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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 October 2009 (15.10.2009)

PCT

(10) International Publication Number
WO 2009/126732 A2

(51) International Patent Classification:
G06Q 30/00 (2006.01) *G06F 17/30* (2006.01)
G06F 7/04 (2006.01) *H04L 9/32* (2006.01)
G06K 9/00 (2006.01)

(21) International Application Number:
PCT/US2009/039943

(22) International Filing Date:
8 April 2009 (08.04.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/043,326 8 April 2008 (08.04.2008) US
61/102,983 6 October 2008 (06.10.2008) US

(71) Applicant *(for all designated States except US)*: **PROXENSE, LLC** [US/US]; 689 Nw Stonepinee Drive, Bend, OR 97701 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **GIOBBI, John, J.** [US/US]; c/o Proxense, LLC, 689 Nw Stonepine Drive, Bend, OR 97701 (US).

(74) Agents: **ISHIHARA, Kanda, V.** et al.; Fenwick & West LLP, Silicon Valley Center, 801 California Street, Mountain View, CA 94041 (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, BR, BW, BY, BZ, CA, CH, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (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, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) **Title**: AUTOMATED SERVICE-BASED ORDER PROCESSING

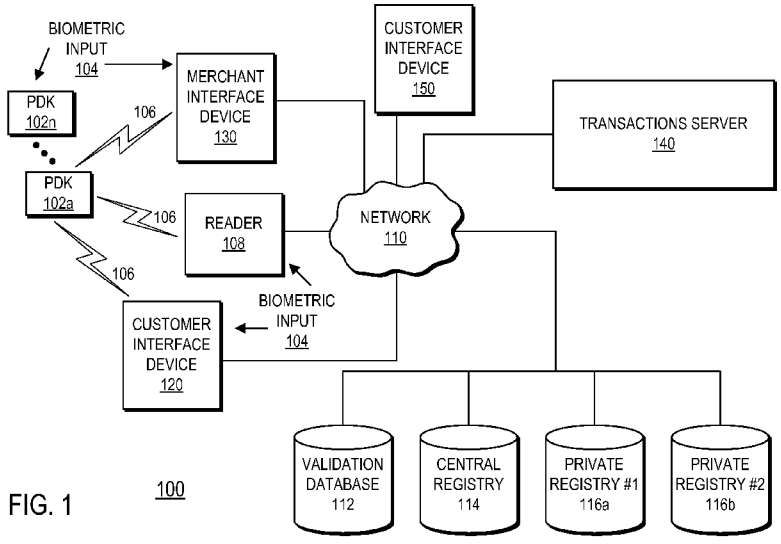

FIG. 1

(57) **Abstract**: A system and method provide efficient, secure and fast automation of order processing. The method includes initiating an order by wirelessly receiving data from a personal digital key (PDK). The method also includes receiving a biometric input and confirming the initiation of the order by authenticating the biometric input. In response to authenticating the biometric input, the order is processed. In another embodiment, the method of further includes automatically initiating an order completion by wirelessly receiving data from a PDK. The method further includes receiving a biometric input and confirming the order completion by authenticating the biometric input. In response to authenticating the biometric input, the order is completed. In yet another embodiment, the method further includes processing rewards based on the order

WO 2009/126732 A2

AUTOMATED SERVICE-BASED ORDER PROCESSING

INVENTORS:

JOHN J. GIOBBI

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Patent Application No. 61/043,326, entitled "Automated Service-Based Order Processing (Prox Order)" filed April 8, 2008 and U.S. Patent Application No. 61/102,983, entitled "Automated Service-Based Order Processing (Prox Order)" filed October 6, 2008, the entire contents of which are all herein incorporated by reference.

BACKGROUND OF THE INVENTION

1. FIELD OF ART

[0002] The disclosure generally relates to the field of electronic order processing, and more specifically, to automated order processing using biometric verification.

2. DESCRIPTION OF THE RELATED ART

[0003] Optimizing sales transactions is one of the many challenges faced by various merchants. Ensuring these processes are secure, efficient and simple is important to merchants, providers, users and consumers alike. Conventionally, technologies such as magnetic cards (e.g., credit cards, debit cards, ATM cards, and employee badges) have been used in attempt to address these needs. More recently, various contactless cards or tokens requiring placement near compatible readers have been used.

[0004] Further, in serviced-based transactions, such as those that would occur at STARBUCKS™, MCDONALDS™, or QUIZNOS™, the transaction may be further delayed during the ordering process due to the various steps involved in processing and completing the transaction. The transaction may be even further delayed due to the fact that, oftentimes, customers customize or change their orders from what is regularly offered. Also, many of these merchants have increased in popularity over the years, leading to increasing number of customers visiting such merchants. The combination of the currently technologies for completing and processing these service-based transactions, coupled with the increase in number of customers frequenting the merchants' establishments leads to longer wait times for a transaction to process and complete. A new technology is needed that provides highly reliable, safe, efficient automation for order processing.

BRIEF SUMMARY OF THE INVENTION

[0005] A system and method provide efficient, secure and fast automation of order processing. A system for automated electronic order processing, including a customer interface device for wirelessly receiving data from a personal digital key (PDK) and a transactions server, adapted for communication with the customer interface device for initiating an order in response to wirelessly receiving the data from the PDK and processing the order. In one embodiment, the system also includes a merchant interface device, adapted to communicate with the transactions server, for wirelessly receiving data from a personal digital key (PDK). The transactions server is adapted for communication with the merchant interface device and for initiating an order completion. In one embodiment, the system also includes a reader, adapted to communicate with the transaction server, for automatically uploading data from the PDK and receiving biometric input from a user.

[0006] The method includes initiating an order by wirelessly receiving data from a personal digital key (PDK). The method also includes receiving a biometric input and confirming the initiation of the order by authenticating the biometric input. In response to authenticating the biometric input, the order is processed. In another embodiment, the method of further includes automatically initiating an order completion by wirelessly receiving data from a PDK. The method further includes receiving a biometric input and confirming the order completion by authenticating the biometric input. In response to authenticating the biometric input, the order is completed. In yet another embodiment, the method further includes processing rewards based on the order.

[0007] The features and advantages described in the specification are not all inclusive and, in particular, many additional features and advantages will be apparent to one of ordinary skill in the art in view of the drawings, specification, and claims. Moreover, it should be noted that the language used in the specification has been principally selected for readability and instructional purposes, and may not have been selected to delineate or circumscribe the disclosed subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] The disclosed embodiments have other advantages and features which will be more readily apparent from the detailed description, the appended claims, and the accompanying figures (or drawings). A brief introduction of the figures is below.

[0009] Figure (FIG.) 1 is a high level block diagram illustrating a system for automated service-based order processing according to one embodiment of the invention.

[0010] FIG. 2A is a block diagram illustrating a Personal Digital Key (PDK) according to one embodiment of the invention.

[0011] FIG. 2B is a block diagram illustrating a biometric reader of a PDK according to one embodiment of the invention.

[0012] FIG. 3 is a block diagram illustrating a reader according to one embodiment of the invention.

[0013] FIG. 4A is a block diagram illustrating a customer interface device according to one embodiment of the invention.

[0014] FIG. 4B is a block diagram illustrating a customer interface device according to another embodiment of the invention.

[0015] FIG. 4C is a block diagram illustrating a customer interface device according to yet another embodiment of the invention.

[0016] FIG. 5A is a block diagram illustrating a merchant interface device according to one embodiment of the invention.

[0017] FIG. 5B is a block diagram illustrating a merchant interface device according to another embodiment of the invention.

[0018] FIG. 6 is a flowchart illustrating one embodiment of a process for authorizing a communication connection using secure authentication.

[0019] FIG. 7 is a flowchart illustrating one embodiment of a process for device authentication by a reader.

[0020] FIG. 8 is a flowchart illustrating one embodiment of a process for profile authentication by a reader.

[0021] FIG. 9A is a flowchart illustrating one embodiment of a process for profile testing using a biometric input.

[0022] FIG. 9B is a flowchart illustrating one embodiment of a process for profile testing using a personal identification number.

[0023] FIG. 9C is a flowchart illustrating one embodiment of a process for profile testing using a picture profile.

[0024] FIG. 9D is a flowchart illustrating one embodiment of a process for profile testing using a private or central registry.

[0025] FIG. 10 illustrates an example scenario of a reader operating in a congested area with multiple PDKs within its proximity zone.

[0026] FIG. 11 is a flowchart illustrating one embodiment of a process for differentiating between multiple PDKs in completing a secure authentication process.

[0027] FIG. 12 is a block diagram illustrating an embodiment of a system for estimating location of a PDK using coordinate triangulation.

[0028] FIG. 13 is a block diagram illustrating an embodiment of a system for location tracking of a PDK.

[0029] FIG. 14 is a block diagram illustrating a transactions server according to one embodiment of the invention.

[0030] FIG. 15 is a flowchart illustrating a process for automated order processing according to one embodiment of the invention.

[0031] FIG. 16 is a flowchart illustrating a process for initializing a PDK according to one embodiment of the invention.

[0032] FIG. 17 is a flowchart illustrating a process for uploading PDK data according to one embodiment of the invention.

[0033] FIG. 18 is a flowchart illustrating interaction between devices of the system for automated service-based order processing according to one embodiment of the invention.

[0034] FIG. 19 is a flowchart illustrating a process for processing an order according to one embodiment of the invention.

[0035] FIG. 20 is a flowchart illustrating interaction between devices of the system for automated service-based order processing according to another embodiment of the invention.

[0036] FIG. 21 is a flowchart illustrating interaction between devices of the system for automated service-based order processing according to yet another embodiment of the invention.

[0037] FIG. 22 is a flowchart illustrating a process for rewards processing according to one embodiment of the invention.

[0038] The figures depict various embodiments of the present invention for purposes of illustration only. One skilled in the art will readily recognize from the following discussion that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles of the invention described herein.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0039] The Figures (FIGS.) and the following description relate to preferred embodiments by way of illustration only. It should be noted that from the following discussion, alternative embodiments of the structures and methods disclosed herein will be readily recognized as viable alternatives that may be employed without departing from the principles of what is claimed.

[0040] Reference will now be made in detail to several embodiments, examples of which are illustrated in the accompanying figures. It is noted that wherever practicable similar or like reference numbers may be used in the figures and may indicate similar or like functionality. The figures depict embodiments of the disclosed system (or method) for purposes of illustration only. One skilled in the art will readily recognize from the following description that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles described herein.

[0041] FIG. 1 is a high level block diagram illustrating a system 100 for automated service-based order processing according to one embodiment of the invention. The system 100 comprises a Personal Digital Key (PDK) 102, a reader 108, a network 110, a customer interface device 120, a merchant interface device 130, a transactions server 140 and one or more external databases including a validation database 112, a central registry 114 and one or more private registries 116. The reader 108, customer interface device 120 and merchant interface device 130 are coupled to the PDK 102 by a wireless link 106 and coupled to a network 110 by either a wired or wireless link. The reader 108, customer interface device 120, merchant interface device 130 are also adapted to receive a biometric input 104 from a user and is capable of displaying status to a user. Similarly, in one embodiment, the PDK 102 is also adapted to receive a biometric input 104 from a user. The network 110 couples the validation database 112, the central registry 114 and two private registries 116 to the reader 108, customer interface device 120, merchant interface device 130 and transactions server 140. In alternative embodiments, different or additional external registries or databases may be coupled to the network 110.

[0042] The system 100 addresses applications where it is important to ensure a specific individual is authorized to perform a given transaction. A transaction as used herein can include executing a purchase or financial dealing, enabling access to physical and/or digital items, verifying identification or personal information or executing other tasks where it is important to authenticate an individual for use. Generally, the reader 108 wirelessly receives information stored in the PDK 102 that uniquely identifies the PDK 102 and the individual carrying the PDK 102. The reader 108 can also receive a biometric input 104 from the individual. Based on the received information, the reader 108 determines if the transaction should be authorized. Beneficially, the system 100 provides comprehensive authentication without the need for PINs or passwords. Moreover, personal biometric information need not be stored in any local or remote storage database and is only stored on the user's own PDK. Furthermore, in one embodiment, purchase transactions can be efficiently completed without

requiring the use of physical credit cards, tokens or other user action beyond initiating the transaction.

[0043] The credibility of the system 100 is ensured by the use of the PDK 102 that stores trusted information. The PDK 102 is a compact, portable uniquely identifiable wireless device typically carried by an individual. The PDK 102 stores digital information in a tamper-proof format that uniquely associates the PDK 102 with an individual. Example embodiments of PDKs are described in more detail in U.S. Patent Application No. 11/292,330 entitled "Personal Digital Key And Receiver/Decoder Circuit System And Method;" U.S. Patent Application No. 11/620,581 entitled "Wireless Network Synchronization Of Cells And Client Devices On A Network;" and U.S. Patent Application No. 11/620,577 entitled "Dynamic Real-Time Tiered Client Access", the entire contents of which are all incorporated herein by reference.

[0044] To establish the trust, credibility and confidence of the authentication system, information stored in the PDK 102 is acquired by a process that is trusted, audited and easily verified. The process is ensured by a trusted third-party system, referred to herein as a Notary that administers the acquisition and storage of information in the PDK 102 according to defined security protocols. In one embodiment, the Notary is a system and/or a trusted individual that witnesses the acquisition and storage either in person or remotely. In another embodiment, the Notary comprises trusted hardware that administers the initialization process by an automated system. Thus, once initialized by the trusted process, the PDK 102 can prove that the information it stores is that of the individual. Example embodiments of the initialization process are described in U.S. Patent Application No. 11/744,832 (Attorney Docket No. 25000-12784), entitled "Personal Digital Key Initialization and Registration For Secure Transaction", the entire contents of which are incorporated herein by reference.

[0045] The reader 108 wirelessly communicates with the PDK 102 when the PDK 102 is within a proximity zone of the reader 108. The proximity zone can be, for example, several meters in radius and can be adjusted dynamically by the reader 108. Example embodiments of a reader with a dynamically adjustable proximity zone are described in U.S. Patent Application No. 11/620,600 (Attorney Docket No. 25000-12199), filed January 5, 2007, entitled "Dynamic Cell Size Variation Via Wireless Link Parameter Adjustment", the entire contents of which are incorporated herein by reference. Thus, in contrast to many conventional RF ID devices, the reader 108 can detect and communicate with the PDK 102 without requiring the owner to remove the PDK 102 from his/her pocket, wallet, purse, etc. Also, in contrast to many conventional RFID devices, the reader 108 and PDK 102 are

designed to operate in a dense client environment – not on a one-by-one reader to client-held device basis. Example embodiments of a reader that provides dense, coordinated system operation is described in U.S. Patent Application No. 11/620,581 (Attorney Docket No. 25000-12194), filed January 5, 2007, entitled "Wireless Network Synchronization Of Cells And Client Devices On A Network", the entire contents of which are incorporated herein by reference. Generally, the reader 108 receives uniquely identifying information from the PDK 102 and initiates an authentication process for the individual carrying the PDK 102. In one embodiment, the reader 108 is adapted to receive a biometric input 104 from the individual. The biometric input 104 comprises a representation of physical or behavioral characteristics unique to the individual. For example, the biometric input 104 can include a fingerprint, a palm print, a retinal scan, an iris scan, a photograph, a signature, a voice sample or any other biometric information such as DNA, RNA or their derivatives that can uniquely identify the individual. The reader 108 compares the biometric input 104 to information received from the PDK 102 to determine if a transaction should be authorized. Alternatively, the biometric input 104 can be obtained by a biometric reader on the PDK 102 and transmitted to the reader 108 for authentication. In an additional alternative embodiment, some or all of the authentication process can be performed by the PDK 102 instead of the reader 108.

[0046] The reader 108 is further communicatively coupled to the network 110 in order to receive and/or transmit information to remote databases for remote authentication. In an alternative embodiment, the reader 108 includes a non-volatile data storage that can be synchronized with one or more remote databases 112 or registries 114-116. Such an embodiment relaxes the requirement for a continuous connection to the network 110 and allows the reader 108 to operate in a standalone mode and for the local data storage to be updated when a connection is available. For example, a standalone reader 108 can periodically download updated registry entries and perform authentication locally without any remote lookup.

[0047] The customer interface devices 120 facilitate in the process of automated order processing. In one embodiment, the customer interface device 120 allows a customer to initiate an order by simply providing a biometric sample. In one embodiment, a customer can initiate an order via the customer interface device 120 with a simple finger swipe. In another embodiment, the customer can initiate, complete and pay for the order by simply providing a biometric sample, such as a finger swipe. In yet another embodiment, the customer need only confirm and/or select his or her order by providing a biometric sample, such as a finger

swipe. More details describing the components and functionality of the customer interface device 120 is provided below with reference to FIGS. 4A and 4B.

[0048] The merchant interface device 130 allows customers to automatically and securely complete order transactions with a simple step of providing a biometric sample. In one embodiment, the merchant interface device 130 allows customers to automatically and securely complete order transactions with a simple swipe of the finger. In another embodiment, the merchant interface device 130 displays customers' orders to be prepared by the merchant. In one embodiment, the customers' orders are displayed in a list in order of when the order what placed. More details describing the components and functionality of the merchant interface device 130 is provided below with reference to FIGS. 5A and 5B.

[0049] The transactions server 140 includes software or routines for automating the process of entering and fulfilling an order. The transactions server 140 facilitates automatic order processing and payment procedures. The transactions server 140 is coupled to and adapted to communicate with the customer interface device 120, the merchant interface device 130 and the reader 108 via the network 110. The transaction server 140 is also coupled to the registries 114-116 for payment information and verification. More details describing the components and functionality of the transactions server 140 is provided below with reference to FIG. 14.

[0050] The network 110 provides communication between the reader 108, customer interface device 120, merchant interface device 130, transactions server 140 and the validation database 112, central registry 114 and one or more private registries 116. In alternative embodiments, one or more of these connections may not be present or different or additional network connections may be present. In one embodiment, the network 110 uses standard communications technologies and/or protocols. Thus, the network 110 can include links using technologies such as Ethernet, 802.11, 802.16, integrated services digital network (ISDN), digital subscriber line (DSL), asynchronous transfer mode (ATM), etc. Similarly, the networking protocols used on the network 110 can include the transmission control protocol/Internet protocol (TCP/IP), the hypertext transport protocol (HTTP), the simple mail transfer protocol (SMTP), the file transfer protocol (FTP), etc. The data exchanged over the network 110 can be represented using technologies and/or formats including the hypertext markup language (HTML), the extensible markup language (XML), etc. In addition, all or some of links can be encrypted using conventional encryption technologies such as the secure sockets layer (SSL), Secure HTTP and/or virtual private networks (VPNs). In another

embodiment, the entities can use custom and/or dedicated data communications technologies instead of, or in addition to, the ones described above.

[0051] The validation database 112 stores additional information that may be used for authorizing a transaction to be processed at the reader 108. For example, in purchase transactions, the validation database 112 is a credit card validation database that is separate from the merchant providing the sale. Alternatively, a different database may be used to validate different types of purchasing means such as a debit card, ATM card or bank account number.

[0052] The registries 114-116 are securely-accessible databases coupled to the network 110 that store, among other items, PDK, Notary, and reader information. In one embodiment, the registries 114-116 do not store biometric information. Information stored in the registries can be accessed by the reader 108 via the network 110 for use in the authentication process. There are two basic types of registries illustrated: private registries 116 and the central registry 114. Private registries 116 are generally established and administered by their controlling entities (e.g., a merchant, business authority, or other entity administering authentication). Private registries 116 can be custom configured to meet the specialized and independent needs of each controlling entity. The central registry 114 is a single highly-secured, centrally-located database administered by a trusted third-party organization. In one embodiment, all PDKs 102 are registered with the central registry 114 and may be optionally registered with one or more selected private registries 116. In some embodiments, these registries 114-116 are financial databases for payment processing. In such embodiments, registries 114-116 are financial databases of credit card companies such as AMERICAN EXPRESS™, VISA™ or MASTERCARD™. In alternative embodiments, a different number or different types of registries may be coupled to the network 110.

