creating a secure channel may be used. By establishing a secure channel, sensitive information related to a portable/payment device (such as account number, CVV values, expiration dates, etc.) may be securely transmitted between the two entities to facilitate a transaction.

[0041] As used herein, short range communication or short range wireless communication may comprise any method of providing short-range contact or contactless communications capability, such as RFID, Bluetooth™, infra-red, or other data transfer capability that can be used to exchange data between a portable device, mobile device, etc., and an access device. In some embodiments, short range communications may be in conformance with a standardized protocol or data transfer mechanism (e.g., ISO 14443/NFC). Short range communication typically comprises communications at a range of less than 2 meters. In some embodiments, it may be preferable to limit the range of short range communications (e.g. to a range of less than 1 meter, less than 10 centimeters, or less than 2.54 centimeters) for security, technical, and/or practical considerations. For instance, it may not be desirable for an access device (e.g., POS terminal) to communicate with every portable device that is within a 2 meter radius because each of those portable devices may not be involved in a transaction, or such communication may interfere with a current transaction involving different financial transaction devices. Typically the portable device or the access device also includes a protocol for determining resolution of collisions (i.e. when two portable devices are communicating with the access device simultaneously). The use of short range communications may be

used when the transactor (e.g., merchant) and the user are in close geographic proximity, such as when the consumer is at the merchant's place of business.

[0042] As used herein, transaction data/information or purchase/payment transaction data/information may refer to any information corresponding to or describing purchases, orders, invoices, payments involving goods, items, services, and/or the like, and may include, but is not limited to, a purchase amount, a merchant identifier, description code (e.g., NAICS: North American Industry Classification System) associated with purchased items, cost of purchased items, and transactions as well as descriptions of purchased items, purchase dates, purchase amounts, indications of payments accounts used, indications of whether purchases were made online, confirmation numbers, order numbers, cancellation numbers, shipment status updates (e.g., order being processed, shipped, delivered, on back order, etc.), delivery tracking numbers, cancellation notices, updates, and/or the like.

[0043] II. Exemplary Transactions

[0044] In typical physical or proximity payment, a user 30 may conduct a transaction using a portable device 36 (e.g., credit card, debit card, etc.) at an access device 38 such as a Point-of-Sale (POS) terminal at a merchant (e.g., grocery store). The user 30 may present his portable device 36 to the access device 38 to pay for an item or service. The portable device 36 and the access device 38 may interact such that information from the portable device (e.g., account identifier, verification value(s), expiration date, etc.) is received by the access device (e.g., via contact or contactless interface). For example, if the transaction is a physical payment transaction, the user 30 may slide his portable device 36 (e.g., credit card) through a slot on the POS terminal or make other physical contact between the portable device 36 and access device 38 to exchange portable device information and other data with the access device 38. If the transaction is a proximity payment, the user 30 may wave or place his portable device 36 near the access device 38 to exchange portable device information and other data with the access device 38.

[0045] The access device 38 or a transactor server 44 associated with the access device 38 may generate an authorization request message that includes the information received from the access device (e.g., information corresponding to the

portable device 36) along with additional transaction information (e.g., a transaction amount, merchant specific information, etc.).

[0046] An authorization request message may be an electronic message that is sent to a transaction processing network and/or an issuer of a payment card to request authorization for a transaction. An authorization request message according to some embodiments may comply with ISO 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a consumer using a portable device or payment account. The authorization request message may include an issuer account identifier that may be associated with a portable/payment device or payment account. An authorization request message may also comprise additional data elements corresponding to “identification information” including, by way of example only: a service code, a CVV (card verification value), a dCVV (dynamic card verification value), an expiration date, etc. An authorization request message may also comprise “transaction information,” such as any information associated with a current transaction, such as the transaction amount, merchant identifier, merchant location, etc., as well as any other information that may be utilized in determining whether to identify and/or authorize a transaction.

[0047] The access device 38 or a transactor server 44 electronically transmits this information to an acquirer (e.g., a computer associated with the acquirer). An acquirer may typically refer to a business entity (e.g., a commercial bank or financial institution) that has a business relationship with a particular merchant or similar entity. Some entities can perform both issuer and acquirer functions. The acquirer may then receive, process, and forward the authorization request message to a transaction processing network 40 (e.g., a server computer associated with a transaction processing network 40), such as Visanet, for authorization. In the alternative the access device 38 or transactor server 44 may send the authorization request message to the transaction processing network 40 without the acquirer.

[0048] The transaction processing network 40 may then send the authorization request message to an issuer associated with the portable device 36. An issuer may typically refer to a business entity (e.g., a bank or other financial institution) that maintains financial accounts for the user 30 and often issues a portable device 36 such as a credit or debit card to the user 30. The issuer may then generate an

authorization response message indicating whether or not the transaction is authorized.

[0049] An authorization response message may be an electronic message reply to an authorization request message generated by an issuing financial institution or a transaction or payment processing network. The authorization response message may include, by way of example only, one or more of the following status indicators: Approval -- transaction was approved; Decline -- transaction was not approved; or Call Center -- response pending more information, merchant must call the toll-free authorization phone number. The authorization response message may also include an authorization code, which may be a code that a credit card issuing bank returns in response to an authorization request message in an electronic message (either directly or through the transaction processing network) to the merchant's access device (e.g. POS equipment) that indicates approval of the transaction. The code may serve as proof of authorization.

[0050] The authorization response message is then sent to the transaction processing network 40 which may then forward it to the transactor access device 38 (optionally via the acquirer or via the transactor server 44).

[0051] In a typical remote transaction, a user 30 may wish to make an online purchase (for example) with a transactor/merchant over the Internet. In this case a user may not use his portable device 36 to interact with an access device 38 as described above. Instead he may enter his payment information via a website associated with the merchant. The transaction may go through the transactor server 44 associated with the merchant, to the transaction processing network (optionally through the acquirer) and then proceeds similar to that which described above for a typical physical and proximity transactions.

[0052] At the end of the day, or at some other predetermined period of time, a clearing and settlement process can occur, via the above-described acquirer or issuer (or their respective computers).

[0053] III. Exemplary Authentication Methods

[0054] FIG. 4 shows a flowchart of an exemplary method according to embodiments of the invention. A user 30 may provide information to register a

portable device for authentication for remote transactions. For example, a user may provide this information to a transactor (e.g., merchant) during a remote, physical, or proximity transaction or a user may utilize an electronic wallet (e.g., Amazon wallet, Google wallet, etc.) and provide information in the electronic wallet. The user 30
5 may provide information that includes his portable device identifier (e.g., an account number associated with his portable device such as a primary account number (PAN)), an expiry date for the portable device, a card verification value (CVV), etc. The user may also provide a mobile phone identifier (e.g., a mobile phone number, SIM card number, device ID number, etc.).

10 **[0055]** The information for the portable device 36 may be sent from the merchant/transactor server 44 to the transaction processing network 40. A server computer at the transaction processing network 40 may receive the information for the portable consumer device that includes the mobile device identifier (202). The server computer at the transaction processing network 40 may store the information
15 for the portable device 36 that includes the mobile device identifier (204) in an authentication database 42 associated with the transaction processing network 40 and indicate that the stored information is not yet authentication verified. As shown in FIG. 2 the server computer at the transaction processing network 40 may store a unique identifier associated with the portable device 36 (221), a mobile identifier
20 (222), an indication whether the portable device is authentication verified (223), among other information (e.g., 224-229) received from the user 30 or other entities/information.

[0056] At a later point in time, the user 30 may conduct a physical or proximity transaction at an access device 38 (e.g., a POS terminal) using the portable device
25 36. For example, the user 30 may present his portable device 36 to the access device 38 (e.g., POS terminal) to pay for an item or service by swiping the portable device 36 in a slot in the POS terminal by placing the portable device 36 near the POS terminal. The access device 38 or a transactor server 44 associated with the access device 38 may generate an authorization request message that includes the
30 information received from the access device 38 (e.g., information corresponding to the portable device 36) along with additional transaction information (e.g., a transaction amount, merchant specific information, etc.), collectively referred to herein as “transaction data.”

[0057] The access device 38 or transactor server 44 may then electronically transmit the authorization request message to the transaction processing network 40 (directly or through an acquirer as explained above). The transaction processing network 40 (e.g., a server computer at the transaction processing network 40) may receive the authorization request message with transaction data for the transaction (206).

[0058] The transaction processing network 40 may then send the authorization request message to the issuer associated with the portable device 36. The issuer may then generate an authorization response message indicating whether or not the transaction is authorized. The authorization response message is then sent to the transaction processing network 42 which may then forward it to the merchant (optionally via the acquirer). This may be all done before, during, or after the following method.

[0059] The transaction processing network 40 determines from the transaction data in the authorization request message, that the transaction is associated with a portable device 36 (208) that has been stored in the authentication database 42 and has not yet been authenticated. For example, the transaction processing network 40 may compare a unique portable device identifier, such as a PAN, included in the authorization request message, with a list of portable device identifiers stored in the authentication database 42. If there is a match between the portable device identifier and a portable device identifier in the authentication database 42 and a field associated with the portable device identifier indicates that the portable device is not yet authentication verified, the transaction processing network 40 can then proceed with authentication verification.

[0060] The server computer at the transaction processing network 40 may then determine a location of the access device 38 (210) that sent the authorization request message. The location of the access device 38 may be determined in many different ways. For example, the server computer at the transaction processing network 40 can use information included in the authorization request message such as the merchant identification and location information to determine the location of the access device 38. The information itself may contain location information, e.g., a field in the authorization request message may contain location information such as

Target store Albany, California 94706. Or the information may contain a particular merchant store identifier such as Target store number 12345 and the transaction processing network may look up information for this particular store number to get the location of the store. In other embodiments, the access device 38 may have
5 similar capabilities as the mobile device and may have a location determination module such as a GPS module. The location of the access device 38 can then be provided to the server computer.

[0061] The server computer at the transaction processing network 40 may then use the mobile identifier stored in the authentication database 42 to determine a location
10 of a mobile device 32 associated with the mobile identifier (212). The location of the mobile device 32 may be determined in many ways. For example, the server computer at the transaction processing network 40 may use GPS, signal tower cell strength, or other location technology to determine a location of the mobile device 32. In some embodiments, the server computer may determine the location of the
15 mobile device 32 only in response to receiving the authorization request message. In other embodiments, the server computer may periodically contact the mobile device 32 (i.e., "ping" the mobile device) to determine its location and this location may be stored in a database. Such embodiments have advantages over the former
20 embodiments, since the mobile device may not always be accessible when the user conducts a transaction. By periodically contacting the phone, a recent location will always be present.

[0062] In another example, the server computer can send a message (e.g., via SMS, MMS, email, etc.) to the mobile device 32 using the mobile device identifier to verify that the user 30 is making or recently made a purchase at that particular
25 merchant. For example, the server computer can send a text or email message asking the consumer "Did you just make a purchase at Target for \$25.23?" Or, the server computer can send a challenge question asking the user "Did you make a purchase today at Target for \$25, \$30, or \$45?" The user may respond with an answer. If the user does not respond, responds that he did not make the purchase,
30 or responds incorrectly, the process will end and the portable device 36 will remain unverified.

[0063] If the server computer at the transaction processing network 40 determines a location of the mobile device 32 via location technology or receives a response indicating that the user did make the purchase, the server computer can confirm the location of the mobile device 32. The server computer at the transaction processing network 40 may determine whether the location of the access device 38 matches the location of the mobile device 32 (214) by comparing the location of each. For example, the location of the access device 38 may be Target Albany, CA 94706 and the location of the mobile device 32 may be near the Target Albany 94706 (e.g., within a predetermined distance from the location of the access device 38 such as .25 miles). Or, the location of the access device 38 may be Target Albany, CA 94706 and the transaction processing network 40 may have confirmed that the user made a purchase with the portable device 36 at the Target Albany, CA 94706. In some embodiments, the location of the mobile device 32 and the location of the access device 38 can be converted to latitude and longitude coordinates, and the coordinates of the mobile device 32 and the access device 38 may be compared to determine if they are co-located.

[0064] If the locations match, the server computer at the transaction processing network 40 may mark the stored information for the portable device 36 as authentication verified in the authentication database 42 (216). The transaction processing network 40 may also generate a digital certificate to indicate that the portable device 36 is authentication verified and may store the digital certificate in the authentication database 42. The transaction processing network 40 may also generate a verification value such as an AAV (Accountholder Authentication Value) or a CAVV (Cardholder Authentication Verification Value) and may store the value in the authentication database 42. Such values may be cryptograms generated at least in part of the portable device identifiers. If the location of the access device 38 and the location of the portable device 36 do not match, the authentication process ends and the portable device 36 will remain unverified.

[0065] If the portable device 36 is marked as authentication verified in the authentication database 42, then the next time the user 30 uses the portable device 36 in a remote transaction, the remote transaction can proceed as an authentication verified transaction. For example, the user 30 may wish to make a remote purchase transaction with a merchant/transactor via the merchant's website over the internet

or via an application installed on a mobile device 32 or client computer 34. The transaction environment may include mobile internet, mobile application (app), MOTO, and even an in-store environment where the user 30 interacts with the store via Airdrop, WIFI, peer-to peer wireless, etc. The user 30 may enter his portable
5 device information (and other information) using a keyboard or other means on his client computer 34 or mobile device 32. Once the user 30 enters the information, the transactor server 44 associated with the merchant website, receives the information and generates an authorization request message that includes transaction data including the information received from the user 30.

10 **[0066]** In an alternative embodiment of the invention, the access device 38 or transactor server 44 associated with the access device 38 may generate a message to send transaction data to the transaction processing network 40 directly, before generating an authorization request message, to request information about whether the portable device 36 is authentication verified. The transactor server 44 may send
15 message with the transaction data to the transaction processing network 40.

[0067] A server computer at the transaction processing network 40 receives the transaction data for the remote transaction. The server computer at the transaction processing network 40 determines whether the remote transaction is associated with a portable device 36 that is stored in the authentication database 42. For example,
20 the server computer at the transaction processing network 40 may compare a portable device identifier included in the transaction data against a list of portable device identifiers stored in an authentication database 42. If there is a match between the portable device identifier included in the transaction data and a portable device identifier in the authentication database 42, then the server computer at the
25 transaction processing network 40 checks to see whether the portable device 36 is authentication verified. As shown in FIG. 2, for example, the transaction process network 40 may look at a field 223 in the authentication database 42 associated with the portable device 36 that indicates whether the portable device 36 is authentication verified or not.

30 **[0068]** If the portable device 36 is not authentication verified, the server computer returns a message to the transactor server 44 indicating that the portable device 36 is not authentication verified. If the portable device 36 is authentication verified, the

server computer returns a message to the transactor server 44 indicating the status of the portable device 36 as authentication verified. The message may include a verification value such as a CAVV or AAV and/or a digital certificate that can be used to send an authorization request message to an issuer. The transaction processing network 40 may add the verification value and/or a digital certificate to an authorization request message to the issuer to authorize the transaction or the transactor server 44 may generate the authorization request message with the verification value and/or the digital certificate. Optionally the merchant/transactor may store the authentication verification (and verification value and/or digital certificate, etc.) locally at the merchant (e.g., in a database associated with the transactor server 44). If the merchant/transactor stores the authentication verification information locally, then the next time the user 30 uses the portable device 36 in a remote transaction, the merchant can look up the portable device 36 (e.g., a unique identifier associated with the portable device 36) in a database associated with the transactor, and determine whether the portable device 36 is authentication verified instead of sending transaction data to the transaction processing network to determine authentication verification. The process may be similar to what is described above for looking up the portable device 36 in the authentication database 42.

[0069] The authorization request message may then be sent to the issuer associated with the portable device 36. The issuer may then generate an authorization response message indicating whether or not the transaction is authorized. The authorization response message is then sent to the transaction processing network 42 which may then forward it to the transactor server 44 (optionally via the acquirer).

[0070] FIG. 5 shows a flowchart of an exemplary method according to embodiments of the invention. In this embodiment, a user 30 may conduct a physical or proximity transaction at an access device 38 (e.g., a POS terminal) using a portable device 36. For example, the user 30 may present his portable device 36 to the access device 38 (e.g., POS terminal) to pay for an item or service by swiping the portable device 36 in a slot in the POS terminal or waving or holding the portable device 36 near the POS terminal. The user may be given the option to enter a mobile device identifier (e.g., a mobile phone number) at the access device 38 or the

mobile device identifier may be stored on the portable device 36 and transferred automatically to the access device 38. The access device 38 or a transactor server 44 associated with the access device 38 may generate an authorization request message that includes the information received from the access device 38 (e.g.,
5 information corresponding to the portable device 36) along with additional transaction information (e.g., a transaction amount, merchant specific information, etc.) and including the mobile device identifier.