[0053] Turning now to FIG. 2A, an example embodiment of a PDK 102 is illustrated. The PDK 102 comprises a memory 210, a programmer I/O 240, control logic 250, and a transceiver 260, coupled by a bus 270. The PDK 102 can be standalone as a portable, physical device or can be integrated into commonly carried items. For example, a PDK 102 can be integrated into a portable electronic device such as a cell phone, Personal Digital Assistant (PDA), or GPS unit, an employee identification tag, a key fob, or jewelry items such as watches, rings, necklaces or bracelets.

[0054] The memory 210 can be a read-only memory, a once-programmable memory, a read/write memory or any combination of memory types including physical access secured and tamperproof memories. The memory 210 typically stores a unique PDK ID 212 and one

or more profiles 220. The PDK ID 212 comprises a public section and a private section of information, each of which can be used for identification and authentication. In one embodiment, the PDK ID 212 is stored in a read-only format that cannot be changed subsequent to manufacture. The PDK ID 212 is used as an identifying feature of a PDK 102 and distinguishes between PDKs 102 in private 116 or Central 114 registry entries. The PDK ID 212 can also be used in basic PDK authentication to ensure that the PDK 102 is a valid device. In one embodiment, the memory 210 also stores a purchase log 290. The purchase log 290 keeps track of the customer's purchases for at a particular merchant's establishment. The data contained in the purchase log 290 can later be used to determine rewards.

[0055] The profile fields 220 can be initially empty at the time of manufacture but can be written to by authorized individuals (e.g., a Notary) and/or hardware (e.g., a Programmer). In one embodiment, each profile 220 comprises a profile history 222 and profile data 230. Many different types of profiles 220 are possible. A biometric profile, for example, includes profile data 230 representing physical and/or behavioral information that can uniquely identify the PDK owner. A PDK 102 can store multiple biometric profiles, each comprising a different type of biometric information. In one embodiment, the biometric profile 220 comprises biometric information transformed by a mathematical operation, algorithm, or hash that represents the complete biometric information (e.g., a complete fingerprint scan). In one embodiment, a mathematical hash is a "one-way" operation such that there is no practical way to re-compute or recover the complete biometric information from the biometric profile. This both reduces the amount of data to be stored and adds an additional layer of protection to the user's personal biometric information. In one embodiment, the PDK 102 also stores one or more biometric profile "samples" associated with each biometric profile. The biometric profile sample is a subset of the complete profile that can be used for quick comparisons of biometric data. In one embodiment, the profile samples can be transmitted over a public communication channel or transmitted with a reduced level of encryption while the full biometric profiles are only transmitted over secure channels. In the case of fingerprint authentication, for example, the biometric profile sample may represent only a small portion area of the full fingerprint image. In another embodiment, the fingerprint profile sample is data that describes an arc of one or more lines of the fingerprint. In yet another embodiment, the fingerprint profile sample can be data representing color information of the fingerprint.

[0056] In another embodiment, the stored profiles 220 include a PIN profile that stores one or more PINs or passwords associated with the PDK owner. Here, the number or

password stored in the PIN profile can be compared against an input provided by the user at the point of transaction to authenticate the user. In one embodiment, a PIN profile sample is also stored with the PIN profile that comprises a subset of the full PIN. For example, a PIN profile sample can be only the first two numbers of the PIN that can be used to quickly compare the stored PIN profile to a PIN obtained at the point of transaction.

[0057] In yet another embodiment, the PDK 102 stores a picture profile that includes one or more pictures of the PDK owner. In a picture profile authentication, the picture stored in the PDK 102 is transmitted to a display at the point of transaction to allow an administrator (e.g., a clerk or security guard) to confirm or reject the identity of the individual requesting the transaction. In another embodiment, an image is captured of the individual at the point of transaction and compared to the picture profile by an automated image analysis means. Furthermore, picture profiles could be used along with other personal identification information, for example, in place of conventional passports or drivers licenses to authenticate the identity of an individual and allow for remote identification of individuals. For example, a police officer following a vehicle could obtain an image and identity of the driver while still maintaining a safe distance from the vehicle. In the hospitality industry, a host could greet a guest at the door of a hotel, casino or restaurant and easily recognize the guest by obtaining the guest's picture profile as he/she enters.

[0058] In another embodiment, the PDK 102 stores purchase information for participating merchants. The PDK 102 also stores regularly ordered items for a particular merchant. In some embodiments, the regularly ordered items are stored as the customer's favorites.

[0059] A registry or database profile typically stores information associating the user with a registry. The registry profile can be used to determine if the individual is associated with the controlling entity for that registry and if different types of transactions are authorized for the individual. A registry profile can further include additional user information for use with the registry. For example, a private registry profile associated with a particular merchant may include a credit card number that the user has selected as a default for that merchant. In one embodiment, a profile can further include spending limits that limits the amount of purchases a user can make with a particular vendor or using a particular profile.

[0060] A profile can further include personal identification information such as name, address, phone number, etc., bank information, credit/debit card information, or membership information. This information can be useful for certain types of transactions. For example, with purchases that require delivery, a PDK 102 can automatically transmit address

information to the reader 108 at the point of transaction. In one embodiment, a profile can store multiple addresses. At the point of transaction, the reader 108 displays the address options and allows the user to select which address to use.

[0061] Generally, some types of profile information (e.g., a biometric profile) can only be acquired during a trusted initialization process that is administered by a trusted Notary. In one embodiment, other secure information such as credit card information is also stored to the PDK in the presence of a Notary. Alternatively, certain types of low-risk information can be added by the user without a Notary, such as, for example a change of address. In another embodiment, once an initial profile has been stored to the PDK 102, a user can add information to the PDK 102 using a Programmer without a Notary through self-authentication. For example, in one embodiment, a PDK 102 that has a stored biometric profile can be "unlocked" by providing a matching biometric input. Then, once unlocked, the user can add additional profiles, credit cards, personal information, etc. to the PDK 102. In another embodiment, the user can make copies of the PDK 102 or move profiles from one PDK 102 to another once the PDK 102 is unlocked.

[0062] The profile history 222 includes a programmer ID field 224, a Notary ID 226, and a site ID field 228. The profile history 222 relates to the specific hardware, Notary, and site used at the time the profile data was created and stored to the PDK. Typically each profile 220 stores its specific profile history 222 along with the profile data 230. The profile history 222 can be recalled for auditing purposes at a later time to ensure the credibility of the stored data. In one embodiment, transaction history can also be stored to the PDK memory 210. Here, the PDK 102 stores information associated with any transactions made with the PDK 102 such as the name of the merchant, the purchase amount, credit card used, etc.

[0063] The PDK 102 also includes a programmer I/O 240 that provides an interface to a trusted Programmer (not shown). The Programmer comprises trusted hardware that is used to program the memory 210 of the PDK 102. An example embodiment of a Programmer is described in U.S. Patent Application No. 11/744,832 (Attorney Docket No. 25000-12784) entitled "Personal Digital Key Initialization and Registration For Secure Transaction", the entire contents of which are incorporated herein by reference. The programmer I/O 240 can be, for example, a USB interface, serial interface, parallel interface, or any other direct or wireless link for transferring information between the PDK 102 and the Programmer. When coupled to the Programmer, the programmer I/O 240 receives initialization data, registration data or other information to be stored in the memory 210.

[0064] The control logic 250 coordinates between functions of the PDK 102. In one embodiment, the control logic 250 facilitates the flow of information between the programmer I/O 240, transceiver 260 and memory 210. The control logic 250 can further process data received from the memories 210, programmer I/O 240 and transceiver 260. Note that the control logic 250 is merely a grouping of control functions in a central architecture, and in other embodiments, the control functions can be distributed between the different modules of the PDK 102. The operation of the control logic will be understood to those skilled in the art based on the description below corresponding to Figs. 6-9D.

[0065] The transceiver 260 is a wireless transmitter and receiver for wirelessly communicating with a reader 108 or other wireless device. The transceiver 260 can send and receive data as modulated electromagnetic signals. Moreover, the data can be encrypted by the transceiver 260 and transmitted over a secure link. Further, the transceiver 260 can actively send connection requests, or can passively detect connection requests from another wireless source. In one embodiment, the transceiver 260 is used in place of a separate programmer I/O 240 and is used to wirelessly communicate with the Programmer for programming. In one embodiment, the transceiver 260 is adapted to communicate over a range of up to around 5 meters.

[0066] Optionally, a PDK 102 can also include a built in biometric reader (not shown) to acquire a biometric input from the user. The biometric input can be used to unlock the PDK 102 for profile updates, or for various types of authentication. For example, in one embodiment, a biometric input is received by the PDK 102 and compared to stored biometric information. Then, if the user is authenticated, the PDK 102 can indicate to the Reader 108 that the user is authenticated and transmit additional information (e.g., a credit card number) needed to complete a transaction.

[0067] FIG. 2B is a block diagram illustrating a biometric reader 270 of a PDK 102 according to one embodiment of the invention. The biometric reader 270 includes a biometric capture module 292, a validation module 294, an enrollment module 296 and persistent storage 298. In one embodiment, the enrollment module 296 registers a user with a PDK 102 by persistently storing biometric data associated with the user. Further, enrollment module 296 registers PDK 102 with a trusted authority by providing the code (e.g., device ID) to the trusted authority. Or conversely, the trusted authority can provide the code to PDK 102 to be stored therein.

[0068] The biometric capture module 292 comprises a scan pad to capture scan data from a user's fingerprint (e.g., a digital or analog representation of the fingerprint). Other

embodiments of the biometric capture module 292 includes retinal scanners, iris scanners, facial scanner, palm scanners, DNA/RNA analyzers, signature analyzers, cameras, microphones, and voice analyzers to capture other identifying biometric data. Using the biometric data, validation module 294 determines whether the user's fingerprint, or other biometric data, matches the stored biometric data from enrollment. Conventional techniques for comparing fingerprints can be used. For example, the unique pattern of ridges and valleys of the fingerprints can be compared. A statistical model can be used to determine comparison results. Validation module 294 can send comparison results to control logic 250 of the PDK 102.

[0069] In other embodiments, validation module 294 is configured to capture biometric data for other human characteristics. For example, a digital image of a retina, iris, and/or handwriting sample can be captured. In another example, a microphone captures a voice sample.

[0070] Persistent storage 298 persistently stores biometric data from one or more users which can be provided according to specific implementations. In one embodiment, at least some of persistent storage 298 is a memory element that can be written to once but cannot subsequently be altered. Persistent storage 298 can include, for example, a ROM element, a flash memory element, or any other type of non-volatile storage element. Persistent storage 298 is itself, and stores data in, a tamper-proof format to prevent any changes to the stored data. Tamper-proofing increases reliability of authentication because it does not allow any changes to biometric data (i.e., allows reads of stored data, but not writes to store new data or modify existing data). Furthermore, data can be stored in an encrypted form.

[0071] In one embodiment, persistent storage 298 also stores the code that is provided by the PDK 102 responsive to successful verification of the user. Further, in some embodiments persistent storage 298 stores other data utilized during the operation of PDK 102. For example, persistent storage 298 can store encryption/decryption keys utilized to establish secure communications links.

[0072] An example embodiment of PDK with a biometric reader is described in U.S. Patent Application No. 11/314,199 (Attorney Docket No. 25000-11062) to John Giobbi, et al., entitled "Biometric Personal Data Key (PDK) Authentication", the entire contents of which are incorporated herein by reference.

[0073] Turning now to FIG. 3, an example embodiment of a Reader 108 is illustrated. The embodiment includes one or more biometric readers 302, a receiver-decoder circuit (RDC) 304, a processor 306, a network interface 308, an I/O port 312 and optionally a credit

card terminal I/O 310. In alternative embodiments, different or additional modules can be included in the Reader 108.

[0074] The RDC 304 provides the wireless interface to the PDK 102. Generally, the RDC 304 wirelessly receives data from the PDK 102 in an encrypted format and decodes the encrypted data for processing by the processor 306. An example embodiment of an RDC is described in U.S. Patent Application No. 11/292,330 entitled "Personal Digital Key And Receiver/Decoder Circuit System And Method", the entire contents of which are incorporated herein by reference. Encrypting data transmitted between the PDK 102 and Reader 108 minimizes the possibility of eavesdropping or other fraudulent activity. In one embodiment, the RDC 304 is also configured to transmit and receive certain types of information in an unencrypted, or public, format.

[0075] The biometric reader 302 receives and processes the biometric input 104 from an individual at the point of transaction. In one embodiment, the biometric reader 302 is a fingerprint scanner. Here, the biometric reader 302 includes an image capture device adapted to capture the unique pattern of ridges and valleys in a fingerprint also known as minutiae. Other embodiments of biometric readers 302 include retinal scanners, iris scanners, facial scanner, palm scanners, DNA/RNA analyzers, signature analyzers, cameras, microphones, and voice analyzers. Furthermore, the Reader 108 can include multiple biometric readers 302 of different types. In one embodiment, the biometric reader 302 automatically computes mathematical representations or hashes of the scanned data that can be compared to the mathematically processed biometric profile information stored in the PDK 102.

[0076] The processor 306 can be any general-purpose processor for implementing a number of processing tasks. Generally, the processor 306 processes data received by the Reader 108 or data to be transmitted by the Reader 108. For example, a biometric input 104 received by the biometric reader 302 can be processed and compared to the biometric profile 220 received from the PDK 102 in order to determine if a transaction should be authorized. In different embodiments, processing tasks can be performed within each individual module or can be distributed between local processors and a central processor. The processor 306 further includes a working memory for use in various processes such as performing the method of Figs. 6-9D.

[0077] The network interface 308 is a wired or wireless communication link between the Reader 108 and one or more external databases such as, for example, a validation database 112, the Central Registry 114 or a private registry 116. For example, in one type of authentication, information is received from the PDK 102 at the RDC 304, processed by the

processor 306, and transmitted to an external database 112-116 through the network interface 308. The network interface 308 can also receive data sent through the network 110 for local processing by the Reader 108. In one embodiment, the network interface 308 provides a connection to a remote system administrator to configure the Reader 108 according to various control settings.

[0078] The I/O port 312 provides a general input and output interface to the Reader 108. The I/O port 312 may be coupled to any variety of input devices to receive inputs such as a numerical or alphabetic input from a keypad, control settings, menu selections, confirmations, and so on. Outputs can include, for example, status LEDs, an LCD, or other display that provides instructions, menus or control options to a user.

[0079] The credit card terminal I/O 310 optionally provides an interface to an existing credit card terminal 314. In embodiments including the credit card terminal I/O 310, the Reader 108 supplements existing hardware and acts in conjunction with a conventional credit card terminal 314. In an alternative embodiment, the functions of an external credit card terminal 314 are instead built into the Reader 108. Here, a Reader 108 can completely replace an existing credit card terminal 314.

[0080] In one embodiment, a Reader 108 is adapted to detect and prevent fraudulent use of PDKs that are lost, stolen, revoked, expired or otherwise invalid. For example, the Reader 108 can download lists of invalid PDKs 102 from a remote database and block these PDKs 102 from use with the Reader 108. Furthermore, in one embodiment, the Reader 108 can update the blocked list and/or send updates to remote registries 114-116 or remote Readers 108 upon detecting a fraudulently used PDK 102. For example, if a biometric input 104 is received by the Reader 108 that does not match the biometric profile received from the PDK 102, the Reader 108 can obtain the PDK ID 212 and add it to a list of blocked PDKs. In another embodiment, upon detecting fraudulent use, the Reader 108 can send a signal to the PDK 102 that instructs the PDK 102 to deactivate itself. The deactivation period can be, for example, a fixed period of time, or until the rightful owner requests re-activation of the PDK 102. In yet another embodiment, the Reader 108 can send a signal instructing the fraudulently obtained PDK 102 to send beacon signals indicating that the PDK 102 is a stolen device. Here, a stolen PDK 102 can be tracked, located and recovered by monitoring the beacon signals. In one embodiment, the Reader 108 stores biometric or other identifying information from an individual that attempts to fraudulently use a PDK 102 so that the individual's identity can be determined.

[0081] Generally, the Reader 108 is configured to implement at least one type of authentication prior to enabling a transaction. In many cases, multiple layers of authentication are used. A first layer of authentication, referred to herein as "device authentication", begins any time a PDK 102 moves within range of a Reader 108. In device authentication, the Reader 108 and the PDK 102 each ensure that the other is valid based on the device characteristics, independent of any profiles stored in the PDK 102. In some configurations, when fast and simple authentication is desirable, only device authentication is required to initiate the transaction. For example, a Reader 108 may be configured to use only device authentication for low cost purchases under a predefined amount (e.g., $25). The configuration is also useful in other types of low risk transactions where speed is preferred over additional layers of authentication.

[0082] Other configurations of the Reader 108 require one or more additional layers of authentication, referred to herein as "profile authentication" based on one or more profiles stored in the PDK 102. Profile authentication can include, for example, a biometric authentication, a PIN authentication, a photo authentication, a registry authentication, etc. or any combination of the above authentication types. Profile authentications are useful when a more exhaustive authentication process is desired, for example, for high purchase transactions or for enabling access to classified assets.

[0083] FIG. 4A is a block diagram illustrating a customer interface device 120A according to one embodiment of the invention. In one embodiment, the customer interface device 120A is a personal computer. In another embodiment, the customer interface device 120A is a smart phone or other mobile computing and communication device. Illustrated are at least one processor 402 coupled to a bus 404. Also coupled to the bus 404 are a memory 406, a storage device 408, a keyboard 410, a graphics adapter 412, a pointing device 414, a network adapter 416 and a reader 420. In one embodiment, the functionality of the bus 404 is provided by an interconnecting chipset. A display 418 is coupled to the graphics adapter 412. In one embodiment, the display 418 is a touch screen display adapted to receive inputs via the screen of the display 418.

[0084] The memory 406 includes an automated order application 430 and a rewards presentation application 436. In one embodiment, the automated order application 430 enables the customer interface device 120A to communicate with the transactions server 140. In another embodiment, the automated order application 430 processes information and data received from the readers 420 and various modules and servers of the transactions server 140. The rewards presentation application 436 is adapted to communicate with the rewards

processing module 1412 of the transactions server 140 to display the status of the customer's rewards on the display 418 of the customer interface device 120A. More details describing the functionality of these applications 430, 436 is provided below with reference to FIGS. 18 and 19.

[0085] The storage device 408 is any device capable of holding data, like a hard drive, compact disk read-only memory (CD-ROM), DVD, or a solid-state memory device. The memory 406 holds instructions and data used by the processor 402. The pointing device 414 may be a mouse, track ball, or other type of pointing device, and is used in combination with the keyboard 410 to input data into the customer interface device 120A. The graphics adapter 412 displays images and other information on the display 418. The network adapter 416 couples the customer interface device 120A to a local or wide area network.

[0086] As is known in the art, a customer interface device 120A can have different and/or other components than those shown in FIG. 4. In addition, the customer interface device 120A can lack certain illustrated components. In one embodiment, a customer interface device 120A lacks a keyboard 410, pointing device 414, graphics adapter 412, and/or display 418. Moreover, the storage device 408 can be local and/or remote from customer interface device 120A (such as embodied within a storage area network (SAN)). The reader 420 includes all or some of the same components as the Reader 108 as shown in FIG. 3.

[0087] As is known in the art, the customer interface device 120A is adapted to execute computer program modules for providing functionality described herein. As used herein, the term "module" refers to computer program logic utilized to provide the specified functionality. Thus, a module can be implemented in hardware, firmware, and/or software. In one embodiment, program modules are stored on the storage device 408, loaded into the memory 406, and executed by the processor 402.

[0088] Embodiments of the entities described herein can include other and/or different modules than the ones described here. In addition, the functionality attributed to the modules can be performed by other or different modules in other embodiments. Moreover, this description occasionally omits the term "module" for purposes of clarity and convenience.

[0089] FIG. 4B is a block diagram illustrating a customer interface device 120B according to another embodiment of the invention. As shown in FIG. 4B, the customer interface device 120B of FIG. 4B includes all or some of the same components as the customer interface device 120B of FIG. 4A. However, memory 406 of the customer interface device 120A of FIG. 4B includes additional applications for order entry, order processing and payment processing.