[0071] The access device 38 or transactor server 44 may then electronically transmit the authorization request message to the transaction processing network 40
10 (directly or through an acquirer as explained above). The transaction processing network 40 (e.g., a server computer at the transaction processing network 40) may receive the authorization request message with transaction data for the transaction that includes the mobile identifier (502). The server computer at the transaction processing network 40 may store the information for the portable device 36 that
15 includes the mobile device identifier (504) in an authentication database 42 associated with the transaction processing network 40 and indicate that the stored information is not yet authentication verified. As shown in FIG. 2 the server computer at the transaction processing network 40 may store a unique identifier associated with the portable device 36 (221), a mobile identifier (222), an indication
20 whether the portable device 36 is authentication verified (223), among other information received from the user 30 or other entities/information.

[0072] The transaction processing network 40 may then send a message to a mobile device 32 associated with the mobile device identifier (506) to ask the user 30 if he would like to register the portable device 36. If the transaction processing
25 network 40 receives a response from the user indicating that he would like to register the portable device 36 (508), the transaction processing network 40 may mark the stored information for the portable device 36 as authentication verified in the authentication database 42 (510). The transaction processing network 40 may also generate a digital certificate to indicate that the portable device 36 is authentication
30 verified and store the digital certificate in the authentication database 42. The transaction processing network 40 may also generate an AAV (Accountholder Authentication Value) or a CAVV (Cardholder Authentication Verification Value) and store the value in the authentication database 42.

[0073] FIG. 6 shows a flowchart of an exemplary method according to embodiments of the invention that utilizes tokens to authenticate a portable device. In traditional payment transactions, a unique identifier such as a PAN is used to identify the portable device. This portable device unique identifier is exposed to various entities involved in the transactions. For example, a PAN may be passed from an access device, to an acquirer system, a transaction processing network, payment gateways, etc. Because the PAN or other portable device unique identifier can be exposed at various points in processing the transaction, a “token” may be used to conduct payment transactions, instead of the portable device unique identifier. A token serves as an additional security layer to the unique identifier and in effect becomes a proxy/surrogate to the portable device unique identifier and may be used in place of the portable device unique identifier while submitting transactions. There may be more than one token associated with a single portable device unique identifier. For example, a token may be device specific such that each device is associated with a separate token for the same portable device unique identifier. For example, a first token may be used to conduct a payment with a mobile device (e.g., mobile phone, tablet, etc.) and a second token may be used to conduct a payment with a payment card (e.g., credit card, debit card, gift card, etc.). Whether a user uses the mobile device or the payment card to conduct a transaction, the token for each device will be resolved at the back end to a single portable device unique identifier. Embodiments of the invention may utilize two different tokens to authenticate a portable device.

[0074] A user 30 may conduct a transaction using a portable device 36 as described above (e.g., a physical, proximity, or remote transaction). An access device 38 or a transactor server 44 may send transaction data to the transaction processing network 40 (e.g., to a server at the transaction processing network). The transaction data may be in the form of an authorization request message and may include information corresponding to the portable device 36 along with transaction information (e.g., a transaction amount, merchant specific information, etc.). Instead of the portable device unique identifier, a first token may be used as the portable device identifier.

[0075] The transaction processing network 40 may receive the transaction data including the first token (602). The transaction processing network 40 determines a

portable device unique identifier associated with the first token (604). For example, the transaction processing network 40 may look up a record in a database associated with the token to determine the portable device unique identifier for the token. The transaction processing network 40 may then store information

5 associated with the portable device unique identifier (606) in an authentication database 42 associated with the transaction processing network 40 and indicate that the portable device is not yet authentication verified. As shown in FIG. 2 the server computer at the transaction processing network 40 may store a unique identifier associated with the portable device 36 (221), an indication whether the portable
10 device is authentication verified (223), among other information (e.g., 224-229) received from the user 30 or other entities/information.

[0076] The user 30 may conduct a second transaction using a portable device 36 as described above (e.g., a physical, proximity, or remote transaction). An access device 38 or a transactor server 44 may send transaction data to the transaction
15 processing network 40 (e.g., to a server at the transaction processing network). The transaction data may be in the form of an authorization request message and may include information corresponding to the portable device 36 along with transaction information (e.g., a transaction amount, merchant specific information, etc.). Instead of the portable device unique identifier, a second token may be used as the portable
20 device identifier. For example, the second transaction may be conducted with a device different that used for the first transaction.

[0077] The transaction processing network 40 may receive the transaction data including the second token (608). The transaction processing network 40 may determine a portable device unique identifier associated with the second token (610).
25 For example, the transaction processing network 40 may look up a record in a database associated with the token to determine the portable device unique identifier for the token. The transaction processing network 40 then determines that the second token is associated with a portable device unique identifier that has not yet been authentication verified. For example, the transaction processing network 40
30 may compare the portable device unique identifier with a list of portable device identifiers stored in the authentication database 42. If there is a match between the portable device identifier and a portable device identifier in the authentication database 42 and a field associated with the portable device identifier indicates that

the portable device is not yet authentication verified, the transaction processing network 40 can then mark the stored information for the portable device as authentication verified (612). The transaction processing network 40 may also generate a digital certificate to indicate that the portable device 36 is authentication verified and may store the digital certificate in the authentication database 42. The transaction processing network 40 may also generate a verification value such as an AAV (Accountholder Authentication Value) or a CAVV (Cardholder Authentication Verification Value) and may store the value in the authentication database 42.

[0078] Once the portable device 36 is marked as authentication verified in the authentication database 42, then the next time the user 30 uses the portable device 36 in a transaction, the transaction can proceed as an authentication verified transaction, as described above.

[0079] IV. Exemplary Devices

[0080] Provided below are descriptions of some devices (and components of those devices) that may be used in the systems and methods described above. These devices may be used, for instance, to receive, transmit, process, and/or store data related to any of the functionality described above. As would be appreciated by one of ordinary skill in the art, the devices described below may have only some of the components described below, or may have additional components.

[0081] With reference to FIG. 7, a block diagram of an exemplary mobile device 32 is shown that may be used in some embodiments. In some embodiments, the mobile device 32 may be a notification device that can receive alert messages, a payment or portable device that can be used to make payments, an access device (e.g. POS device) that may receive information from a consumer to conduct a transaction, and/or a multi-purpose general use device. The exemplary mobile device 32 may comprise a computer readable medium 32(b) that be present within the body (or outer casing) 32(h), or the computer readable medium 32(b) could be detachable from the device (e.g. the computer readable medium 32(b) could comprise an external memory that could be connected through a physical interface such as a USB connection, or the data could be hosted remotely and accessed wirelessly by the device - e.g. the data could be hosted and stored at a remoter server in the "cloud"). The computer readable medium 32(b) may be in the form of a

memory that stores data. The memory may store information such as financial information, transit information (e.g., as in a subway or train pass), access information (e.g., access badges), serial numbers, mobile account information, and any other suitable information. In general, any of this information may be transmitted
5 by the mobile device 32 (such as to an access device 38), via any suitable method, including the use of antenna 32(a) or contactless element 32(g). The body 32(h) may be in the form a plastic substrate, housing, or other structure.

[0082] In some embodiments, the mobile device 32 may further include a contactless element 32(g), which is typically implemented in the form of a
10 semiconductor chip (or other data storage element) with an associated wireless transfer (e.g., data transmission) element, such as an antenna. Contactless element 32(g) may be coupled to (e.g., embedded within) the mobile device 32 and data or control instructions that are transmitted via a cellular network may be applied to the contactless element 32(g) by means of a contactless element interface (not shown).
15 The contactless element interface functions to permit the exchange of data and/or control instructions between the mobile device circuitry and an optional contactless element 32(g), or between another device having a contactless element (e.g. a POS terminal or a portable/payment device). Contactless element 32(g) may be capable of transferring and receiving data using a short range wireless communication
20 capability. As noted above, mobile device 32 may comprise components to both be the interrogator device (e.g. receiving data) and the interrogated device (e.g. sending data). Thus, the mobile device 32 may be capable of communicating and transferring data or control instructions via both cellular network (or any other suitable wireless network - e.g. the Internet or other data network) and short range
25 communications.

[0083] The mobile device 32 may also include a processor 32(c) (e.g., a microprocessor) for processing the functions of the mobile device 32 and a display 32(d) to allow a user to see phone numbers and other information and messages. The mobile device 32 may further include input elements 32(e) to allow a user to
30 input information into the device, a speaker 32(f) to allow the user to hear voice communication, music, etc., and a microphone 32(i) to allow the user to transmit her voice through the mobile device 32. The mobile device 32 may also include an antenna 32(a) for wireless data transfer (e.g., data transmission). The mobile device

32 may further include a location determination element 32(j) that may be hardware and/or software capable of determining location coordinates (e.g., a GPS element).

[0084] The various participants and elements (e.g., the transaction processing network, transactor, acquirer, issuer, etc.) in embodiments of the invention may also
5 operate one or more computer apparatuses (e.g., a server computer, client computer, mobile device, access device, transactor server, etc.) to facilitate the functions described herein. Any of the elements in embodiments of the invention may use any suitable number of subsystems to facilitate the functions described herein. Examples of such subsystems or components are shown in FIG. 8.

10 **[0085]** FIG. 8 illustrates an exemplary computer system 300, in which various embodiments may be implemented. The system 300 may be used to implement any of the computer systems described above (e.g., a server computer, client computer, mobile device, access device, transactor server, etc.). The computer system 300 is shown comprising hardware elements that may be electrically coupled via a bus 324.
15 The hardware elements may include one or more central processing units (CPUs) 302, one or more input devices 304 (e.g., a mouse, a keyboard, touchpad, etc.), and one or more output devices 306 (e.g., a display device, a printer, etc.). The computer system 300 may also include one or more storage devices 308. By way of example, the storage device(s) 308 may include devices such as disk drives, optical
20 storage devices, solid-state storage device such as a random access memory ("RAM") and/or a read-only memory ("ROM"), which may be programmable, flash-updateable and/or the like.

[0086] The computer system 300 may additionally include a computer-readable storage media reader 312, a communications system 314 (e.g., a modem, a network
25 card (wireless or wired), an infra-red communication device, etc.), and working memory 318, which may include RAM and ROM devices as described above. In some embodiments, the computer system 300 may also include a processing acceleration unit 316, which may include a digital signal processor DSP, a special-purpose processor, and/or the like.

30 **[0087]** The computer-readable storage media reader 312 may further be connected to a computer-readable storage medium 310, together (and, optionally, in combination with storage device(s) 308) comprehensively representing remote, local,

fixed, and/or removable storage devices plus storage media for temporarily and/or more permanently containing, storing, transmitting, and retrieving computer-readable information. The communications system 314 may permit data to be exchanged with the network and/or any other computer described above with respect to the system
5 300.

[0088] The computer system 300 may also comprise software elements, shown as being currently located within a working memory 318, including an operating system 320 and/or other code 322, such as an application program (which may be a client application, Web browser, mid-tier application, RDBMS, etc.). It should be
10 appreciated that alternate embodiments of a computer system 300 may have numerous variations from that described above. For example, customized hardware might also be used and/or particular elements might be implemented in hardware, software (including portable software, such as applets), or both. Further, connection to other computing devices such as network input/output devices may be employed.

[0089] Storage media and computer readable media for containing code, or portions of code, may include any appropriate media known or used in the art, including storage media and communication media, such as but not limited to volatile and non-volatile, removable and non-removable media implemented in any method or technology for storage and/or transmission of information such as computer
20 readable instructions, data structures, program modules, or other data, including RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disk (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, data signals, data transmissions, or any other medium which may be used to store or transmit the
25 desired information and which may be accessed by the computer. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art may appreciate other ways and/or methods to implement the various embodiments.

[0090] Embodiments of the invention have a number of advantages. In conventional transaction systems, payment processors and issuers have a difficult
30 time determining whether or not transactions conducted remotely with mobile devices are authentic or not, since a physical portable device such as a physical credit card is not present. By using embodiments of the invention, a transaction

conducted remotely with a mobile device can be verified such that a payment processor or issuer can have confidence that the mobile device conducting the transaction is authentic. Consequently, the approval of potentially fraudulent transactions is significantly reduced using embodiments of the invention. Further, the verification process utilized is relatively seamless and convenient, since the user uses a normal payment transaction to verify that future transactions conducted with a mobile device are authentic.

[0091] It should be understood that the present invention as described above may be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art may know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software

[0092] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0093] The above description is illustrative and is not restrictive. Many variations of the invention may become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0094] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0095] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1 1. A method comprising:
2 receiving, at a server computer, information for a portable device that
3 includes a mobile device identifier;
4 storing, by the server computer, the information for the portable device
5 that includes the mobile device identifier in a database associated with the server
6 computer;
7 receiving, by the server computer, transaction data from an access
8 device for a transaction conducted at the access device;
9 determining, by the server computer, from the transaction data that the
10 transaction is associated with the portable device;
11 determining, by the server computer, a location of the access device;
12 determining, by the server computer, a location of a mobile device
13 associated with the mobile device identifier;
14 determining, by the server computer, that the location of the mobile
15 device matches the location of the access device; and
16 marking, by the server computer, the stored information for the portable
17 device as authentication verified.

1 2. The method of claim 1 further comprising:
2 receiving, at the server computer, a second transaction data for a
3 remote transaction conducted via a transactor server computer;
4 determining, by the server computer, from the second transaction data
5 that the remote transaction is associated with the portable device;
6 determining, by the server computer, that information for the portable
7 device is marked as authentication verified; and
8 sending, by the server computer, a message to the transactor server
9 computer indicating the status of the portable device as authentication verified.

1 3. The method of claim 2 wherein sending the message to the
2 transactor server computer indicating the status of the portable device as
3 authentication verified includes sending a digital certificate to the transactor server
4 computer.

1 4. The method of claim 1 further comprising:
2 generating, by the server computer, a digital certificate indicating that
3 the status of the portable device is authentication verified; and
4 storing, by the server computer, the digital certificate in the database
5 associated with the server computer.

1 5. The method of claim 1 wherein determining the location of the
2 access device includes determining the location of the access device from location
3 information included in the transaction data.

1 6. The method of claim 1 wherein determining the location of the
2 mobile device includes sending a message to the mobile device requesting
3 information to confirm the location of the mobile device.

1 7. The method of claim 6 wherein requesting information includes
2 a request for confirmation for a recent transaction or a challenge question.

1 8. The method of claim 1 wherein determining the location of the
2 mobile device includes utilizing location technology to determine the geographical
3 position of the mobile device.

1 9. The method of claim 1 wherein storing the information for the
2 portable device that includes the mobile device identifier further comprises indicating
3 that the stored information for the portable device is not yet authentication verified.

1 10. A server computer comprising:
2 a processor; and
3 a non-transitory computer readable medium coupled with the
4 processor, the computer readable medium comprising instructions executable by the
5 processor, the instructions comprising:
6 receiving information for a portable device that includes a mobile
7 device identifier;
8 storing the information for the portable device that includes the mobile
9 device identifier in a database associated with the server computer;

10 receiving transaction data from an access device for a transaction
11 conducted at the access device;
12 determining from the transaction data that the transaction is associated
13 with the portable device;
14 determining a location of the access device;
15 determining a location of a mobile device associated with the mobile
16 device identifier;
17 determining that the location of the mobile device matches the location
18 of the access device; and
19 marking the stored information for the portable device as authentication
20 verified.

1 11. The server computer of claim 10, the instructions further
2 comprising:
3 receiving a second transaction data for a remote transaction conducted
4 via a transactor server computer;
5 determining from the second transaction data that the remote
6 transaction is associated with the portable device;
7 determining that information for the portable device is marked as
8 authentication verified; and
9 sending a message to the transactor server computer indicating the
10 status of the portable device as authentication verified.

1 12. The server computer of claim 10 wherein sending the message
2 to the transactor server computer indicating the status of the portable device as
3 authentication verified includes sending a digital certificate to the transactor server
4 computer.