[0090] The memory 406 in FIG. 4B includes an automated order application 430, an order processing application 432 and a payment processing application 434. The applications 430, 432, 434 enable the customer interface device 120B to communicate with the modules 1406, 1408, 1412 of the transactions server 140 and the validation database 112 and registries 114, 116a, 116b of the system 100. The applications 430, 432, 434 enable a customer to place their order and pay for their order in one transaction. The automated order application 430 allows a customer to initiate an order by simply possessing a PDK. In one embodiment, automated order application 430 allows a customer to initiate an order by simply possessing a PDK and providing a biometric sample. The order processing application 432 processes the customer's order by communicating with the order processing module 1406 and order completion module 1408. The payment processing application 434 allows a customer to pay for their order after entering the order by simply providing a biometric sample, such as a finger swipe, or some other form of authentication. The rewards presentation application 436 is adapted to communicate with the rewards processing module 1412 of the transactions server 140 to display the status of the customer's rewards on the display 418 of the customer interface device 120B. More details describing the functionality of this application 430 is provided below with reference to FIGS. 18 and 19.

[0091] FIG. 4C is a block diagram illustrating a customer interface device 150 according to yet another embodiment of the invention. As shown in FIG. 4C, the customer interface device 150 of FIG. 4C includes all or some of the same components as the customer interface devices 120A of FIG. 4A and 120B of FIG. 4B. However, memory 406 of the customer interface device 150 of FIG. 4C includes an application for initializing and updating customer data.

[0092] As shown in FIG. 4C, customer interface device 150 includes an information update application 450. The information update application 450 enables the customer interface device 150 to communicate with the transactions server 140 via the network 110. Specifically, the information update application 450 enables the customer interface device 150 to communicate with the PDK initialization module 1402 and customer database 1410 of the transactions server 140. The information update application 450 allows a customer to initialize a PDK by entering their identifying information, including payment information, via the customer interface device 150. The information update application 450 also allows a customer to update information, including payment information, on the customer's PDK. More details describing the functionality of the customer interface device 150 is provided below with reference to FIG. 16.

[0093] FIG. 5A is a block diagram illustrating a merchant interface device 130A according to one embodiment of the invention. In one embodiment, the merchant interface device 130A is a personal computer. In another embodiment, the merchant interface device 130A is a smart phone or other mobile computing and communication device. Illustrated are at least one processor 502 coupled to a bus 504. Also coupled to the bus 504 are a memory 506, a storage device 508, a keyboard 510, a graphics adapter 512, a pointing device 514, a network adapter 516 and a reader 520. In one embodiment, the functionality of the bus 504 is provided by an interconnecting chipset. A display 518 is coupled to the graphics adapter 512. In one embodiment, the display 518 is a touch screen display adapted to receive inputs via the screen of the display 518.

[0094] The memory 506 includes an order completion application 530 and a rewards presentation application 532. In one embodiment, the order completion application 530 enables the merchant interface device 130A to communicate with the transactions server 140. In another embodiment, the order completion application 530 processes information and data received from the readers 520 and various modules and servers transactions server 140. The rewards presentation application 532 is adapted to communicate with the rewards processing module 1412 of the transaction server 140 in order to present the status of a customer's rewards on the display 518 of the merchant interface device 130A. More details describing the functionality of these applications 530, 532 is provided below with reference to FIGS. 20 and 21.

[0095] The storage device 508 is any device capable of holding data, like a hard drive, compact disk read-only memory (CD-ROM), DVD, or a solid-state memory device. The memory 506 holds instructions and data used by the processor 502. The pointing device 514 may be a mouse, track ball, or other type of pointing device, and is used in combination with the keyboard 510 to input data into the merchant interface device 130A. The graphics adapter 512 displays images and other information on the display 518. The network adapter 516 couples the merchant interface device 130A to a local or wide area network.

[0096] As is known in the art, a merchant interface device 130A can have different and/or other components than those shown in FIG. 5A. In addition, the merchant interface device 130A can lack certain illustrated components. In one embodiment, a merchant interface device 130A lacks a keyboard 510, pointing device 514, graphics adapter 512, and/or display 518. Moreover, the storage device 508 can be local and/or remote from merchant interface device 130A (such as embodied within a storage area network (SAN)). The reader 520 includes all or some of the same components as the Reader 108 as shown in FIG. 3.

[0097] As is known in the art, the merchant interface device 130A is adapted to execute computer program modules for providing functionality described herein. As used herein, the term "module" refers to computer program logic utilized to provide the specified functionality. Thus, a module can be implemented in hardware, firmware, and/or software. In one embodiment, program modules are stored on the storage device 508, loaded into the memory 506, and executed by the processor 502.

[0098] FIG. 5B is a block diagram illustrating a merchant interface device 130B according to another embodiment of the invention. The merchant interface device 130B of FIG. 5B includes all or some of the same components as the merchant interface device 130A of FIG. 5A. However, memory 506 of the merchant interface device 130B includes different applications for order presentations.

[0099] As shown in FIG. 5B, memory 506 of merchant interface device 130B includes an order presentation application 550. The order presentation application 550 is adapted to communication with the order processing module 1406 and order completion module 1408 of the transaction server 140 to display customers' orders. In one embodiment, the order presentation application 550 displays a list of customers' order. In another embodiment, the order presentation application 550 displays the list of customers' orders in the order that they were entered. The order presentation application 550 allows a merchant to visually see the orders that need to be prepared. In one embodiment, the order presentation application 550 allows the merchant to select an order to prepare and delete that order once the order has been prepared. More details describing the functionality of this application 550 and this embodiment of the merchant interface device 130B is provided below with reference to FIGS. 20 and 21B.

[0100] Embodiments of the entities described herein can include other and/or different modules than the ones described here. In addition, the functionality attributed to the modules can be performed by other or different modules in other embodiments. Moreover, this description occasionally omits the term "module" for purposes of clarity and convenience.

[0101] FIG. 6 is a flowchart illustrating one embodiment of a process for authorizing a communication connection using secure authentication. When a PDK 102 comes within range of a Reader 108, communication is automatically established 602 between the RDC 304 of the Reader 108 and the PDK 102. In one embodiment, the RDC 304 continually transmits beacons that are detected by the PDK 102 when it enters a proximity zone of the Reader 108. In an alternative embodiment, the communication is instead initiated by the PDK 102 and acknowledged by the Reader 108. Generally, initial communication between

the Reader 108 and the PDK 102 is not encrypted in order to provide faster and more power efficient communication.

[0102] In step 604, a device authentication is performed. Here, the Reader 108 establishes if the PDK 102 is a valid device and PDK 102 establishes if the Reader 108 is valid. Furthermore, device authentication determines if the PDK is capable of providing the type of authentication required by the Reader 108.

[0103] An example embodiment of a method for performing 604 device authentication is illustrated in FIG. 7. The RDC 304 receives and analyzes 702 information from the PDK 102; and the PDK 102 receives and analyzes 702 information received from the RDC 304. Generally, this initial information is transmitted over a public communication channel in an unencrypted format. Based on the received information, each device 102, 304 determines 704 if the other is valid. As will be apparent to one of ordinary skill in the art, a number of different protocols can be used for this type of authentication such as, for example, a challenge-response authentication or a challenge handshake authentication protocol (CHAP). If either of the devices 102, 304 is invalid 712, the process ends. If both the PDK 102 and the RDC 304 are determined by the other to be valid, the Reader 108 requests and receives 706 authentication type information from the PDK 102 indicating the different types of authentication the PDK 102 is capable of satisfying based on the types of profiles the PDK 102 stores. The available profile types in the PDK 102 are compared against the authentication types that can be used by the Reader 108. For example, a particular Reader 108 may be configured to perform only a fingerprint authentication and therefore any PDK without a fingerprint biometric profile cannot be used with the Reader 108. In one embodiment, the Reader 108 can allow more than one type of profile to be used. In another embodiment, the Reader 108 requires more than one type of profile for authentication, while in yet further embodiments no profile authentications are required. Next, the method determines 708 whether the PDK 102 has one or more profiles sufficient for authentication. If the PDK 102 does not have one or more profiles sufficient for authentication with the Reader 108, the devices 102, 304 are determined to be invalid 712 because they cannot be used with each other. If the PDK 102 does have one or more sufficient types of profiles, the devices are valid 710.

[0104] Turning back to FIG. 6, if either the PDK 102 or RDC 304 is not found valid during device authentication 604, the transaction is not authorized 618 and the process ends. If the devices are valid, the RDC 304 temporarily buffers 608 the received PDK information. It is noted that in one embodiment, steps 602-608 are automatically initiated each time a PDK

102 enters the proximity zone of the Reader 108. Thus, if multiple PDKs 102 enter the proximity zone, the Reader 108 automatically determines which PDKs 102 are valid and buffers the received information from each valid PDK 102.

[0105] The method next determines 610 whether profile authentication is required based on the configuration of the Reader 108, the type of transaction desired or by request of a merchant or other administrator. If the Reader 108 configuration does not require a profile authentication in addition to the PDK authentication, then the Reader 108 proceeds to complete the transaction for the PDK 102. If the Reader 108 does require profile authentication, the profile authentication is performed 612 as will be described below with references to Figs 8-9D. If a required profile is determined 614 to be valid, the Reader 108 completes 616 the transaction. Otherwise, the Reader 108 indicates that the transaction is not authorized 618. In one embodiment, completing 616 the transaction includes enabling access to secure physical or digital assets (e.g., unlocking a door, opening a vault, providing access to a secured hard drive, etc.). In another embodiment, completing 416 the transaction includes charging a credit card for a purchase. Alternatively, bank information, debit/check/ATM card information, coupon codes, or any other purchasing means information (typically stored in a profile memory field 232) can be transmitted by the PDK 102 in place of credit card information. In one embodiment, the PDK 102 is configured with multiple purchasing means and a default is configured for different types of transactions. In another embodiment, each credit card or other purchasing means is displayed to the customer by the Reader 108 and the customer is allowed to select which to use for the transaction.

[0106] Turning now to FIG. 8, an embodiment of a process for profile authentication is illustrated. In step 802, a secure communication channel is established between the RDC 304 and the PDK 102. Information sent and received over the secure channel is in an encrypted format that cannot be practically decoded, retransmitted, reused, or replayed to achieve valid responses by an eavesdropping device. The Reader 108 transmits 804 profile authentication requests to the PDK 102 requesting transmission of one or more stored profiles over the secure channel. At 808, the process determines whether a "trigger" is required for authentication. The requirement for a trigger depends on the configuration of the Reader 108, the specific type of transaction to be executed and the type of authentication requested.

[0107] In a first configuration, a trigger is required to continue the process because of the type of authentication being used. For example, in biometric authentication, the authentication process cannot continue until the Reader detects a biometric contact and receives biometric information. It is noted that biometric contact is not limited to physical

contact and can be, for example, the touch of a finger to a fingerprint scanner, the positioning of a face in front of a facial or retinal scanner, the receipt of a signature, the detection of a voice, the receipt of a DNA sample, RNA sample, or derivatives or any other action that permits the Reader 108 to begin acquiring the biometric input 104. By supplying the biometric contact, the user indicates that the authentication and transaction process should proceed. For example, a PDK holder that wants to make a withdrawal from an Automated Teller Machine (ATM) equipped with a Reader 108 initiates the withdrawal by touching a finger to the Reader 108. The ATM then begins the transaction process for the withdrawal.

[0108] In a second configuration, some other user action is required as a trigger to proceed with the transaction even if the authentication process itself doesn't necessarily require any input. This can be used for many purchasing transactions to ensure that the purchase is not executed until intent to purchase is clear. For example, a Reader 108 at a gas station can be configured to trigger the transaction when a customer begins dispensing gas. At a supermarket, a Reader 108 can be configured to trigger the transaction when items are scanned at a checkout counter.

[0109] In a third configuration, no trigger is used and the Reader 108 automatically completes the remaining authentication/transaction with no explicit action by the user. This configuration is appropriate in situations where the mere presence of a PDK 102 within range of the Reader 108 is by itself a clear indication of the PDK owner's desire to complete a transaction. For example, a Reader 108 can be positioned inside the entrance to a venue hosting an event (e.g., a sporting event, a concert, or a movie). When a PDK owner walks through the entrance, the Reader 108 detects the PDK 102 within range, authenticates the user, and executes a transaction to purchase an electronic ticket for the event. In another embodiment, the electronic ticket can be purchased in advance, and the Reader 108 can confirm that the user is a ticket holder upon entering the venue. Other examples scenarios where this configuration is useful include boarding a transportation vehicle (e.g., a train, bus, airplane or boat), entering a hotel room, or accessing secure facilities or other assets. Thus, if no trigger is required, the process next performs 814 the requested profile authentication tests.

[0110] If a trigger is required, the Reader monitors 810 its inputs (e.g., a biometric reader, key pad, etc.) and checks for the detection 812 of a trigger. If the required trigger is detected, the process continues to perform 814 one or more profile authentication test. Figs. 9A-9D illustrate various embodiments of profile authentication tests. According to different configurations of the Reader 108, one or more of the illustrated authentication processes may

be used. Further, in some embodiments, one or more of the processes may be repeated (e.g., for different types of biometric inputs).

[0111] Referring first to FIG. 9A, it illustrates a process for biometric authentication. In biometric authentication, a Reader 108 compares a biometric profile stored in the PDK 102 to the biometric input 104 acquired by the biometric reader 302. Advantageously, the biometric input 104 is not persistently stored by the Reader 108, reducing the risk of theft or fraudulent use. If 902 biometric authentication is requested, the Reader 108 scans 904 the biometric input 104 supplied by the user. In one embodiment, scanning 904 includes computing a mathematical representation or hash of the biometric input 104 that can be directly compared to the biometric profile.

[0112] Furthermore, in one embodiment, scanning 904 also includes obtaining a biometric input sample from the biometric input according to the same function used to compute the biometric profile sample stored in the PDK 102. Optionally, the Reader 108 receives 908 a biometric profile sample from the PDK 102 and determines 910 if the biometric profile sample matches the biometric input sample. If the biometric profile sample does not match the input sample computed from the scan, the profile is determined to be invalid 918. If the biometric profile sample matches, the full biometric profile 912 is received from the PDK 102 to determine 914 if the full biometric profile 912 matches the complete biometric input 104. If the profile 912 matches the scan, the profile 912 is determined to be valid 920, otherwise the profile 912 is invalid 918. It is noted that in one embodiment, steps 908 and 910 are skipped and only a full comparison is performed.

[0113] It will be apparent to one of ordinary skill that in alternative embodiments, some of the steps in the biometric profile authentication process can be performed by the PDK 102 instead of the Reader 108 or by an external system coupled to the Reader 108. For example, in one embodiment, the biometric input 104 can be scanned 904 using a biometric reader built into the PDK 102. Furthermore, in one embodiment, the steps of computing the mathematical representation or hash of the biometric input 104 and/or the steps of comparing the biometric input 104 to the biometric profile can be performed by the PDK 102, by the Reader 108, by an external system coupled to the Reader 108, or by any combination of the devices. In one embodiment, at least some of the information is transmitted back and forth between the PDK 102 and the Reader 108 throughout the authentication process. For example, the biometric input 104 can be acquired by the PDK 102, and transmitted to the Reader 108, altered by the Reader 108, and sent back to the PDK 102 for comparison. Other variations of information exchange and processing are possible without departing from the

scope of the invention. The transfer of data between the PDK 102 and the Reader 108 and/or sharing of processing can provide can further contribute to ensuring the legitimacy of each device.

[0114] FIG. 9B illustrates a process for PIN authentication. If PIN authentication is requested 924, a PIN is acquired 926 from the user through a keypad, mouse, touch screen or other input mechanism. Optionally, the Reader 108 receives 928 a PIN sample from the PDK 102 comprising a subset of data from the full PIN. For example, the PIN sample can comprise the first and last digits of the PIN. If the Reader 108 determines 930 that the PIN sample does not match the input, the profile is immediately determined to be invalid 936. If the PIN sample matches, the full PIN profile is received 932 from the PDK and compared to the input. If the Reader 108 determines 934 that the profile matches the input, the profile is determined to be valid and is otherwise invalid 936. It is noted that in one embodiment, steps 928 and 930 are skipped.

[0115] FIG. 9C illustrates a process for a picture authentication. If the Reader 108 determines 924 that picture authentication is requested, a picture profile is received 944 from the PDK 102 by the Reader 108 and displayed 946 on a screen. An administrator (e.g., a clerk, security guard, etc.) is prompted 948 to compare the displayed picture to the individual and confirms or denies if the identities match. If the administrator confirms that the identities match, the picture profile is determined to be valid 964 and is otherwise invalid 952. In an alternative embodiment, the process is automated and the administrator input is replaced with a process similar to that described above with reference to FIG. 9A. Here, an image of the user is captured and face recognition is performed by comparing picture profile information received from the PDK 102 to the captured image.

[0116] FIG. 9D illustrates a process for authentication with a private registry 114 or the Central Registry 116. If the Reader 108 determines that registry authentication is requested, a secure communication channel is established 962 over the network 110 between the Reader 108 and one or more registries (e.g., the Central Registry 114, any private registry 116, or other validation database 112). If any additional information is needed to process the registry authentication (e.g., a credit card number), the Reader 108 requests and receives the additional information from the PDK 102. Identification information is transmitted 964 from the Reader 108 to the registry 114-116 through the network interface 308. The PDK status is received 966 from the registry to determine 968 if the status is valid 972 or invalid 970. In one embodiment, the information is processed remotely at the registry 114-116 and the registry 114-116 returns a validation decision to the Reader 108. In another embodiment, the

Reader 108 queries the private 116 or Central registry 114 for information that is returned to the Reader 108. The information is then analyzed by the Reader 108 and the authorization decision is made locally. In one embodiment, the process involves transmitting credit card (or other purchasing information) to a validation database 112 to authorize the purchase and receive the status of the card. Status information may include, for example, confirmation that the card is active and not reported lost or stolen and that sufficient funds are present to execute the purchase.

[0117] FIG. 10 illustrates an example scenario of a reader operating in a congested area with multiple PDKs within its proximity zone. In this figure, a scenario is illustrated where multiple PDKs 102a-e are present near a Reader 108. This scenario is common when a Reader 108 is located in a high occupancy area such as, for example, a hospital lobby or waiting area. Here, the Reader 108 can communicate with PDKs 102a-d within the proximity zone 1002 and does not communicate with PDKs 102e-f outside the proximity zone 1002. In one embodiment, the Reader 108 receives the unique PDK ID from a PDK 102 when it enters the proximity zone 1002 and records its time of arrival. In one embodiment, the Reader 108 further initiates a device authentication of the PDK 102 after a predefined period of time (e.g., 5 seconds) that the PDK 102 is within the proximity zone 1002. For profile authentication, the Reader 108 automatically determines which PDK 102 should be associated with an authentication test and the transaction. For example, if the Reader 108 receives a biometric input 102 from an individual, the Reader 108 automatically determines which PDK 102a-d is associated with the individual supplying the biometric input 122. In another embodiment, a different trigger is detected (e.g., a PIN input) to initiate the differentiation decision. In yet another embodiment, the differentiation decision is initiated without any trigger. It is noted that in some embodiments, where no trigger is required (such as a registry authentication), no differentiation decision is made and authentications are instead performed for each PDK 102 within the proximity zone 1002.

[0118] FIG. 11 illustrates an embodiment of an authentication process 1100 for the scenario where multiple PDKs 102 are present within the proximity zone 1002 of the Reader 108. In a PDK data accumulation phase 1102, PDK data 1130 is accumulated and buffered in the Reader 108 for any valid PDKs 102 that enter the proximity zone 1002. In one embodiment, the accumulation phase 1102 begins for a PDK 102 after it has been within the proximity zone 1002 for a predetermined period of time. In one embodiment, the PDK data accumulation phase 1102 is similar to the steps 802-808 described above in detail with reference to FIG. 8 for each PDK 102a-d in the proximity zone 1002.