1 13. The server computer of claim 10, the instructions further
2 comprising:
3 generating a digital certificate indicating that the status of the portable
4 device is authentication verified; and
5 storing the digital certificate in the database associated with the server
6 computer.

1 14. The server computer of claim 10 wherein determining the
2 location of the access device includes determining the location of the access device
3 from location information included in the transaction data.

1 15. The server computer of claim 10 wherein determining the
2 location of the mobile device includes sending a message to the mobile device
3 requesting information to confirm the location of the mobile device.

1 16. The server computer of claim 10 wherein requesting information
2 includes a request for confirmation for a recent transaction or a challenge question.

1 17. The server computer of claim 10 wherein determining the
2 location of the mobile device includes utilizing location technology to determine the
3 geographical position of the mobile device.

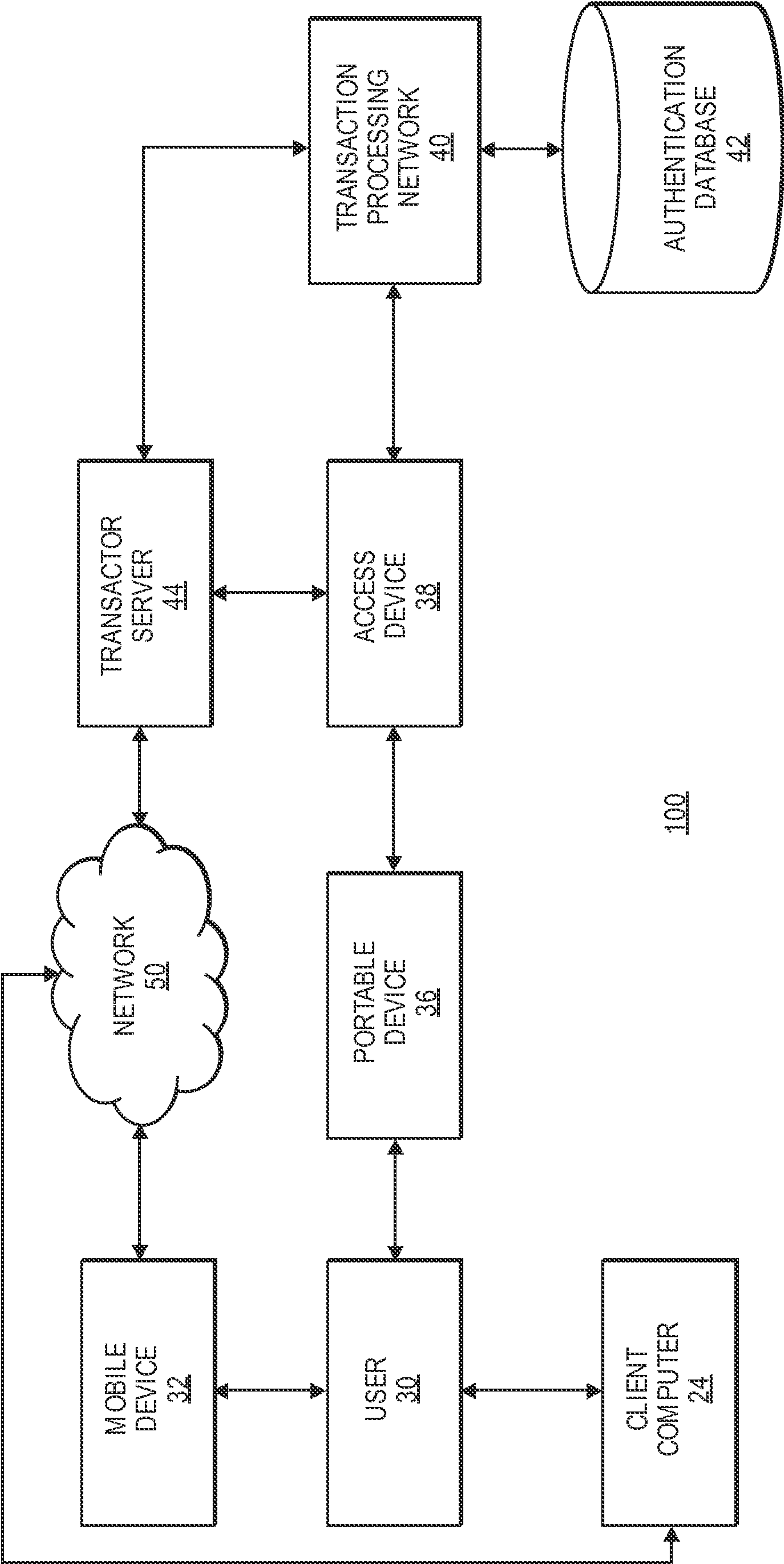
1 18. The server computer of claim 10 wherein storing the information
2 for the portable device that includes the mobile device identifier further comprises
3 indicating that the stored information for the portable device is not yet authentication
4 verified.

1 19. The server computer of claim 10 wherein the access device is
2 an electronic cash register.

1 20. A computer apparatus comprising:
2 a processor; and
3 a non-transitory computer readable medium coupled with the
4 processor, the computer readable medium comprising instructions executable by the
5 processor, the instructions comprising:
6 sending information for a portable device that includes a mobile device
7 identifier, to a server computer wherein the server computer stores the information
8 for the portable device that includes the mobile device identifier in a database
9 associated with the server computer;
10 receiving transaction data for a transaction conducted using the
11 portable device; and

12 sending the transaction data to the server computer wherein the server
13 computer determines a location of an access device associated with the mobile
14 device identifier, determines a location of a mobile device associated with the mobile
15 device identifier, determines that the location of the mobile device identifier matches
16 the location of the access device, and marks the stored information in the
17 authentication database as authentication verified.

1 21. The computer apparatus of claim 20, the instructions further
2 comprising:
3 sending to the server computer, a second transaction data for a remote
4 transaction conducted wherein the server computer determines from the second
5 transaction data that the remote transaction is associated with the portable device
6 and determines that information for the portable device is marked as authentication
7 verified; and
8 receiving a message from the server computer indicating the status of
9 the portable device as authentication verified.



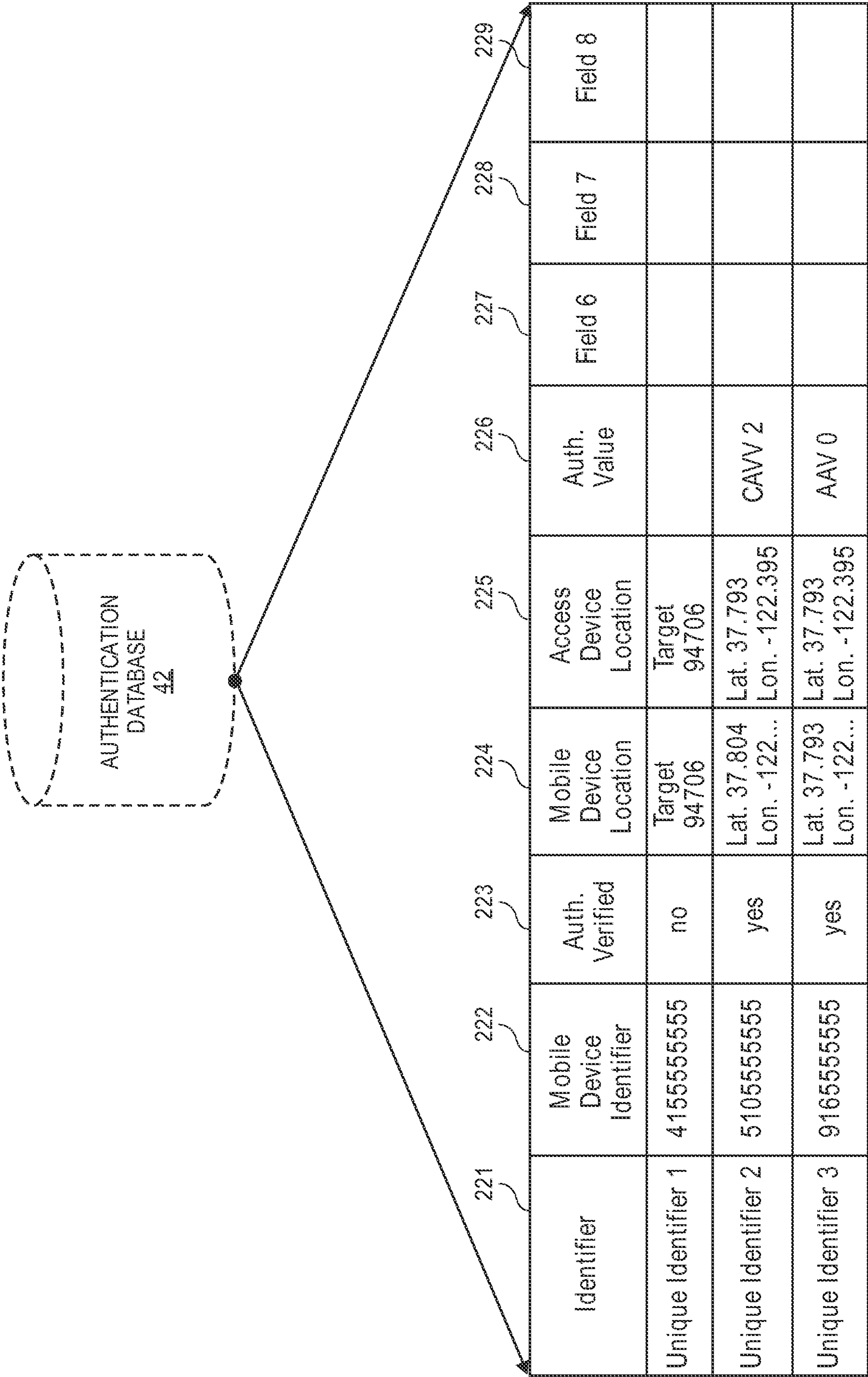


FIG. 2

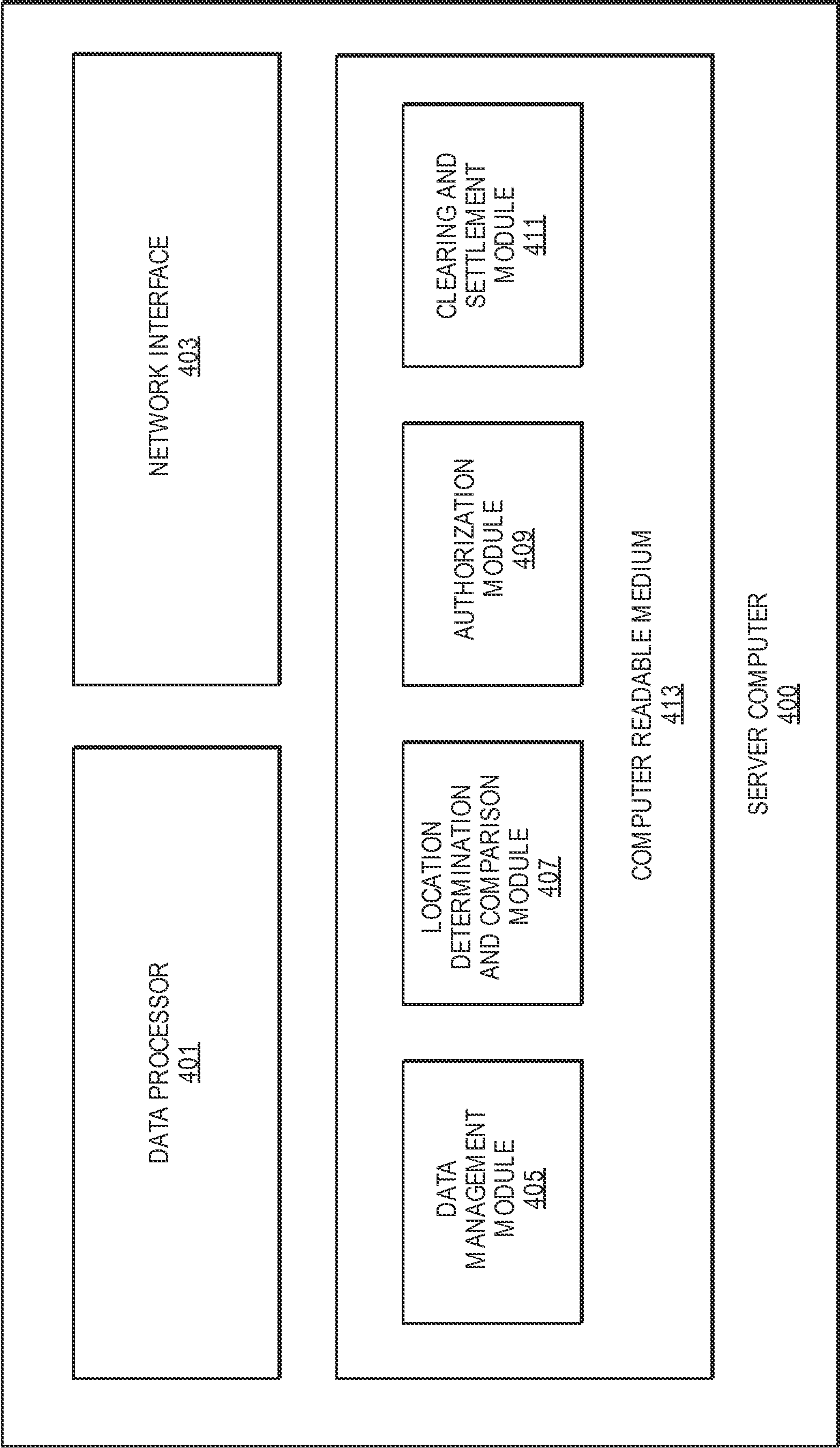