[0119] As illustrated, the accumulated PDK data 1130 includes one or more differentiation metrics from each valid PDK 102 within range of the Reader 108. The differentiation metrics can include any information that can be used by the Reader 108 to determine which PDK 102 should be associated with the authentication and/or transaction request. According to various embodiments, differentiation metrics can include one or more of distance metrics 1132, location metrics 1134 and duration metrics 1136.

[0120] In one embodiment, a distance metric 1132 indicates the relative distance of a PDK 102 to the Reader 108. This information is useful given that a PDK 102 having the shortest distance to the Reader 108 is generally more likely to be associated with a received authentication trigger (e.g., a biometric input, a PIN input or a transaction request). The distance metrics 1132 can include, for example, bit error rates, packet error rates and/or signal strength of the PDKs 102. These communication measurements can be obtained using a number of conventional techniques that will be apparent to those of ordinary skill in the art. Generally, lower error rates and high signal strength indicate the PDK 102 is closer to the Reader 108.

[0121] Location metrics 1134 can be used to determine a location of a PDK 102 and to track movement of a PDK 102 throughout an area. This information can be useful in determining the intent of the PDK holder to execute a transaction. For example, a PDK holder that moves in a direct path towards a cashier and then stops in the vicinity of the cashier is likely ready to make a purchase (or may be waiting in line to make a purchase). On the other hand, if the PDK moves back and forth from the vicinity of a cashier, that PDK holder is likely to be browsing and not ready to make a purchase. Examples of systems for determining location metrics are described in more detail below with reference to FIGs. 14-15.

[0122] The differentiation metrics can also include duration metrics 1136 that tracks the relative duration a PDK 102 remains within the proximity zone 1002. Generally, the PDK 102 with the longest time duration within the proximity zone 1002 is most likely to be associated with the authentication request. For example, if the Reader 108 is busy processing a purchasing transaction at a cashier and another PDK 102 has a long duration within the proximity zone 1002, it is likely that the user is waiting in line to make a purchase. In one embodiment, the Reader 108 tracks duration 1136 by starting a timer associated with a PDK 102 when the PDK 102 enters the proximity zone 1002 and resetting the time to zero when the PDK exists. As another example, the Reader 108 tracks the duration when a PDK of a doctor enters the proximity zone of a patient's room. A long duration of the doctor's PDK

within the proximity zone can provide evidence that the doctor is spending an adequate amount of time examining the patient. On the other hand, a short duration of the doctor's PDK within the proximity zone can provide evidence that the doctor just merely stopped by and did not perform any thorough examination. This information is useful in monitoring patient treatment and provider performance to help ensure quality patient care.

[0123] In one embodiment, the Reader 108 can also receive and buffer profile samples 1138 prior to the start of a profile authentication instead of during the authentication process as described in FIG. 11A-11B. In one embodiment, the Reader 108 determines which types of biometric profile samples 1138 to request based on, for example, the configuration of the Reader 108, the type of transactions performed by the Reader 108, or manual requests from a clerk, security guard, etc. In one embodiment, the PDK 102 transmits one or more of the requested sample types based on profiles available in the PDK 102 and/or user preferences. In another embodiment, the PDK 102 transmits one or more samples 1138 it has available and only samples that match the authentication types configured for the Reader 108 are buffered. For example, if a Reader 108 is configured for fingerprint authentication, a PDK 102 may transmit samples 1138 for several different fingerprint profiles (each corresponding to a different finger, for example). It will be apparent to one of ordinary skill in the art that other variations are possible to provide flexibility in both the configuration of the Reader 108 for various types of authentication and flexibility for the PDK owner to determine which types of authentication to use.

[0124] Because profile samples 1138 only comprise a subset of the profile information, in one embodiment, the samples can be safely transmitted over a public channel without needing any encryption. In another embodiment, the profile samples 1138 are transmitted with at least some level of encryption. In yet another embodiment, some of the data is transmitted over a public communication channel and additional data is transmitted over a secure communication channel. In different configurations, other types of profile information can be accumulated in advance. For example, in one embodiment, a photograph from a picture profile can be obtained by the Reader 102 during the data accumulation phase 1102. By accumulating the profile sample 1138 or other additional information in advance, the Reader 108 can complete the authentication process more quickly because it does not wait to receive the information during authentication. This efficiency becomes increasingly important as the number of PDKs 102 within the proximity zone 1002 at the time of the transaction becomes larger.

[0125] The PDK accumulation phase 1102 continues until a trigger (e.g., detection of a biometric input) is detected 1104 to initiate a profile authentication process. If a biometric input is received, for example, the Reader 108 computes a mathematical representation or hash of the input that can be compared to a biometric profile and computes one or more input samples from the biometric input. It is noted that in alternative embodiments, the process can continue without any trigger. For example, in one embodiment, the transaction can be initiated when a PDK 102 reaches a predefined distance from the Reader 108 or when the PDK 102 remains within the proximity zone 1002 for a predetermined length of time.

[0126] The process then computes a differentiation decision 1106 to determine which PDK 102a-d should be associated with the authentication. In one embodiment, the Reader 108 computes a differentiation result for each PDK using one or more of the accumulated data fields 1130. For example, in one embodiment, the differentiation result is computed as a linear combination of weighted values representing one or more of the differentiation metrics. In another embodiment, a more complex function is used. The differentiation results of each PDK 102 are compared and a PDK 102 is selected that is most likely to be associated with the transaction.

[0127] In another embodiment, for example, in a photo authentication, the differentiation decision can be made manually by a clerk, security guard, or other administrator that provides a manual input 1112. In such an embodiment, a photograph from one or more PDKs 102 within the proximity zone 1002 can be presented to the clerk, security guard, or other administrator on a display and he/she can select which individual to associate with the transaction. In yet another configuration, the decision is made automatically by the Reader 108 but the clerk is given the option to override the decision.

[0128] An authentication test 1108 is initiated for the selected PDK 102. The authentication test 908 can include one or more of the processes illustrated in FIGs. 11A-11D. Note that if profile samples 1138 are acquired in advance, they need not be acquired again in the authentication steps of FIGs. 11A-11B. It is additionally noted that in one embodiment, the Reader 108 compares the profile samples 1138 of the PDKs 102 to the computed input sample until a match is found before performing a full profile comparison. In one embodiment, the Reader first compares samples from the selected PDK 102 until a match is found. For example, a Reader 108 may have accumulated multiple fingerprint profiles samples 1138 (e.g., corresponding to different fingers) for the selected PDK 102. The Reader 108 receives a fingerprint input from, for example, the left index finger, computes the input sample, and does a quick comparison against the accumulated samples 1138 for the selected

PDK 102 to efficiently determine a matching profile. The Reader 108 then performs the full comparison using the matching profile. In an alternative embodiment, the Reader 108 performs a comparison of a first sample from each PDK 102 and if no match is found, performs comparisons of second samples from each PDK 102. It will be apparent to one of ordinary skill in the art that samples can be compared in a variety of other orders without departing from the scope of the invention.

[0129] If the authentication test 1108 indicates a valid profile, the transaction is completed 1110 for the matching PDK 102. If the authentication test 1108 determines the profile is invalid, a new differentiation decision 1106 is made to determine the next mostly likely PDK 102 to be associated with the transaction. The process repeats until a valid profile is found or all the PDKs 102 are determined to be invalid.

[0130] Turning now to FIG. 12, an example system is illustrated for determining a location metric 1134 of a PDK 102 using a coordinate triangulation technique. In one embodiment of coordinate triangulation, multiple transmitting devices (e.g., Readers 108a-c) are spaced throughout an area. In one embodiment, the Readers 108a-care coupled by a network. Each Reader 108a-c has a range 1204 and the ranges 1204 overlap. Each Reader 108a-c determines a distance D1-D3 between the Reader108 and the PDK 102. Distance may be estimated, for example, by monitoring signal strength and/or bit error rate as previously described. Then using conventional trigonometry, an approximate location of the PDK 102 can be calculated from D1-D3. Although only three transmitters are illustrated, it will be apparent that any number of transmitters can be used to sufficiently cover a desired area. Location information can be computed at predetermined time intervals to track the movement of PDKs throughout a facility.

[0131] Another embodiment of location tracking is illustrated in FIG. 13. Here, transmitters 1302 having ranges 1304 are distributed throughout an area. The ranges 1304 can vary and can be overlapping or non-overlapping. In this embodiment, each transmitter 1302 can detect when a PDK 102 enters or exists its range boundaries 1304. By time-stamping the boundary crossings, a location vector can be determined to track the PDK's movement. For example, at a first time, t1, the PDK 102 is detected within the range of transmitter 1302a. At a second time, t2, the PDK 102 is detected within the range of transmitter 1302b. At a third time, t3, the PDK 102 is within the range of transmitter 1302c and at a fourth time, t4, the PDK 102 is within the range of transmitter 1302d. Using the location and time information, approximate motion vectors, v1, v2, v3, and v4 can be

computed to track the motion of the PDK 102 without necessarily computing exact distance measurements.

[0132] FIG. 14 is a block diagram illustrating a transactions server 140 according to one embodiment of the invention. The transactions server 140 includes software or routines for automating the process of entering and fulfilling an order. The transactions server 140 facilitates automating order processing and payment procedures. The transaction server 140 is a hardware device, such as a computer designed to run applications for the aforementioned functions and processes. The transactions server 140 is adapted to communicate with the reader 108, the customer interface device 120 and the merchant interface device 130. The transactions server 140 includes a PDK initialization module 1402, a data update module 1404, an order processing module 1406, an order completion module 1408, a rewards processing module 1412 and a customer database 1410.

[0133] The PDK initialization module 1402 includes software or routines for initializing a PDK for use in the system 100. In one embodiment, the PDK initialization module 1402 is adapted to communicate with the customer interface device 150 via the network 110. In another embodiment, the PDK initialization module 1402 is adapted to communicate with the merchant interface device 130 via the network 110. The PDK initialization module 1402 facilitates the uploading of new customer information, such as biometric information and profile information, including payment information, to a new PDK. The PDK initialization module 1402 sends verification data to the merchant interface device 130. The PDK initialization module 1402 is also coupled to the customer database 1410 and sends some of the new customer information, such as profile information and payment information to the customer database 1410 for storage therein. More details describing the process performed by the PDK initialization module 1402 is provided below with reference to FIG. 16.

[0134] The data update module 1404 includes software or routines for updating PDK 102 data to the customer database 1410. The data update module 1404 is adapted to communicate with the reader 108 via the network 110 and is coupled to the customer database 1410. The data update module 1404 receives PDK 102 information, including customer information, from the reader 108 and uploads new PDK 102 information to the customer database 1410. The data update module 1404 facilitates the maintenance of current PDK information within the system 100. More details describing the process performed by the data update module 1404 is provided below with reference to FIG. 17.

[0135] The order processing module 1406 includes software or routines for automating the process of entering customer orders in system 100. The order processing module 1406 is

adapted to communicate with the customer interface device 120 via the network 110 and is coupled to the order completion module 1408, customer database 1410 and rewards processing module 1412. The order processing module 1406 processes data received from the customer interface device 120 and obtains data from the customer's PDK in order to process the orders. In some embodiments, the order processing module 1406 obtains data from the customer database 1410 in order to process the orders. The order processing module 1406 also sends order information to the rewards processing module 1412 in order to enable the determination of customer rewards based on order activity. The order processing module 1406 also sends order information to the order completion module 1408 in order to complete such orders. More details describing the process performed by the order processing module 1406 is provided below with reference to FIGS. 18 and 19.

[0136] The order completion module 1408 includes software or routines for automating the process of completing customer orders in system 100. The order completion module 1408 is adapted to communicate with the merchant interface device 130 via the network 110 and is coupled to the order processing module 1406 and customer database 1408. In some embodiments, the order completion module 1408 is adapted to communicate with the customer interface device 120. In one embodiment, the order completion module 1408 is also coupled to the rewards processing module 1412. The order completion module 1406 receives confirmed order information from the order processing module 1406 and sends completed order information to be displayed in the merchant interface device 130. In one embodiment, the order completion module 1406 receives confirmed order information from the order processing module 1406 and sends completed order information to be displayed in the customer interface device 120. In one embodiment, the order completion module 1408 sends order information to the rewards processing module 1412 in order to enable the determination of customer rewards based on order completion activity. More details describing the process performed by the order completion module 1408 is provided below with reference to FIGS. 20 and 21.

[0137] The customer database 1410 is coupled to and adapted to communicate with the PDK initialization module 1402, the data update module 1404, the order processing module 1406, the order completion module 1408 and the rewards processing module 1412. The customer database 1410 stores PDK 102 information as well as customer information associated with the PDKs 102. In one embodiment, the customer database 1410 is adapted to communicate with the validation database 112 and registries 114, 116a, 116b. In such embodiments, data from the customer database 1410 is replicated to the validation database

112 and registries 114, 116a, 116b to ensure maintenance of current customer information within the system 100.

[0138] The rewards processing module 1412 includes software or routines for processing and recording customer activity for the purposes of determining customer rewards. The rewards processing module 1412 is coupled to the order processing module 1406, the order completion module 1408 and the customer database 1410. The rewards processing module 1412 receives order information from the order processing module 1406 and determines customer rewards based on order activity. In one embodiment, the rewards processing module 1412 receives order information from the order completion module 1408 and determines customer rewards based on order completion activity. The rewards processing module 1412 sends reward information to the customer database 1014 to be stored therein. More details describing the process performed by the rewards processing module 1412 is provided below with reference to FIG. 22.

[0139] Embodiments of the entities described herein can include other and/or different modules than the ones described here. In addition, the functionality attributed to the modules can be performed by other or different modules in other embodiments. Moreover, this description occasionally omits the term "module" for purposes of clarity and convenience

[0140] FIG. 15 is a flowchart illustrating a general process 1500 for automated order processing according to one embodiment of the invention. The process 1500 is performed by the various modules 1404, 1406, 1408, 1412 of the transactions server 140. When a customer with an associated PDK 102 walks into a store, the connection is established 1502 between the customer's PDK 102 and the reader 108 and the customer's PDK 102 is authenticated 1502 by the reader 108. An example embodiment of a method for establishing 1502 connection and performing device authentication is illustrated in FIGS. 6 and 7.

[0141] The reader 108 then reads the customer's information from the PDK 102, such as customer name and favorite orders, and sends it to the transactions server 140. The data update module 1404 of the transaction server 140 uploads 1504 current PDK information received from the reader 108 to the customer database 1410 of the transactions server 140. Connection is then established 1506 between the reader 420 of the customer interface device 120 and the customer's PDK 102 and the customer's PDK 102 is authenticated 1506 be the reader 420. The order processing module 1406 obtains the customer information from the customer's PDK and processes 1508 the customer's order. In some embodiments, the rewards processing module 1412 processes 1510 rewards based on the customer's order. The processed order is sent to the order completion module 1408 and the transaction is completed

1512. In some embodiments, the customer's PDK establishes another connection between the reader 520 of the merchant interface device 130 in order to complete the order. More details describing the specific steps of this general process 1500 is provided below with reference to FIGS. 16-22.

[0142] FIG. 16 is a flowchart illustrating a process 1600 for initializing a PDK according to one embodiment of the invention. In one embodiment, the process is performed by the customer interface device 120C. In other embodiments, the process is performed by the merchant interface device 130A. For purposes of illustration, the flow chart will be described as being performed by the customer interface device 120C. Connection is established 1601 between the reader 420 and the customer's PDK 102 and the customer's PDK 102 is authenticated. The customer interface device 120C requests 1602 a biometric sample. In one embodiment, this request is displayed on the display 418 of the customer interface device 120C. A sample is received via the reader 420 of the customer interface device 120C. The biometric sample can be acquired by, for example, a fingerprint scan, iris scan, retinal scan, palm scan, face scan, DNA analysis, signature analysis, voice analysis or any other input mechanism that provides physical or behavioral characteristics uniquely associated with the individual. The customer interface device 120C then requests 1606 customer profile information. In one embodiment, the customer's profile information includes the customer's name, address, picture, list of frequently visited merchants, favorite orders associated with the merchants, birthday, telephone numbers, and email address. In one embodiment, this request is displayed on the display 418 of the customer interface device 120C. The customer interface device 120C receives 1608 the customer profile information via the input devices of the customer interface device 120C, such as the keyboard 410, pointing device 414 and/or display 418. Next, the customer interface device 120C requests 1610 payment information, such as a credit card number, debit card number, or gift card authorization number, along with other identifying and authorization information of the customer's payment method. The customer interface device 120C receives 1612 the payment information via the reader 420, keyboard 410, pointing device 414 and/or display 418 of the customer interface device 120C. Once all the data is received, the information update application 450 verifies 1614 the data and uploads the information to the customer's PDK 102. In some embodiments, some of the data, such as the customer profile information, is sent to the transactions server 140 to be saved in the customer database 1410. In one embodiment, verification of the data includes storing the customer information and associating the customer information with a particular

PDK 102. Finally, the PDK 102 is initialized 1616 and ready to be used. In one embodiment initialization of the PDK 102 includes activating the PDK 102 for initial use.

[0143] In some embodiments, a customer can add or edit information with the process described above. For example, if a customer receives a gift card for a particular merchant, the customer can add the information detailing the merchant associated with the gift card and the amount of the gift card and that information is loaded onto the customer's PDK 102 for later use at the merchant's establishment. Connection is established 1601 between the reader 420 and the customer's PDK 102 and the customer's PDK 102 is authenticated. Optionally, biometric sample is requested 1602. A sample is received via the reader 420 of the customer interface device 120C. The customer interface device 120C then requests 1606 customer profile information. During this step 1606, the customer can edit already-existing information. The customer interface device 120C receives 1608 the customer profile information via the input devices of the customer interface device 120C, such as the keyboard 410, pointing device 414 and/or display 418. Next, the customer interface device 120C requests 1610 payment information, such as a credit card number, debit card number, or gift card authorization number, along with other identifying and authorization information of the customer's payment method. During this step 1610, the gift card information is entered. The customer interface device 120C receives 1612 the payment information via the reader 420, keyboard 410, pointing device 414 and/or display 418 of the customer interface device 120C. Once all the data is received, the information update application 450 verifies 1614 the data and uploads the information, including the gift card information, to the customer's PDK 102. The PDK 102 is re-initialized 1616 with current information and ready to be used.

[0144] FIG. 17 is a flowchart illustrating a process 1700 for uploading PDK data according to one embodiment of the invention. When a PDK 102 comes within range of a Reader 108, communication is automatically established 1702 between the RDC 304 of the Reader 108 and the PDK 102. In one embodiment, the RDC 304 continually transmits beacons that are detected by the PDK 102 when it enters a proximity zone of the Reader 108. In an alternative embodiment, the communication is instead initiated by the PDK 102 and acknowledged by the Reader 108. Generally, initial communication between the Reader 108 and the PDK 102 is not encrypted in order to provide faster and more power efficient communication.

[0145] In step 1704, a device authentication is performed. Here, the Reader 108 establishes if the PDK 102 is a valid device and PDK 102 establishes if the Reader 108 is valid. Furthermore, device authentication determines if the PDK is capable of providing the

type of authentication required by the Reader 108. An example embodiment of a method for performing 604 device authentication is illustrated in FIG. 7. If either the PDK 102 or RDC 304 is not found valid (1706-No) during device authentication 1704, the transaction is not authorized 1708 and the process ends. If the devices are valid (1706-Yes), a determination 1710 is made as to whether customer data is available. If customer data is not available (1710-No), the process ends. However, if customer data is available (1710-Yes), the customer data is retrieved 1712 and the data is sent to the to the customer database 1410 of the transactions server 140. If the customer's information already exists, the already-existing data is updated with the new data received by the customer database 1410. If the customer's information does not yet exists, the data is sent 1714 to the transactions server 140 and stored 1716 in the customer database 1410 of the transactions server 140 for future use.

[0146] Turning now to FIG. 18, a flowchart illustrating interaction between devices 102, 120 and 140 of the system for automated service-based order processing according to one embodiment of the invention is shown. This figure illustrates more directly the specific device or entity performing the steps of this embodiment of the present invention. FIG. 18 is divided into four vertical sections with each section depicting portions of the process that are performed by that device or entity. The first and left most section shows the steps performed by the user, the second section and the next to the right show the steps performed by the PDK 102, the third section shows the steps performed by the customer interface device 120 and the right most section show the steps performed by the transactions server 140. As is readily apparent from FIG. 18, the method of the present invention requires minimal but sufficient involvement from the user, namely the positioning of the user's body for biometric reading. This advantageously requires the user do almost nothing to initiate the processing of an order, yet achieves user authentication by capturing biometric information sufficient to ensure that the user is authorizing and initiating the transaction.

[0147] The process begins with the Reader 420 of the customer interface device 120 sending 1804 out a beacon signal to start the proximity authentication process. The beacon signal is preferably repeatedly sent such as at a periodic interval. The PDK 102 monitors 1802 for a beacon signal from any Reader 420 in range. If there is no such signal then the PDK 102 is outside the proximity range of any Reader 420. Once the PDK 102 detects a beacon, the PDK 102 responds by sending information to set up a secure communication channel. This process has been described above with reference to Figures 6-9D. Any of the embodiments disclosed above may be used here. Once the secure communication channel has been established, the PDK 102 sends 1806 PDK data and biometric data to the Reader

420. Then the Reader 420 receives 1808 the PDK data and biometric data, and temporarily store the data in working memory of the Reader 420. The reader 420 then authenticates 1810 the PDK 102 using the PDK data. For example, the PDK data may include a profile 220. The reader 420 validates the PDK 102 according to reader's requirements and the requirements specified in the profile 200. This may be any number of types or combinations of authentication as has been described above with reference to FIGS. 8 and 9. In one alternate embodiment (not shown), the Reader 420 may communicate with a third party system such as a registry 112, 114, 116 to validate the PDK 102 and/or the Reader 420. After step 1810, the method continues with the user positioning 1812 his body for a biometric read. In one embodiment, this is swiping his finger over a reader 108. For the other type of biometric scanning, the user need only perform the affirmative act of allowing his body to be scanned such as for a retinal, face, palm, DNA analysis etc. Once the user has performed then inputting step 1812, the Reader 420 receives 1814 the biometric input. In this embodiment, the biometric reader is part of Reader 420 so receipt is automatic. However, where the biometric reader is on the PDK 102, the PDK 102 wirelessly transmits the biometric input to the Reader 420 that in turn receives it. Biometric authentication is then performed 1816 according to the various embodiments illustrated in FIGS. 9A-9D.

[0148] It should be noted that the biometric authentication described above is performed without the requirement of an external database containing biometric data to be searched. The security of maintaining all biometric data to be searched within the user-owned and carried PDK 102 is apparent, as is the vastly improved speed in searching only those immediately surrounding PDK's for a match. Additionally, it will be noticed that in order to complete the transaction, the person possessing the PDK 102 containing the secure data must provide the Reader 420 with a scan (or sample) of biologically identifying material. The importance of the foregoing to the tracking and apprehension of anyone fraudulently attempting to use another person's PDK will be understood by those skilled in the art, as well as extensions of this technology to act as an aid in law enforcement in the detection, tracking and retrieval of lost, stolen or fraudulently obtained PDK's.

[0149] Next, once biometric authentication is established, the transaction is initiated 1818 and order processing is performed 1820. Turning now to FIG. 19, a flowchart illustrating a process for performing 1820 the order processing according to one embodiment of the invention is shown. The order processing module 1406 requests 1902 order information. In one embodiment, the order processing module 1406 can retrieve information identifying the order that the customer typically purchases when the customer visits the merchants. For

example, the order processing module 1406 directs the customer interface device 120 to display "Do you want your Favorite drink?" with the options of "Yes" and "No" to select. The information is received 1904 and a determination is made as to whether the order is complete. For example, in one embodiment, the order processing module 1406 directs the customer interface device 120 to display "Would you like to place another order?" with the options of "Yes" and "No" to select, and if the order processing module 1406 receives a "No" selection, the order processing module continues to receive order information. If the order is complete (1906-Yes), a determination 1908 is made as to whether any new information should be saved and associated with the customer's information in the customer database 1410. If the new information needs to be stored (1908-Yes), then the information is sent to the customer's PDK 102. In one embodiment, the new information is sent to the customer database 1410 for update and storage. If the new information does not need to be saved, or no new information exists (1908-No), the process proceeds to step 1912 and the payment information is retrieved 1912 from the customer's PDK. Existing payment options are displayed 1914. For example, if the customer has more than one method of payment stored on their PDK 102, the existing methods of payments are displayed for selection. Next, the payment selection is received 1916 and payment is processed. Optionally, the processed order and payment information is sent to the rewards processing module 1412 and the data is processed 1918 for eligibility for rewards. A detailed description outlining the steps involved in the processing of data for rewards is provided below with reference to FIG. 22. Finally, the order is sent 1822 to the order completion module 1408 for completion.

[0150] Turning back to FIG. 18, once the transaction status is sent 1822 to the order completion module 1408, the customer interface device 120 presents 1824 the transaction status on the display 418 of the customer interface device 120. For example, the display 418 of the customer interface device 120 may display "Order Complete. Thank you," or "Order Complete. Please Proceed to Register," indicating that the order entry process has been completed and the customer can proceed to the next step of completing and receiving their order. Finally, the customer's PDK 102 receives 1826 and stored that transaction status.

[0151] FIG. 20 is a flowchart illustrating interaction between devices 102, 130 and 140 of the system for automated service-based order processing according to another embodiment of the invention. Similar to FIG. 18, this figure also illustrates more directly the specific device or entity performing the steps of this embodiment of the present invention. Like FIG. 18, FIG. 20 is divided into four vertical sections with each section depicting portions of the process that are performed by that device or entity. The first and left most section shows the

steps performed by the user, the second section and the next to the right show the steps performed by the PDK 102, the third section shows the steps performed by the merchant interface device 130 and the right most section show the steps performed by the transactions server 140. As is readily apparent from FIG. 20, the method of the present invention requires minimal but sufficient involvement from the user, namely the positioning of the user's body for biometric reading. This advantageously requires the user do almost nothing to initiate the processing of an order, yet achieves user authentication by capturing biometric information sufficient to ensure that the user is authorizing and completing the transaction.

[0152] The process begins with the reader 520 of the merchant interface device 130 sending 2004 out a beacon signal to start the proximity authentication process. The beacon signal is preferably repeatedly sent such as at a periodic interval. The PDK 102 monitors 2002 for a beacon signal from any reader 520 in range. If there is no such signal then the PDK 102 is outside the proximity range of any reader 520. Once the PDK 102 detects a beacon, the PDK 102 responds by sending information to set up a secure communication channel. This process has been described above with reference to Figures 6-8. Any of the embodiments disclosed above may be used here. Once the secure communication channel has been established, the PDK 102 sends 2006 PDK data and biometric data to the reader 520. Then the reader 520 receives 2008 the PDK data and biometric data, and temporarily stores the data in working memory of the reader 520. The reader 520 then authenticates 2010 the PDK 102 using the PDK data. For example, the PDK data may include a profile 220. The reader 520 validates the PDK 102 according to reader's requirements and the requirements specified in the profile 200. This may be any number of types or combinations of authentication as has been described above with reference to Figures 8 and 9. In one alternate embodiment (not shown), the reader 520 may communicate with a third party system such as a registry 112, 114, 116 to validate the PDK 102 and/or the reader 520.

[0153] After step 2010, the method continues with the user positioning 2012 his body for a biometric read. In one embodiment, this is swiping his finger over a reader 108. For the other type of biometric scanning, the user need only perform the affirmative act of allowing his body to be scanned such as for a retinal, face, palm, DNA analysis etc. Once the user has performed then inputting step 2012, the Reader 520 receives 2014 the biometric input. In this embodiment, the biometric reader is part of Reader 520 so receipt is automatic. However, where the biometric reader is on the PDK 102, the PDK 102 wirelessly transmits the biometric input to the Reader 520 that in turn receives it. Biometric authentication is then performed 2016 according to the various embodiments illustrated in FIGS. 9A-9D.

[0154] It should be noted that the biometric authentication described above is performed without the requirement of an external database containing biometric data to be searched. The security of maintaining all biometric data to be searched within the user-owned and carried PDK 102 is apparent, as is the vastly improved speed in searching only those immediately surrounding PDK's for a match. Additionally, it will be noticed that in order to complete the transaction, the person possessing the PDK 102 containing the secure data must provide the Reader 420 with a scan (or sample) of biologically identifying material. The importance of the foregoing to the tracking and apprehension of anyone fraudulently attempting to use another person's PDK will be understood by those skilled in the art, as well as extensions of this technology to act as an aid in law enforcement in the detection, tracking and retrieval of lost, stolen or fraudulently obtained PDK's. Next, once biometric authentication is established, the order completion may be performed 2020 by the order completion module 1408 of the transactions server 140.

[0155] Once the transaction is completed 2020 the order completion module 1408 of the transactions server 140 sends 2022 the transaction status to the merchant interface device 130 and the merchant interface device 130 presents 2024 the transaction status on the display 518 of the merchant interface device 130. For example, the display 518 of the merchant interface device 130 may display "Order Complete. Thank you," or "Order Approved. Thank you." indicating that the order completion process has been approved and completed and the customer can receive their order. Finally, the customer's PDK 102 receives 2026 and stores that transaction status.

[0156] According to one embodiment, order processing and order completion is performed by the customer interface device 120. In such embodiments, steps 1802 to 1820 remain the same. After step 1820, since connection is already established and authentication is already performed, the order completed by the order completion module 1408 of the transactions server 140 sends 2022 the transaction status to the customer interface device 120 and the transaction status is displayed 2024 on the display 418 of the customer interface device 120. The customer's PDK receives 2026 and stores the transaction status.

[0157] In some embodiments, biometric input is not required. In such embodiments, another form of confirmation may be required, such as selecting "Yes" to continue to process the order or asking a merchant to "confirm" that the identity of the customer.

[0158] Turning to FIG. 21 a flowchart illustrating interaction between devices 102, 120 and 140 of the system for automated service-based order processing according to yet another embodiment of the invention is shown. In this embodiment, a customer need only interact

with the customer interface device 120 in order to initiate and complete an order. Additionally, the customer needs to only provide a biometric sample once in order to initiate and complete the order. The process begins with the Reader 420 of the customer interface device 120 sending 2104 out a beacon signal to start the proximity authentication process. The beacon signal is preferably repeatedly sent such as at a periodic interval. The PDK 102 monitors 2102 for a beacon signal from any Reader 420 in range. If there is no such signal then the PDK 102 is outside the proximity range of any Reader 420. Once the PDK 102 detects a beacon, the PDK 102 responds by sending information to set up a secure communication channel. This process has been described above with reference to Figures 6-9D. Any of the embodiments disclosed above may be used here. Once the secure communication channel has been established, the PDK 102 sends 2106 PDK data and biometric data to the Reader 420. Then the Reader 420 receives 2108 the PDK data and biometric data, and temporarily store the data in working memory of the Reader 420. The reader 420 then authenticates 2110 the PDK 102 using the PDK data. For example, the PDK data may include a profile 220. The reader 420 validates the PDK 102 according to reader's requirements and the requirements specified in the profile 200. This may be any number of types or combinations of authentication as has been described above with reference to FIGS. 8 and 9. In one alternate embodiment (not shown), the Reader 420 may communicate with a third party system such as a registry 112, 114, 116 to validate the PDK 102 and/or the Reader 420. After step 2110, the transaction is initiated 2112 and order processing is performed 1820. FIG. 19, described above, shows a flowchart illustrating a process for performing 1820 the order processing. In order to complete the processed order, a the transaction server 140 requests 2116 a biometric sample and the request is displayed 2118 on the display 418 of the customer interface device 120.

[0159] The method continues with the user positioning 2120 his body for a biometric read. In one embodiment, this is swiping his finger over a reader 108. In an embodiment where biometric input is not required, the transaction server 140 requests confirmation and the request is displayed on the customer interface device 120. Once the user has performed then inputting step 2021, the Reader 420 receives 2122 the biometric input. In this embodiment, the biometric reader is part of Reader 420 so receipt is automatic. However, where the biometric reader is on the PDK 102, the PDK 102 wirelessly transmits the biometric input to the Reader 420 that in turn receives it. Biometric authentication is then performed 1816 according to the various embodiments illustrated in FIGS. 9A-9D.

[0160] Next, once biometric authentication is established, order completion is performed 2020 and the transaction status is sent 2128 to the customer interface device 120. Once the transaction status is sent 2128, the customer interface device 120 presents 2130 the transaction status on the display 418 of the customer interface device 120. For example, the display 418 of the customer interface device 120 may display "Order Complete. Thank you," or "Order Complete. Please Proceed to Register," indicating that the order entry process has been completed and the customer can proceed to the next step of completing and receiving their order. Finally, the customer's PDK 102 receives 2132 and stored that transaction status.

[0161] FIG. 22 is a flowchart illustrating a process 2200 for rewards processing according to one embodiment of the invention. The rewards processing module 1412 receives 2102 order information. In one embodiment, the rewards processing module 1412 receives the order information from the order processing module 1406. In another embodiment, the rewards processing module 1412 receives the order information from the order completion module 1408 after the order has been completed. Next, the rewards processing module 1412 determines 2104 if the order is eligible for a reward. For example, the requirement for reward eligibility may be that the purchase must exceed a certain amount. As another example, the requirement for reward eligibility may be that the purchase must be paid for with a credit card. If the transaction is eligible for a reward (2104-Yes), the appropriate reward is applied 2206 and associated with the customer's information. If the transaction is not eligible for a reward (2104-No), the process ends 2210. Once the reward is applied 2206, an updated rewards count is sent 2208 to the customer database 1410 for update and storage. In one embodiment, the rewards count is also sent to the customer's PDK and stored in the purchase log 290. In another embodiment, the rewards count is sent to the customer interface device 120 for display by the rewards presentation application 436. In yet another embodiment, the rewards count is sent to the merchant interface device 130 for display by the rewards presentation application 532.

[0162] In one embodiment, the rewards processing module 1412 determines the appropriate reward to apply by referring to a look-up table (not shown). For example, the look-up table may have a list of items eligible for specific rewards and if the customer has purchased a certain item on the table, that specific reward is applied.

[0163] The order in which the steps of the methods of the present invention are performed is purely illustrative in nature. The steps can be performed in any order or in parallel, unless otherwise indicated by the present disclosure. The methods of the present invention may be performed in hardware, firmware, software, or any combination thereof

operating on a single computer or multiple computers of any type. Software embodying the present invention may comprise computer instructions in any form (e.g., source code, object code, interpreted code, etc.) stored in any computer-readable storage medium (e.g., a ROM, a RAM, a magnetic media, a compact disc, a DVD, etc.). Such software may also be in the form of an electrical data signal embodied in a carrier wave propagating on a conductive medium or in the form of light pulses that propagate through an optical fiber.

[0164] While particular embodiments of the present invention have been shown and described, it will be apparent to those skilled in the art that changes and modifications may be made without departing from this invention in its broader aspect.

[0165] In the above description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the invention. It will be apparent, however, to one skilled in the art that the invention can be practiced without these specific details. In other instances, structures and devices are shown in block diagram form in order to avoid obscuring the invention.

[0166] Reference in the specification to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the invention. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment.

[0167] Some embodiments may be described using the expression "coupled" and "connected" along with their derivatives. It should be understood that these terms are not intended as synonyms for each other. For example, some embodiments may be described using the term "connected" to indicate that two or more elements are in direct physical or electrical contact with each other. In another example, some embodiments may be described using the term "coupled" to indicate that two or more elements are in direct physical or electrical contact. The term "coupled," however, may also mean that two or more elements are not in direct contact with each other, but yet still co-operate or interact with each other. The embodiments are not limited in this context.

[0168] As used herein, the terms "comprises," "comprising," "includes," "including," "has," "having" or any other variation thereof, are intended to cover a non-exclusive inclusion. For example, a process, method, article, or apparatus that comprises a list of elements is not necessarily limited to only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. Further, unless expressly stated to the contrary, "or" refers to an inclusive or and not to an exclusive or. For

example, a condition A or B is satisfied by any one of the following: A is true (or present) and B is false (or not present), A is false (or not present) and B is true (or present), and both A and B are true (or present).

[0169] In addition, use of the "a" or "an" are employed to describe elements and components of the embodiments herein. This is done merely for convenience and to give a general sense of the invention. This description should be read to include one or at least one and the singular also includes the plural unless it is obvious that it is meant otherwise

[0170] Some portions of the detailed description are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven 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.

[0171] It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the discussion, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

[0172] The present invention also relates to an apparatus for performing the operations herein. This apparatus can be specially constructed for the required purposes, or it can comprise a general-purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program can be stored in a computer readable storage medium, such as, but is not limited to, any type of disk including floppy disks, optical disks, CD-ROMs, and magnetic-optical disks, read-only memories (ROMs),

random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus.

[0173] The algorithms and modules presented herein are not inherently related to any particular computer or other apparatus. Various general-purpose systems can be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatuses to perform the method steps. The required structure for a variety of these systems will appear from the description below. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages can be used to implement the teachings of the invention as described herein. Furthermore, as will be apparent to one of ordinary skill in the relevant art, the modules, features, attributes, methodologies, and other aspects of the invention can be implemented as software, hardware, firmware or any combination of the three. Of course, wherever a component of the present invention is implemented as software, the component can be implemented as a standalone program, as part of a larger program, as a plurality of separate programs, as a statically or dynamically linked library, as a kernel loadable module, as a device driver, and/or in every and any other way known now or in the future to those of skill in the art of computer programming. Additionally, the present invention is in no way limited to implementation in any specific operating system or environment.

[0174] It will be understood by those skilled in the relevant art that the above-described implementations are merely exemplary, and many changes can be made without departing from the true spirit and scope of the present invention.

[0175] Upon reading this disclosure, those of skill in the art will appreciate still additional alternative structural and functional designs for a system and a process for automating order processing through the disclosed principles herein. Thus, while particular embodiments and applications have been illustrated and described, it is to be understood that the disclosed embodiments are not limited to the precise construction and components disclosed herein. Various modifications, changes and variations, which will be apparent to those skilled in the art, may be made in the arrangement, operation and details of the method and apparatus disclosed herein without departing from the spirit and scope defined in the appended claims.

CLAIMS

WHAT IS CLAIMED IS:

1. A computer-implemented method for electronic order processing, comprising:
automatically initiating an order by wirelessly receiving data from a personal digital key (PDK);
receiving order information; and
in response to receiving the order information, processing the order.

2. The method of claim 1, comprising completing the order.

3. The method of claim 1, comprising processing rewards based on the received order information.

4. The method of claim 1, comprising presenting an order selection based on the received order information.

5. A computer-implemented method for electronic order processing, comprising:
automatically initiating an order by wirelessly receiving data from a personal digital key (PDK);
receiving a biometric input and order information;
confirming the initiation by authenticating the biometric input; and
in response to authenticating the biometric input, processing the order.

6. The method of claim 1, further comprising:
automatically initiating an order completion by wirelessly receiving data from a PDK;
receiving a second biometric input for the order completion;
confirming the order completion by authenticating the second biometric input; and
in response to authenticating the second biometric input, completing the order.

7. The method of claim 5 further comprising:
processing rewards based on the received order information.

8. The method of claim 7, wherein processing the rewards further maintaining a rewards count.

9. The method of claim 5, comprising presenting an order selection based on the received order information.

10. The method of claim 9, wherein the order selection includes a favorite selection.

11. The method of claim 5, wherein processing the order includes receiving payment information.

12. The method of claim 5, comprising storing the data from the PDK, including customer information in a customer database.

13. The method of claim 12, further comprising replicating the customer information from the customer database to additional databases.