FIG. 3

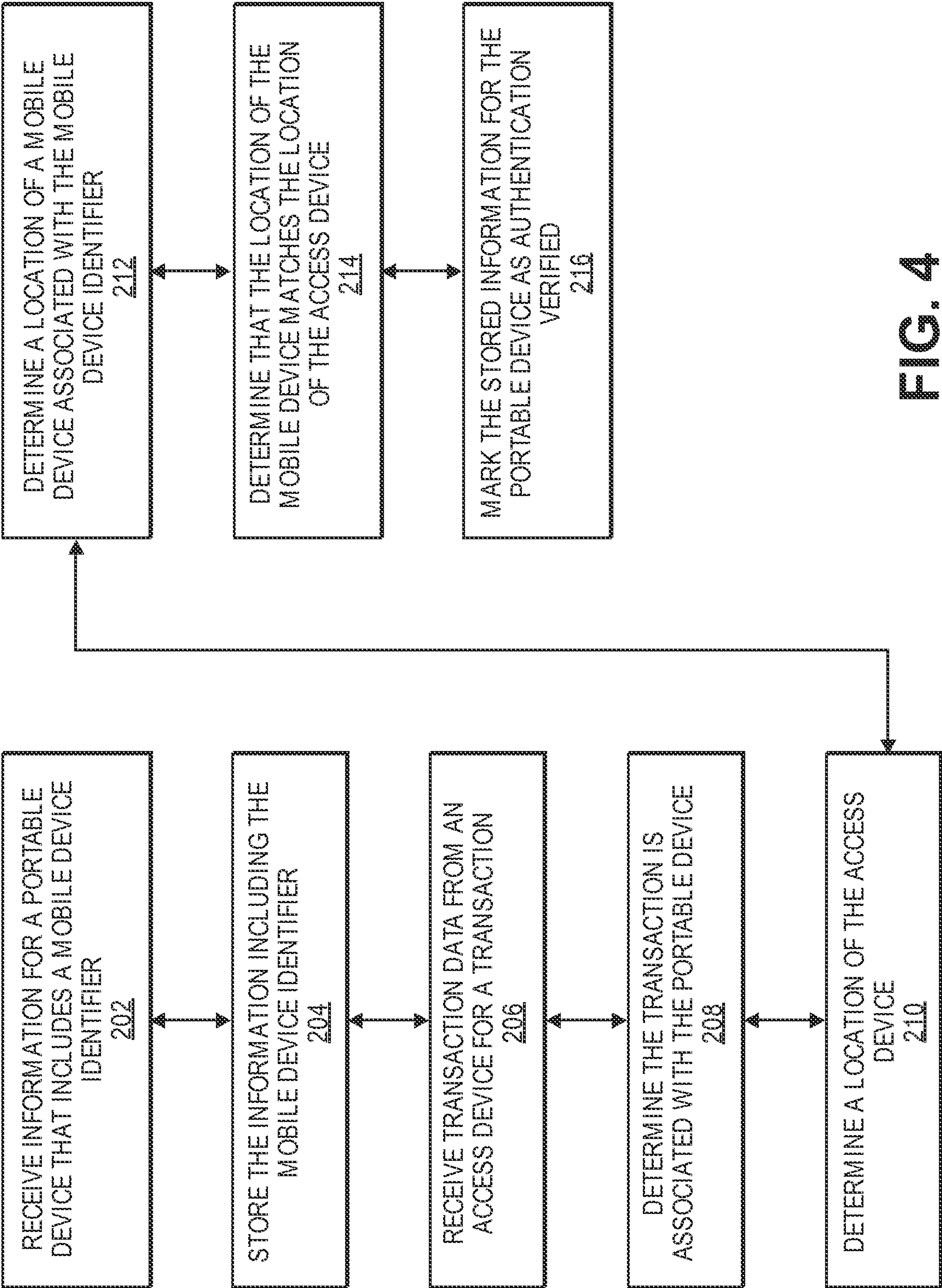
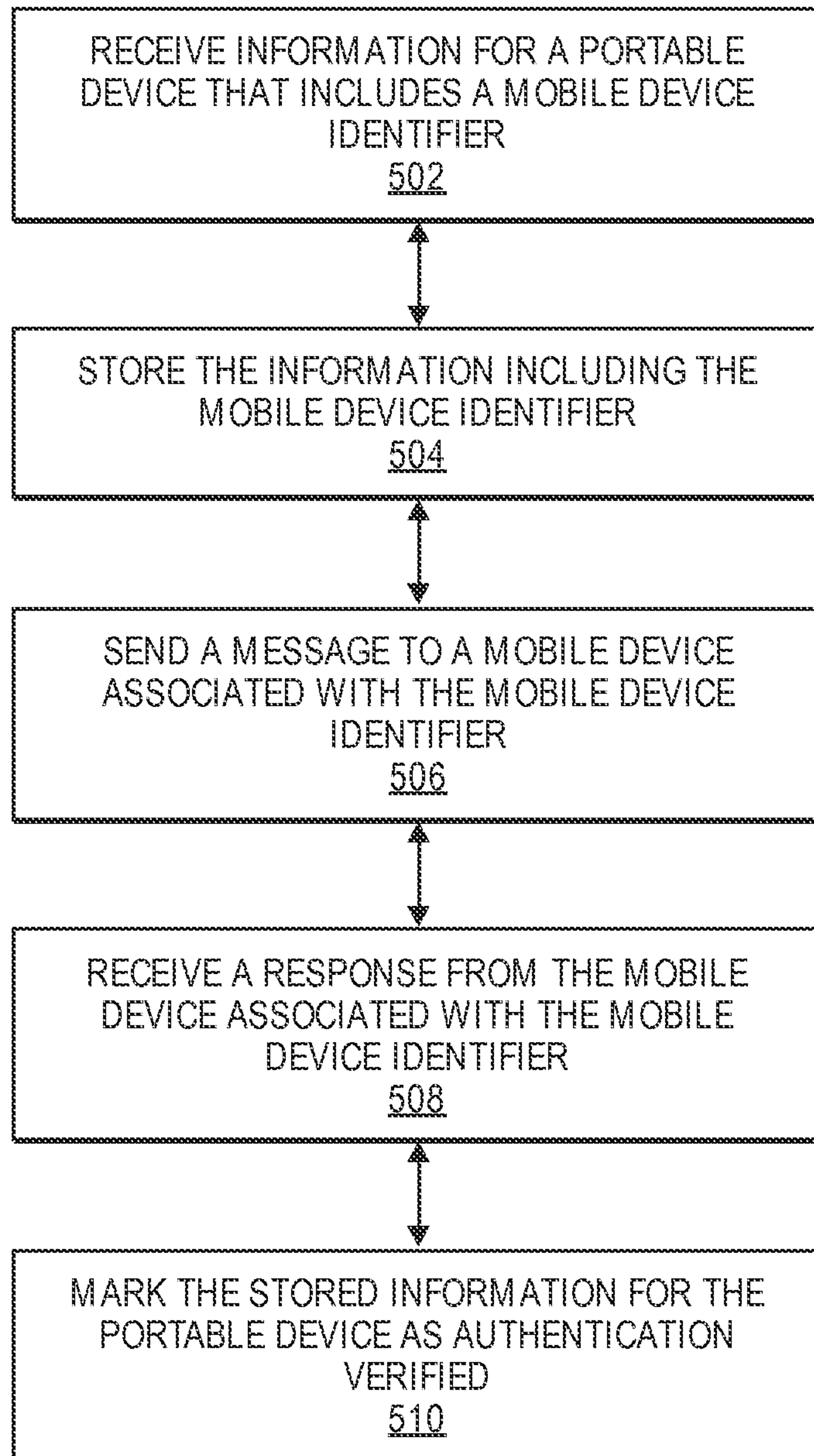