14. The method of claim 5, wherein receiving the biometric input comprises performing at least one of a fingerprint scan, a retinal scan, an iris scan, a facial scan, a palm scan, a DNA analysis, a signature analysis, and a voice analysis.

15. The method of claim 5, comprising establishing a secure communication channel between the PDK and a reader, and wherein a profile is sent from the PDK to the reader.

16. The method of claim 6, wherein receiving the biometric input comprises performing at least one of a fingerprint scan, a retinal scan, an iris scan, a facial scan, a palm scan, a DNA analysis, a signature analysis, and a voice analysis.

17. The method of claim 6, wherein comprising establishing a secure communication channel between the PDK and a reader, and wherein a profile is sent from the PDK to the reader.

18. A system for electronic order processing, comprising:

a customer interface device for wirelessly receiving data from a personal digital key (PDK);

a transactions server, adapted for communication with the customer interface device for initiating an order in response to wirelessly receiving the data from the PDK and processing the order;

19. The system of claim 18, further comprising:
a merchant interface device, adapted to communicate with the transactions server, for wirelessly receiving data from a personal digital key (PDK); and
wherein the transactions server is adapted for communication with the merchant interface device and for initiating an order completion.

20. The system of claim 18, further comprising:
a reader, adapted to communicate with the transaction server, for automatically uploading data from the PDK and receiving biometric input from a user.

21. The system of claim 18, wherein the transactions server further comprises an order processing module, adapted to communicate with the customer interface device, for receiving order information and processing the order.

22. The system of claim 19, wherein the transactions server further comprises an order completion module, adapted to communicate with the merchant interface device, for receiving order completion confirmation and completing the order.

23. The system of claim 21, wherein the transactions server further comprises a rewards processing module, adapted to communicate with the order processing module, for processing rewards based on the order.

24. The system of claim 19, further comprising a customer database for storing data including customer information.

25. The system of claim 24, wherein the data from the customer database is replicated to additional databases.

26. The system of claim 25 wherein the additional databases include a validation database, a central registry and a private registry.

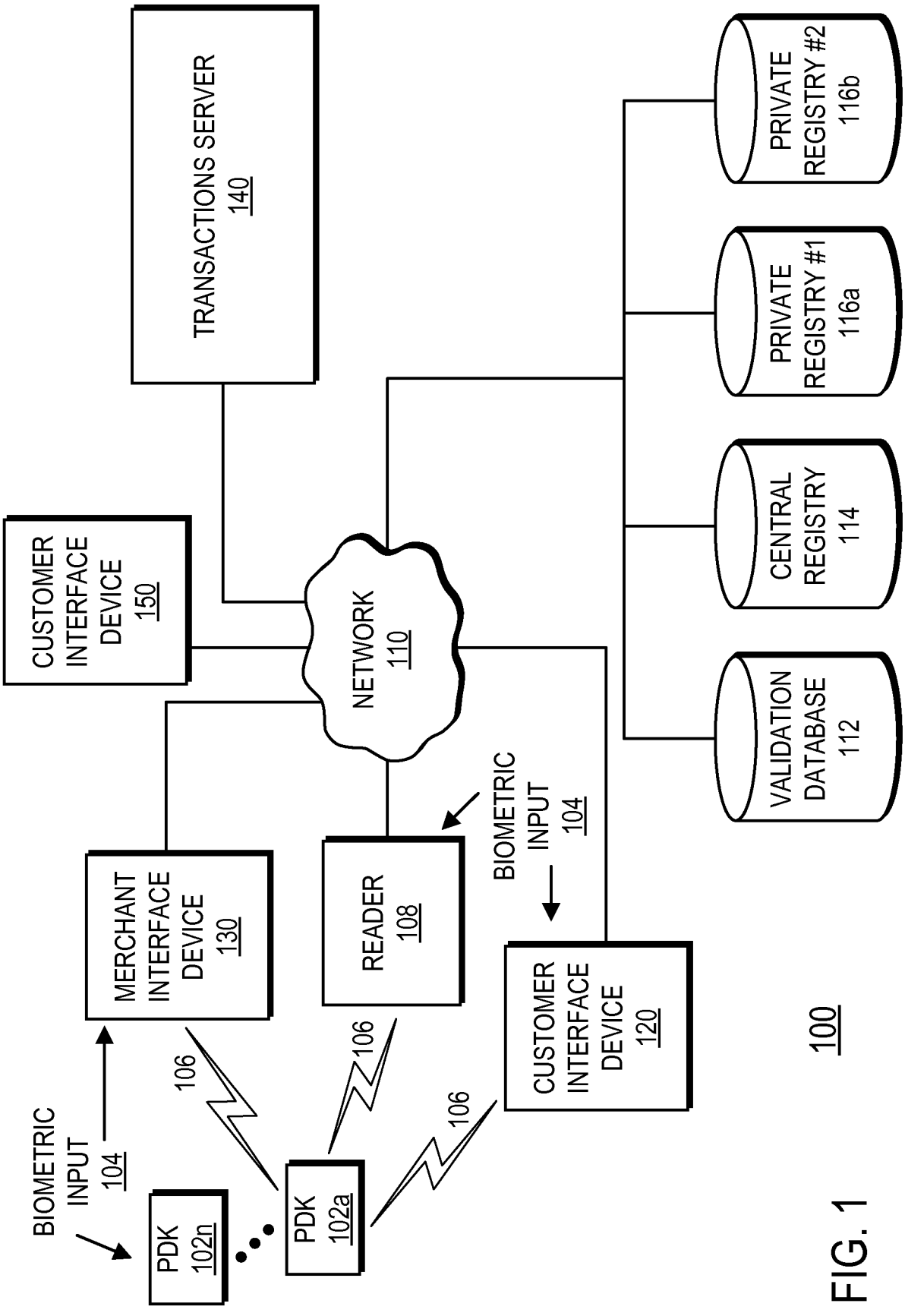
TRANSACTIONS SERVER
140
PRIVATE
REGISTRY #2
116b
PRIVATE
REGISTRY #1
116a
CENTRAL
REGISTRY
114
VALIDATION
DATABASE
112
CUSTOMER
INTERFACE
DEVICE
150
NETWORK
110
MERCHANT
INTERFACE
DEVICE
130
READER
108
BIOMETRIC
INPUT
104
CUSTOMER
INTERFACE
DEVICE
120
BIOMETRIC
INPUT
104
106
106
106
PDK
102n
PDK
102a
100

FIG. 1

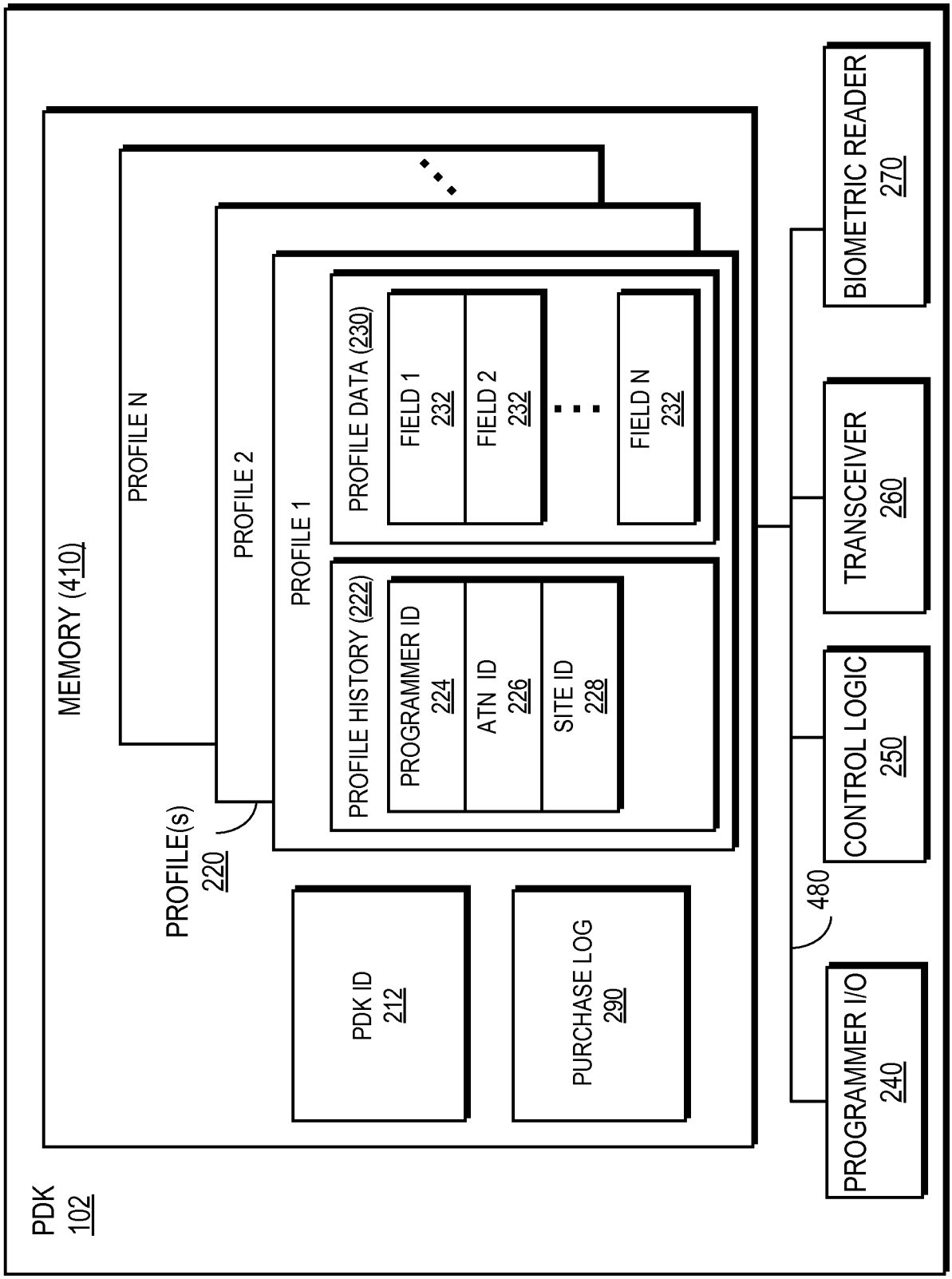
PDK
102
MEMORY (410)
PROFILE N
PROFILE 2
PROFILE 1
PROFILE(s)
220
PROFILE DATA (230)
FIELD 1
232
FIELD 2
232
FIELD N
232
PROFILE HISTORY (222)
PROGRAMMER ID
224
ATN ID
226
SITE ID
228
PDK ID
212
PURCHASE LOG
290
480
PROGRAMMER I/O
240
CONTROL LOGIC
250
TRANSCEIVER
260
BIOMETRIC READER
270

FIG. 2A

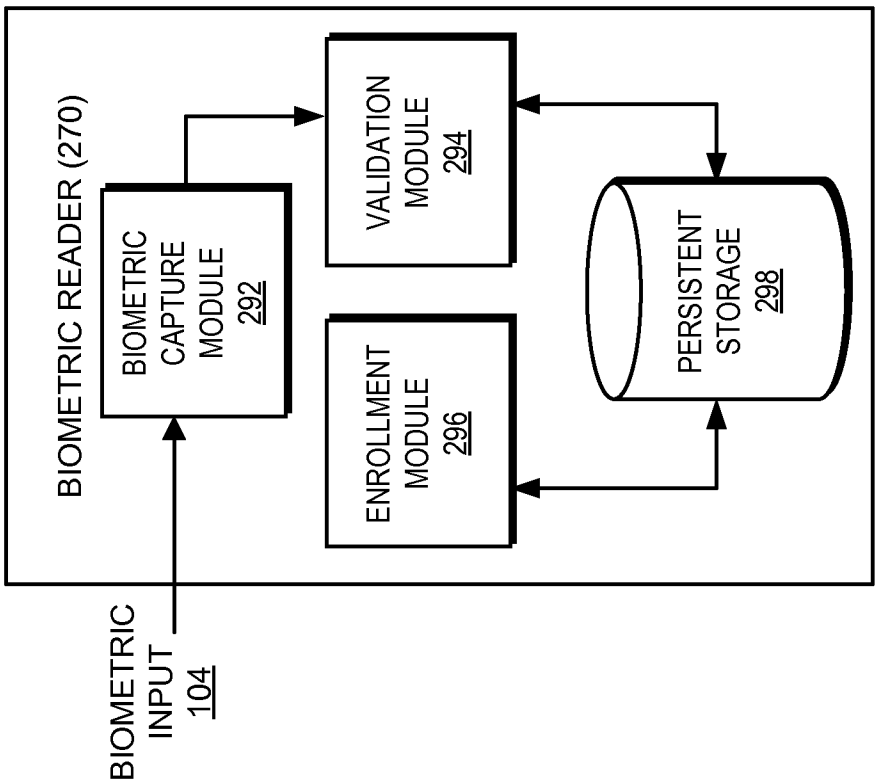
BIOMETRIC READER (270)
BIOMETRIC CAPTURE MODULE 292
VALIDATION MODULE 294
ENROLLMENT MODULE 296
PERSISTENT STORAGE 298
BIOMETRIC INPUT 104

FIG. 2B

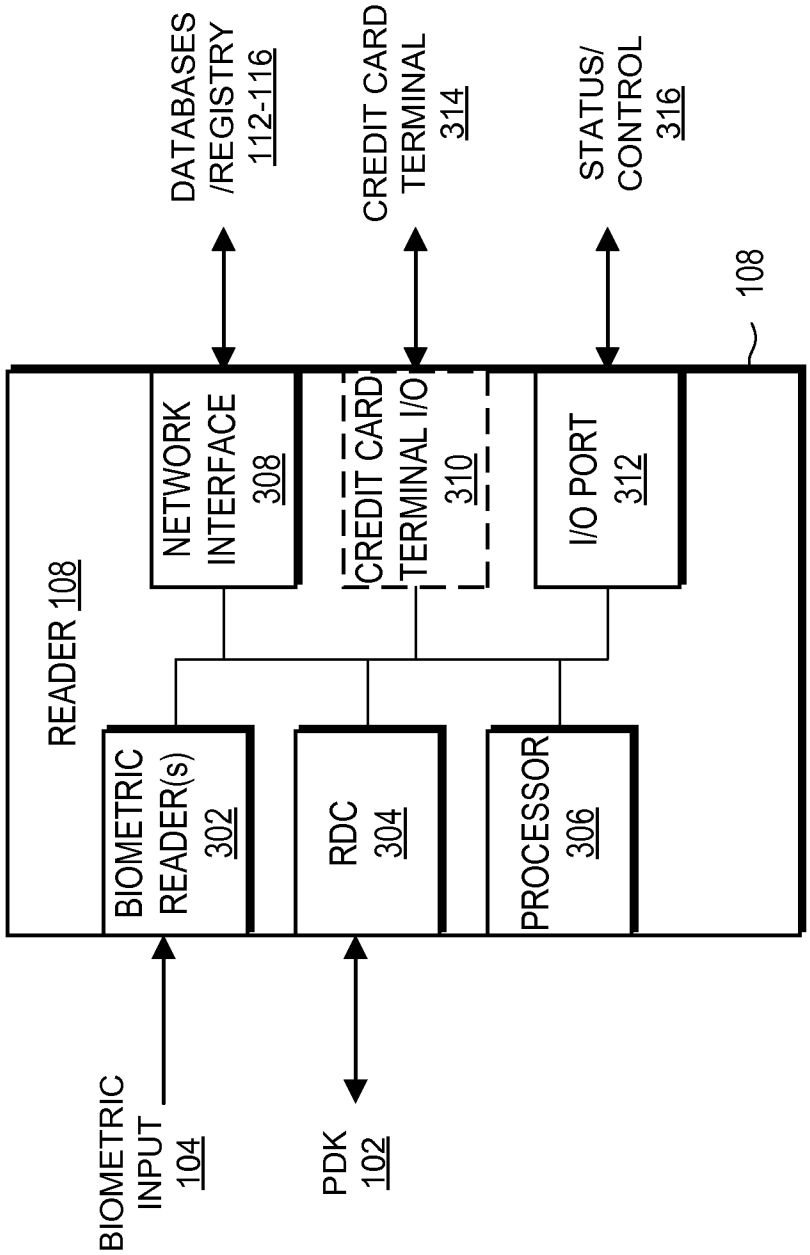
DATABASES /REGISTRY 112-116
CREDIT CARD TERMINAL 314
STATUS/ CONTROL 316
108
READER 108
NETWORK INTERFACE 308
CREDIT CARD TERMINAL I/O 310
I/O PORT 312
BIOMETRIC READER(s) 302
RDC 304
PROCESSOR 306
BIOMETRIC INPUT 104
PDK 102

FIG. 3

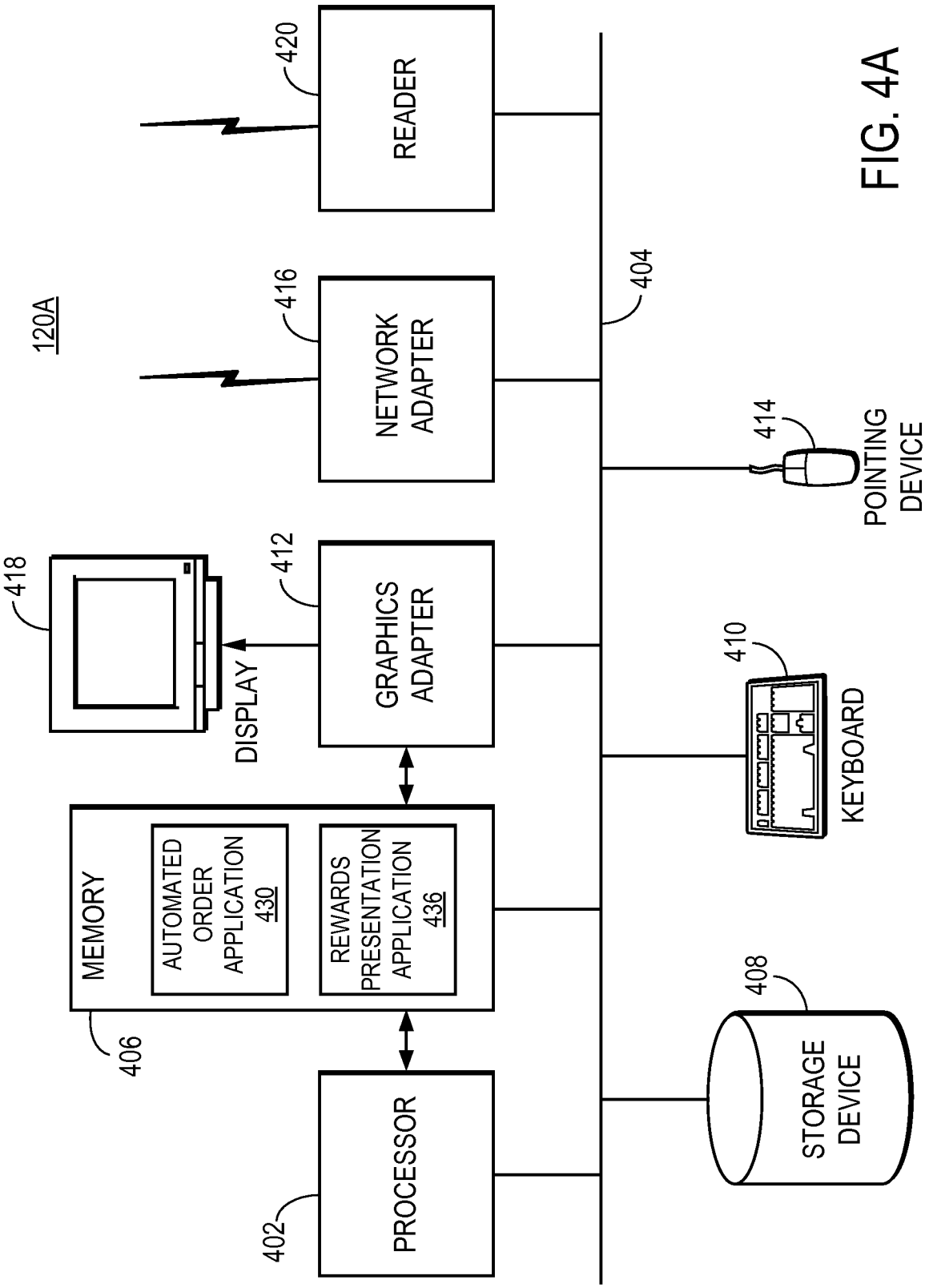
120A
READER
420
NETWORK ADAPTER
416
404
POINTING DEVICE
414
418
DISPLAY
412
GRAPHICS ADAPTER
410
KEYBOARD
MEMORY
AUTOMATED ORDER APPLICATION 430
REWARDS PRESENTATION APPLICATION 436
406
408
STORAGE DEVICE
PROCESSOR
402