FIG. 4

5/8

**FIG. 5**

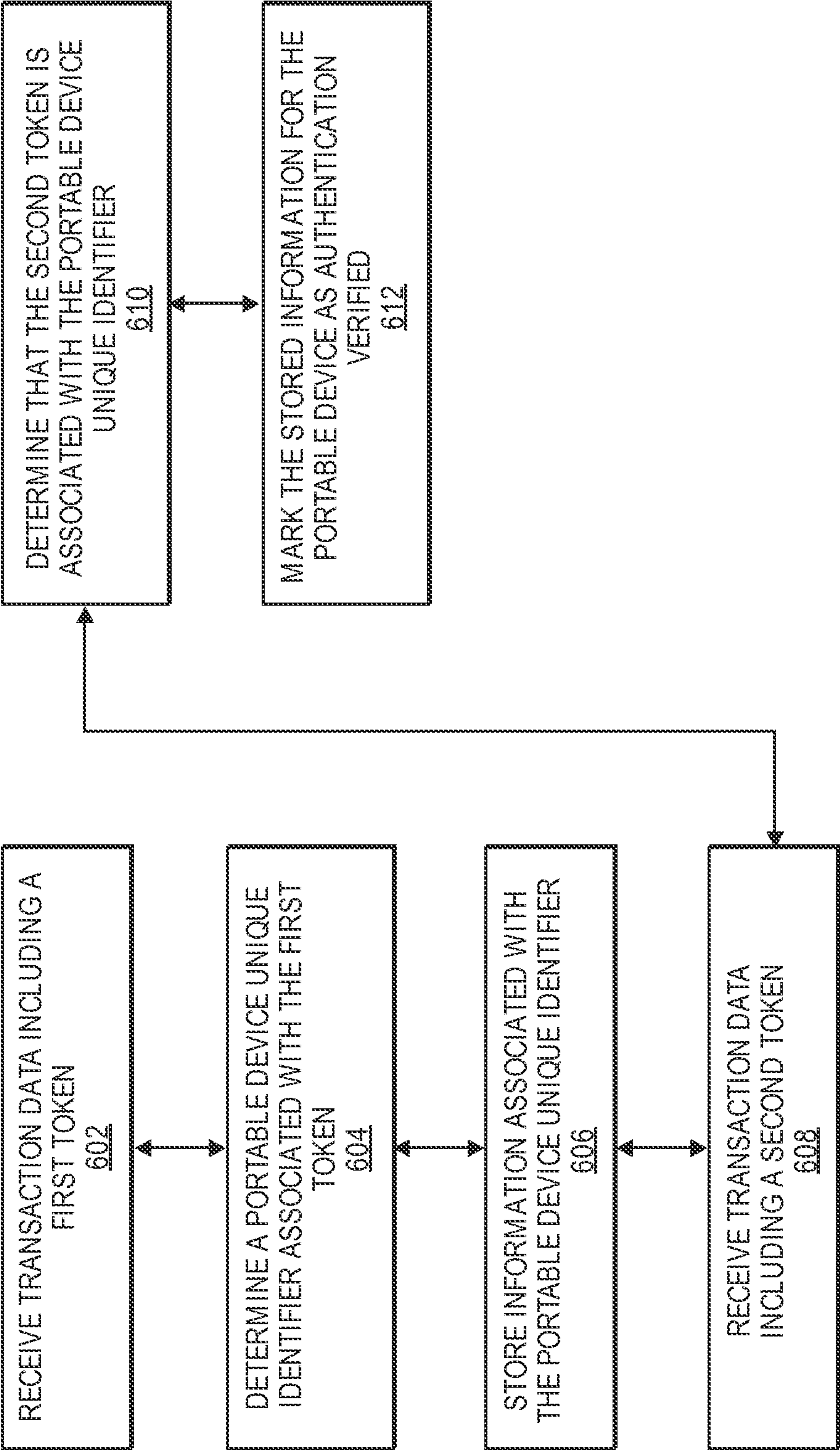


FIG. 6

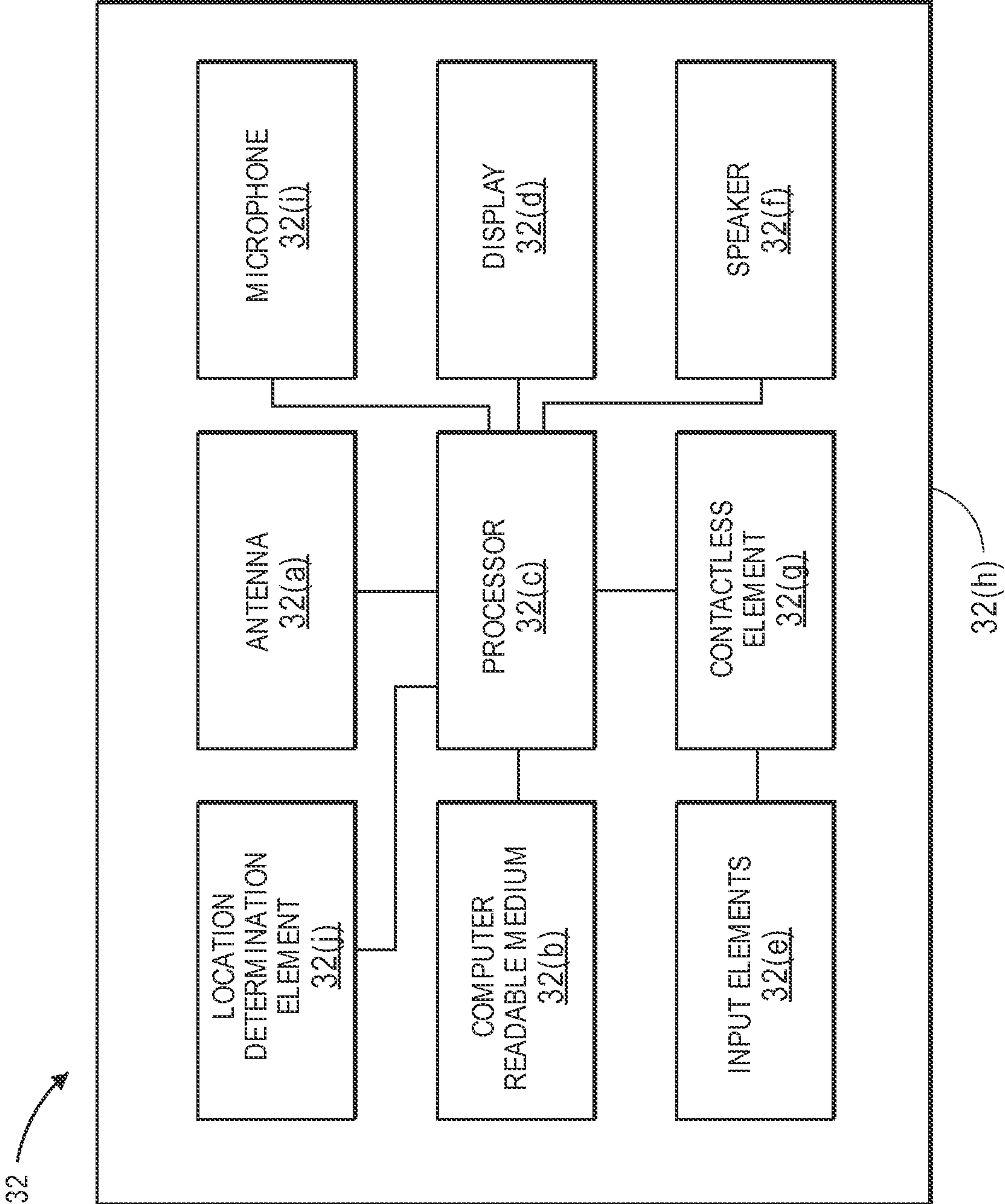


FIG. 7

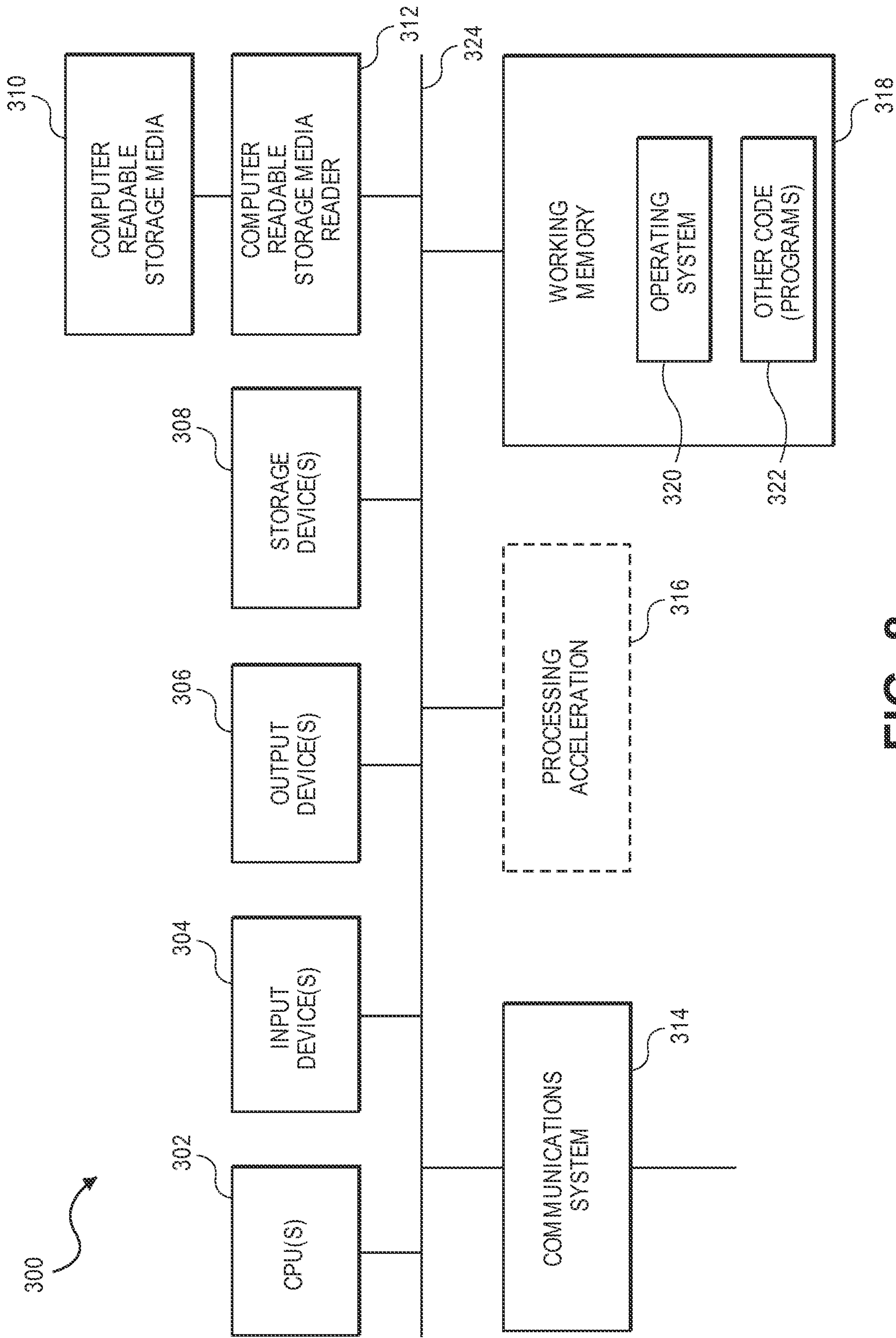


FIG. 8

FIG. 1