FIG. 4A

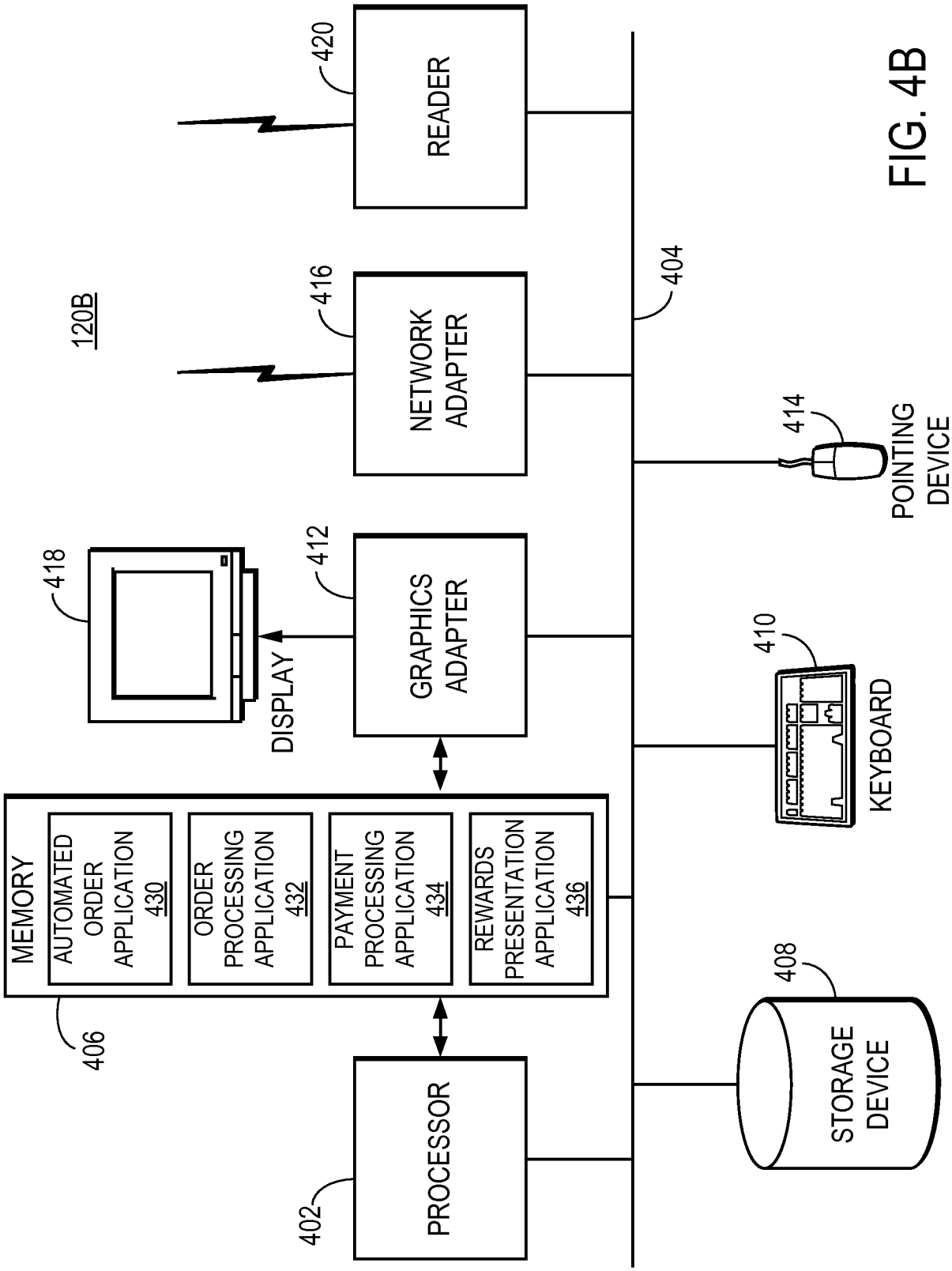
120B
READER
420
NETWORK ADAPTER
416
404
POINTING DEVICE
414
DISPLAY
418
GRAPHICS ADAPTER
412
KEYBOARD
410
MEMORY
AUTOMATED ORDER APPLICATION 430
ORDER PROCESSING APPLICATION 432
PAYMENT PROCESSING APPLICATION 434
REWARDS PRESENTATION APPLICATION 436
406
STORAGE DEVICE
408
PROCESSOR
402

FIG. 4B

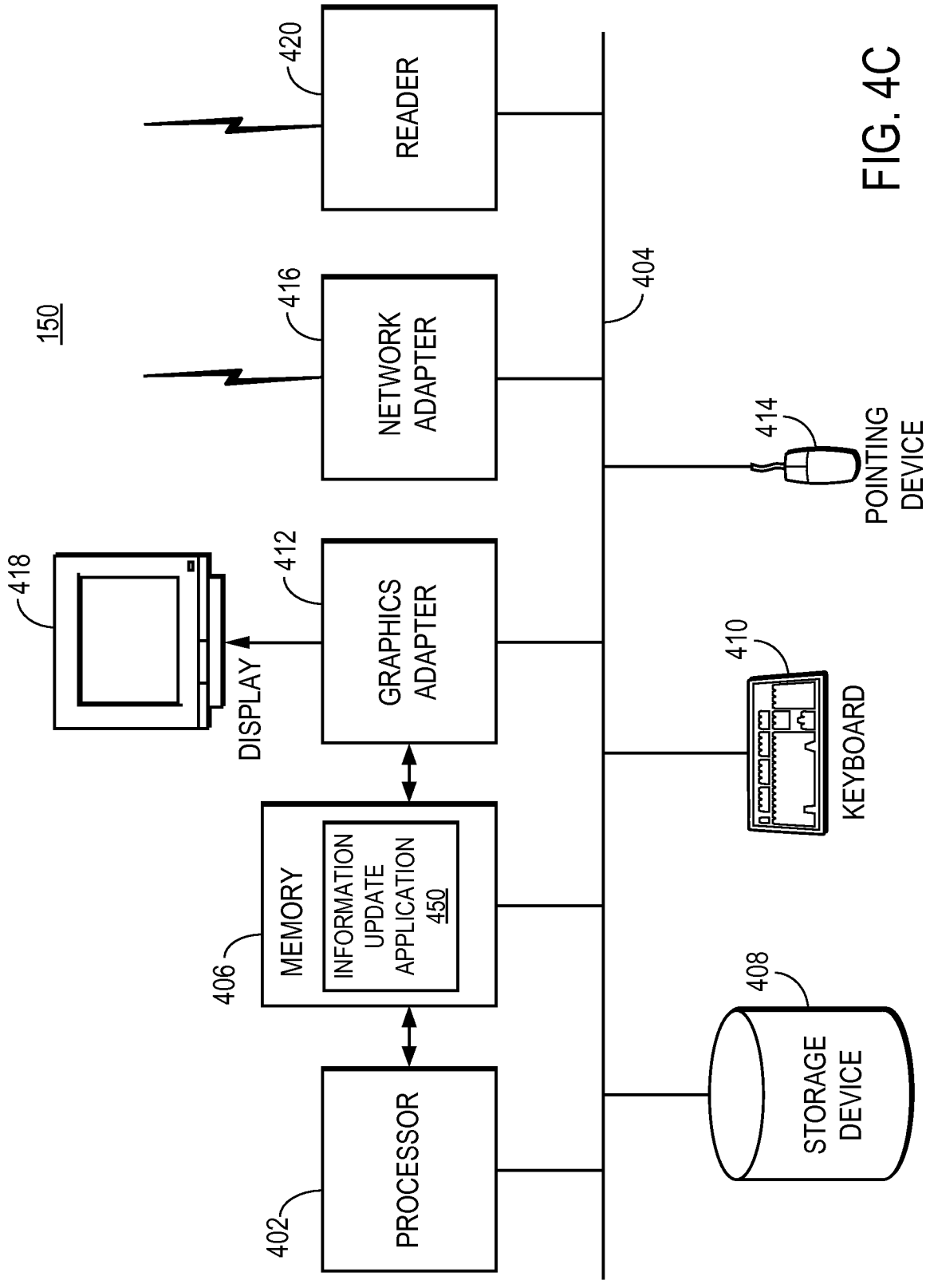
150
PROCESSOR
402
MEMORY
406
INFORMATION UPDATE APPLICATION 450
GRAPHICS ADAPTER
412
DISPLAY
418
NETWORK ADAPTER
416
READER
420
404
POINTING DEVICE
414
KEYBOARD
410
STORAGE DEVICE
408

FIG. 4C

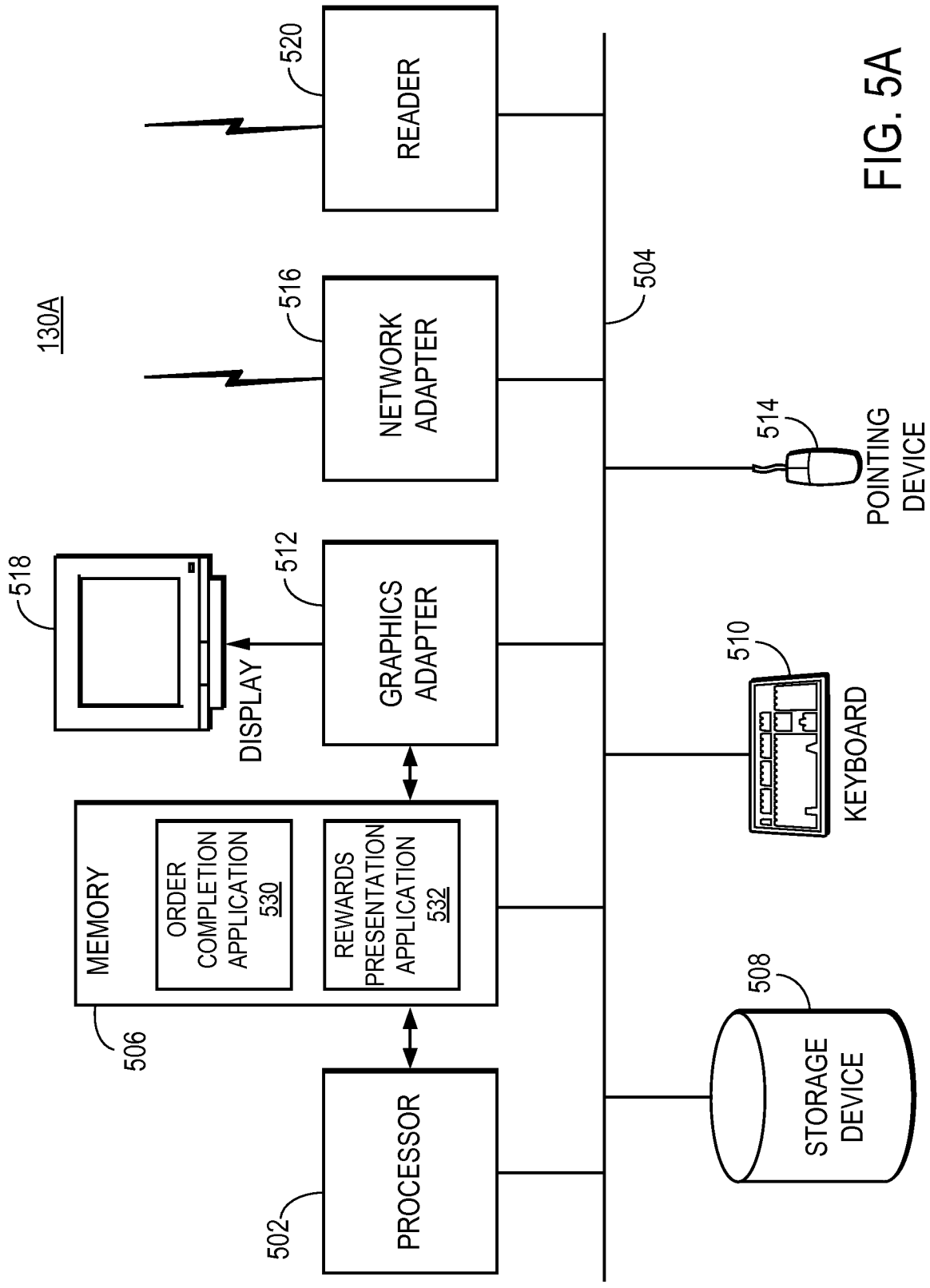
130A
READER
520
NETWORK ADAPTER
516
504
514
POINTING DEVICE
518
DISPLAY
512
GRAPHICS ADAPTER
510
KEYBOARD
MEMORY
ORDER COMPLETION APPLICATION 530
REWARDS PRESENTATION APPLICATION 532
506
508
STORAGE DEVICE
PROCESSOR
502

FIG. 5A

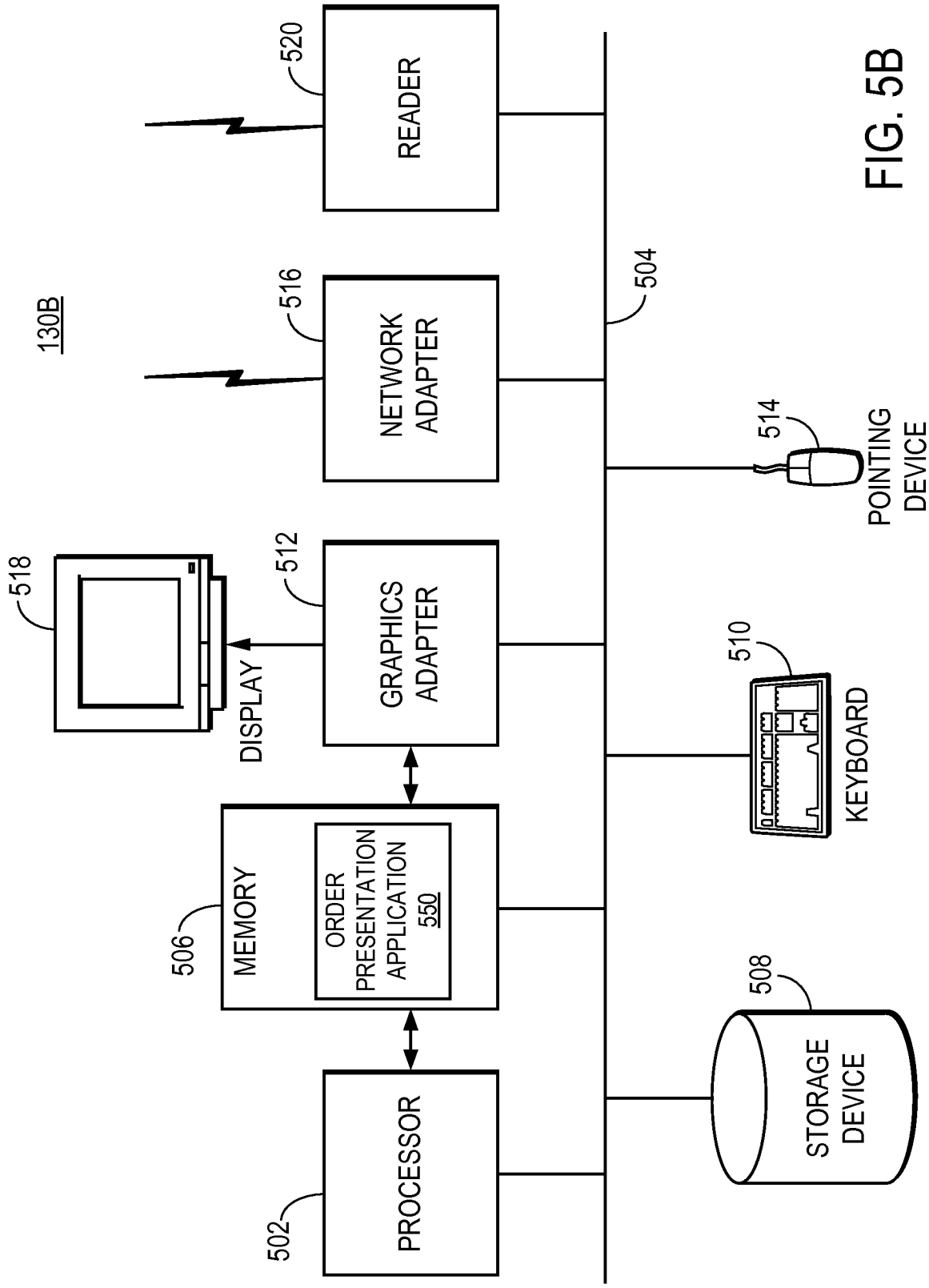
130B
READER
520
NETWORK ADAPTER
516
504
514
POINTING DEVICE
518
DISPLAY
512
GRAPHICS ADAPTER
510
KEYBOARD
MEMORY
506
ORDER PRESENTATION APPLICATION 550
508
STORAGE DEVICE
PROCESSOR
502

FIG. 5B

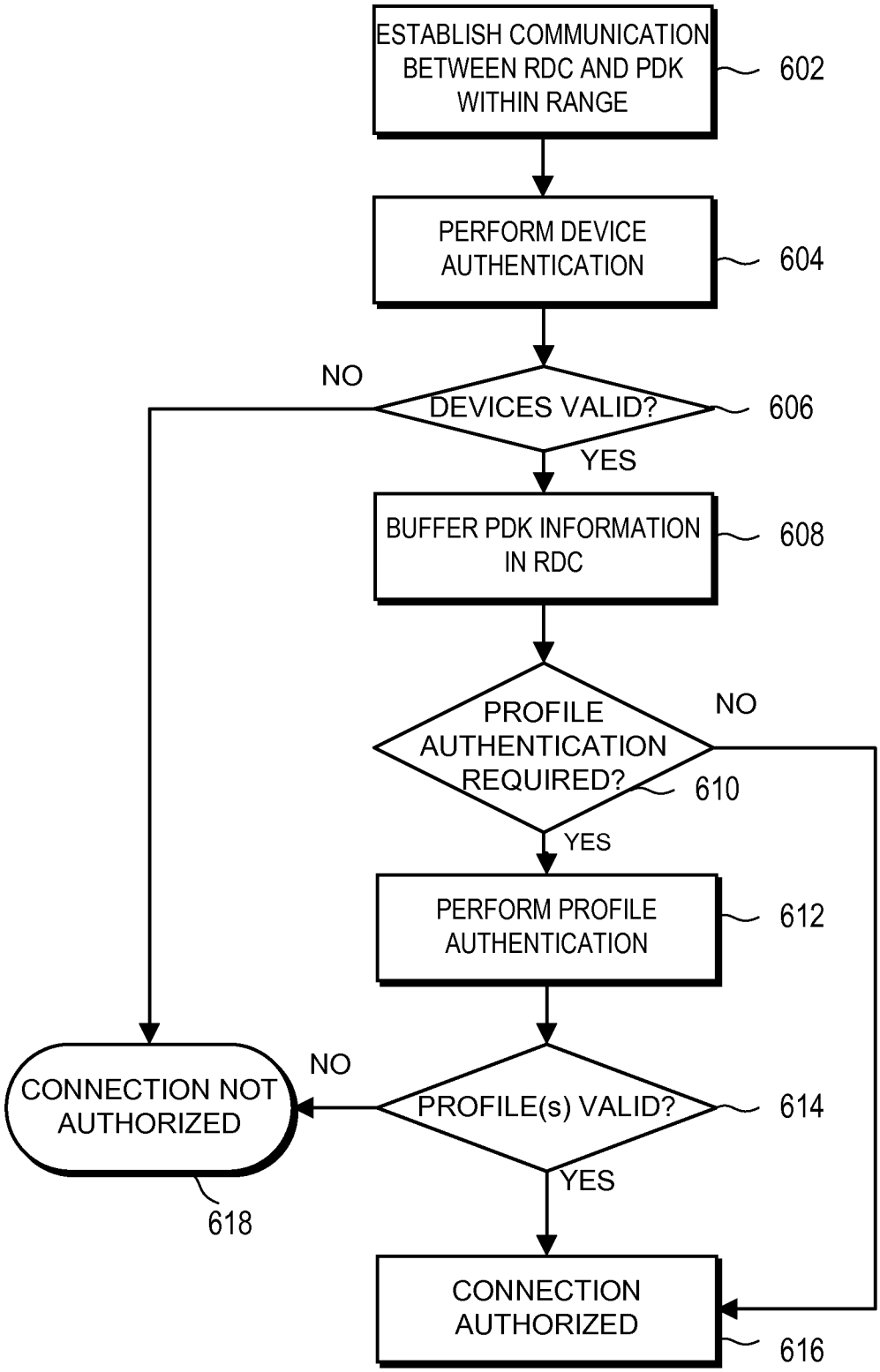
ESTABLISH COMMUNICATION BETWEEN RDC AND PDK WITHIN RANGE
602
PERFORM DEVICE AUTHENTICATION
604
NO
DEVICES VALID?
606
YES
BUFFER PDK INFORMATION IN RDC
608
PROFILE AUTHENTICATION REQUIRED?
610
NO
YES
PERFORM PROFILE AUTHENTICATION
612
CONNECTION NOT AUTHORIZED
NO
PROFILE(s) VALID?
614
YES
618
CONNECTION AUTHORIZED
616

FIG. 6

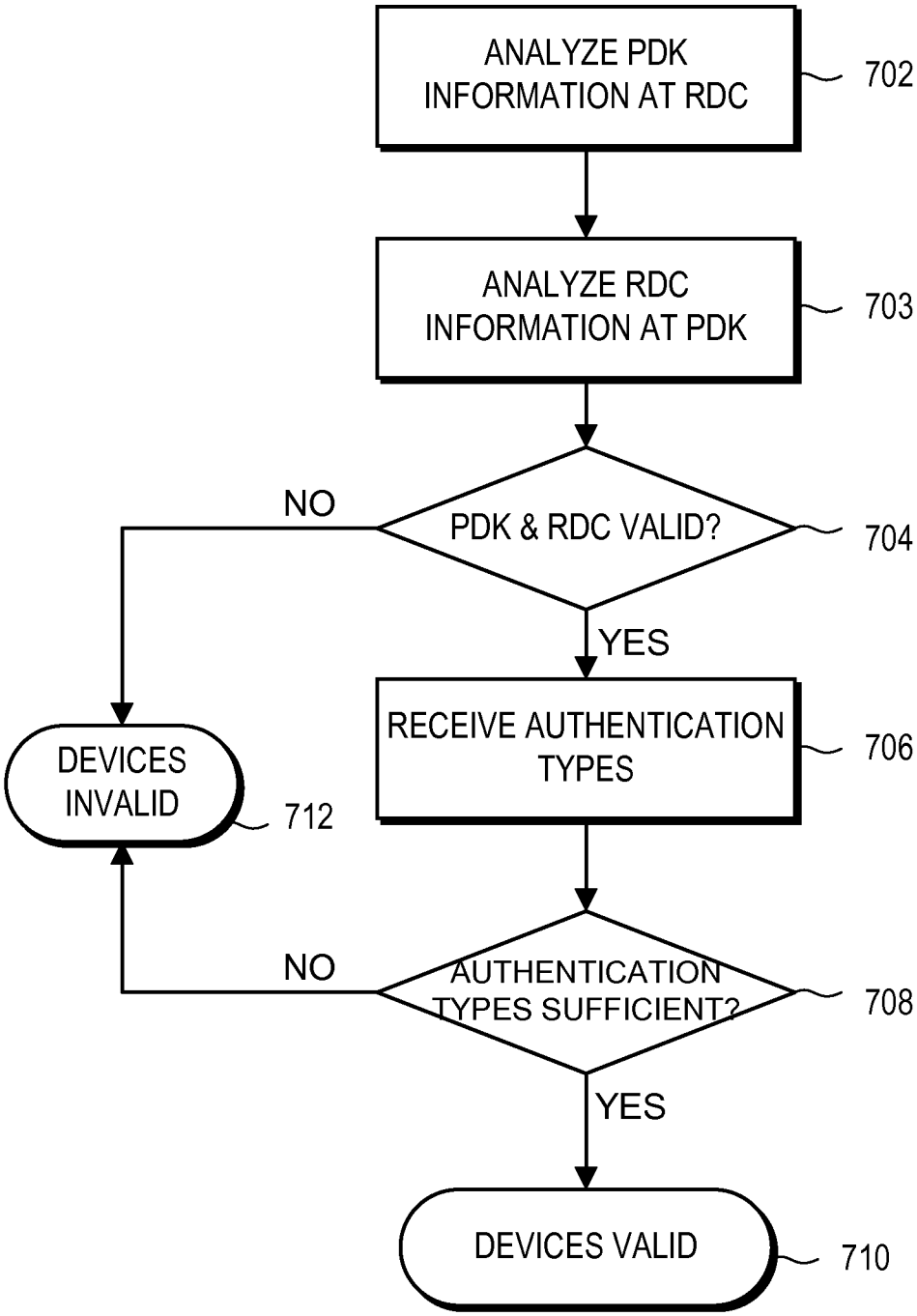
ANALYZE PDK INFORMATION AT RDC
702
ANALYZE RDC INFORMATION AT PDK
703
PDK & RDC VALID?
704
NO
YES
RECEIVE AUTHENTICATION TYPES
706
DEVICES INVALID
712
AUTHENTICATION TYPES SUFFICIENT?
708
NO
YES
DEVICES VALID
710

FIG. 7

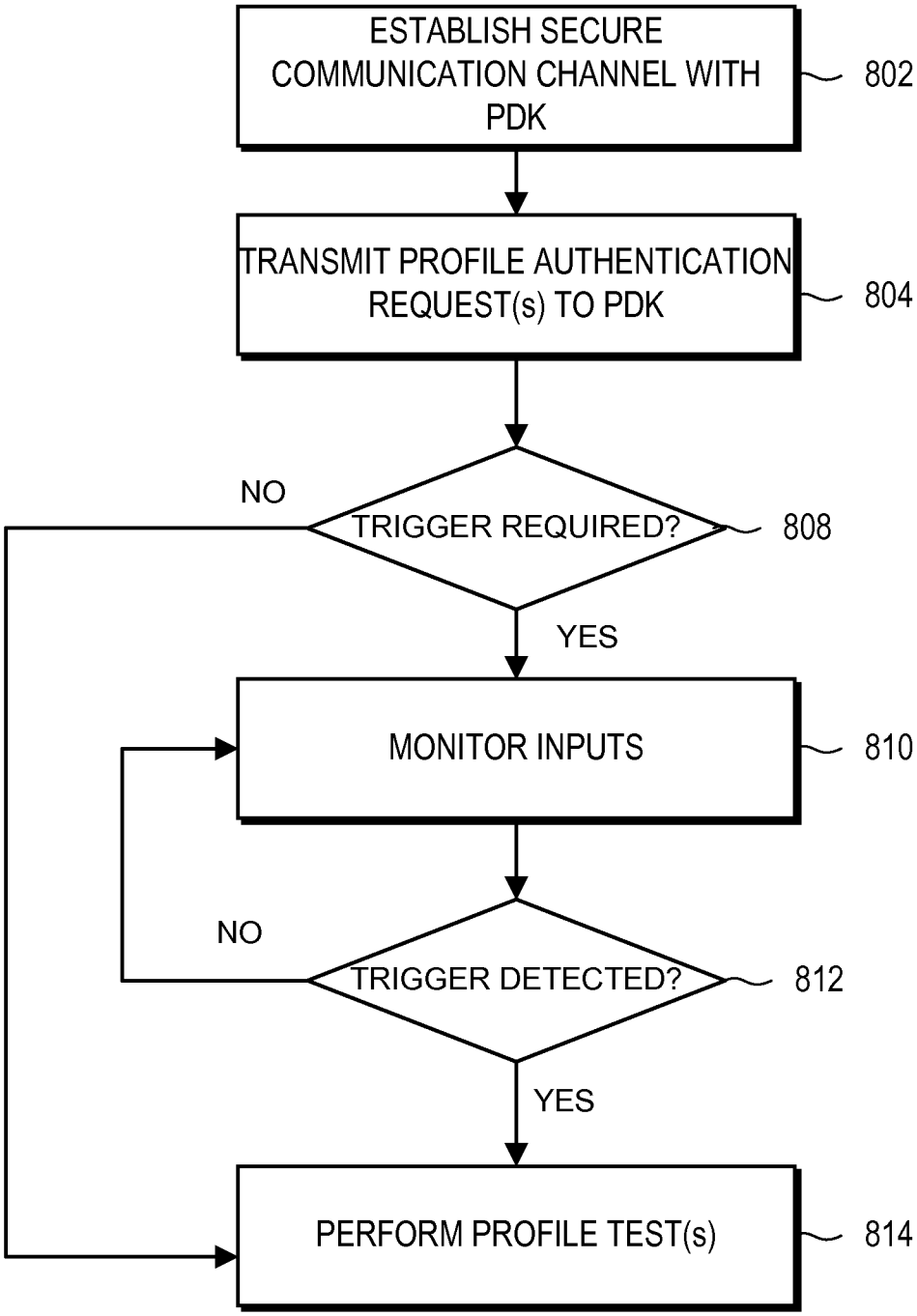
ESTABLISH SECURE COMMUNICATION CHANNEL WITH PDK
802
TRANSMIT PROFILE AUTHENTICATION REQUEST(s) TO PDK
804
NO
TRIGGER REQUIRED?
808
YES
MONITOR INPUTS
810
NO
TRIGGER DETECTED?
812
YES
PERFORM PROFILE TEST(s)
814

FIG. 8

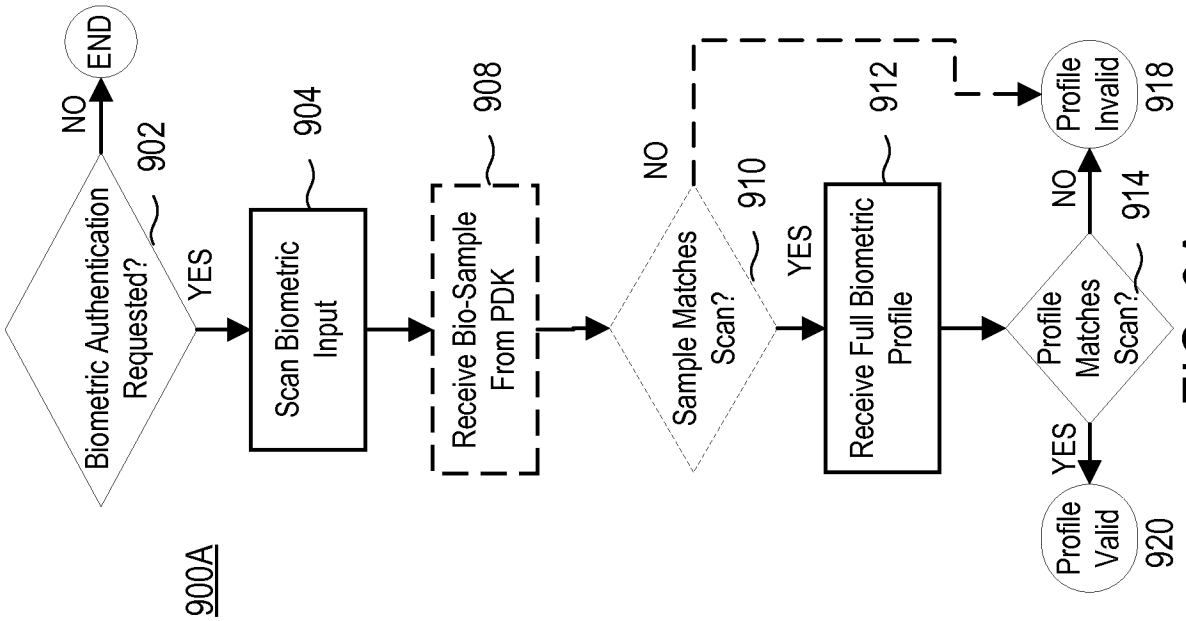
900A
Biometric Authentication Requested?
902
NO
END
YES
Scan Biometric Input
904
Receive Bio-Sample From PDK
908
Sample Matches Scan?
910
NO
YES
Receive Full Biometric Profile
912
Profile Matches Scan?
914
NO
YES
Profile Invalid
918
Profile Valid
920

FIG. 9A

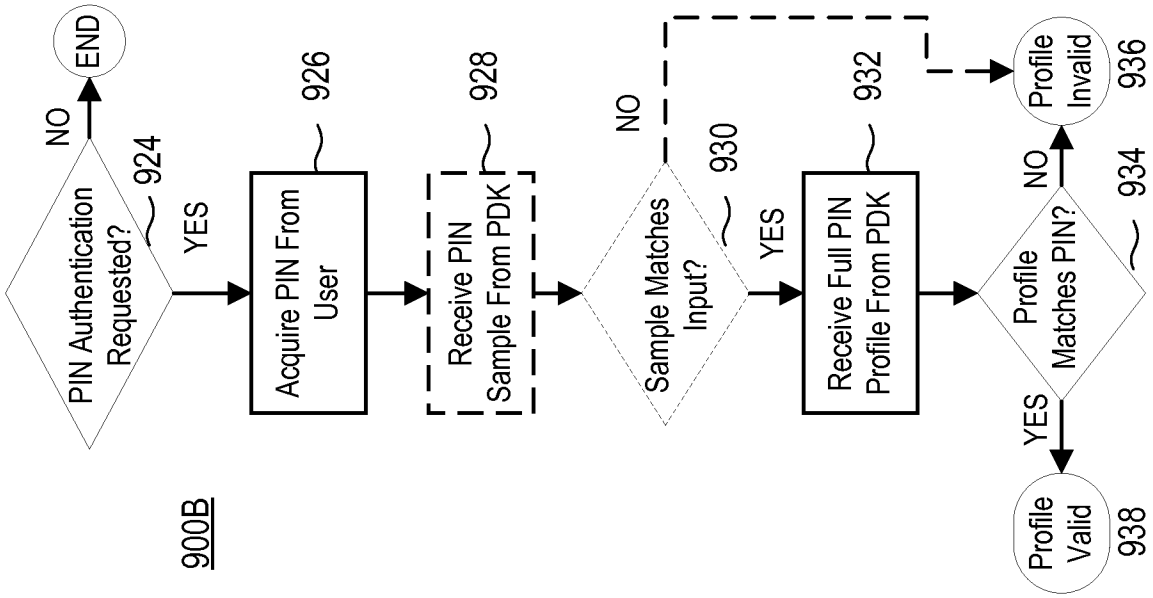
900B
PIN Authentication Requested?
924
NO
END
YES
Acquire PIN From User
926
Receive PIN Sample From PDK
928
Sample Matches Input?
930
NO
YES
Receive Full PIN Profile From PDK
932
Profile Matches PIN?
934
NO
YES
Profile Invalid
936
Profile Valid
938

FIG. 9B

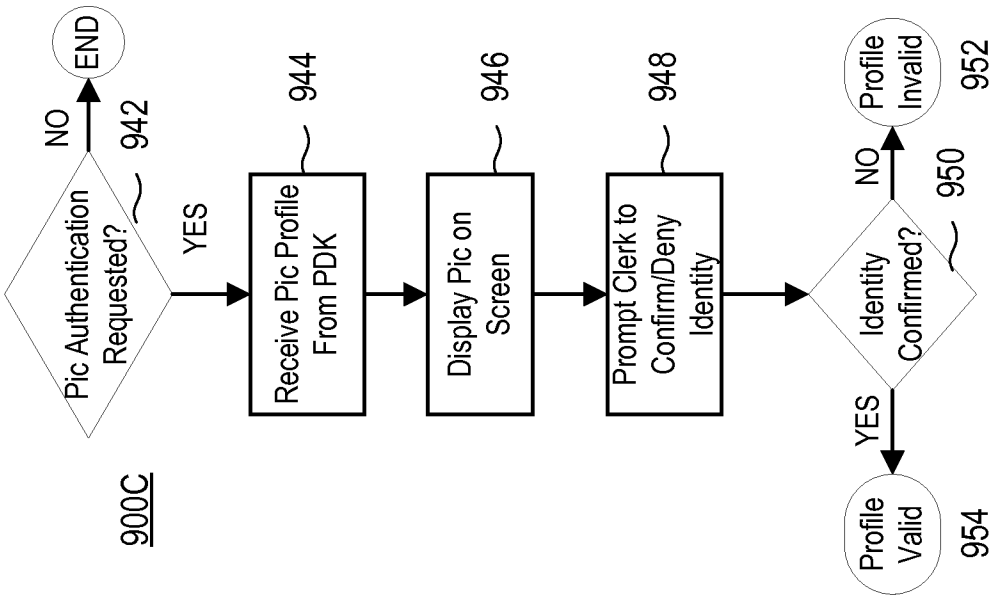
900C
Pic Authentication Requested?
942
NO
END
YES
Receive Pic Profile From PDK
944
Display Pic on Screen
946
Prompt Clerk to Confirm/Deny Identity
948
Identity Confirmed?
950
NO
Profile Invalid
952
YES
Profile Valid
954

FIG. 9C

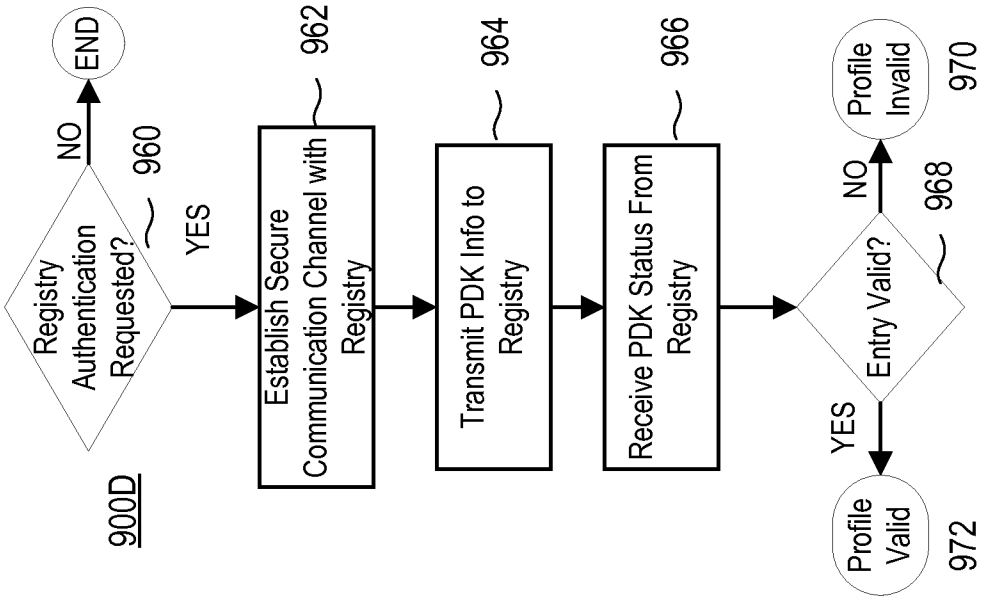
900D
Registry Authentication Requested?
960
NO
END
YES
Establish Secure Communication Channel with Registry
962
Transmit PDK Info to Registry
964
Receive PDK Status From Registry
966
Entry Valid?
968
NO
Profile Invalid
970
YES
Profile Valid
972

FIG. 9D

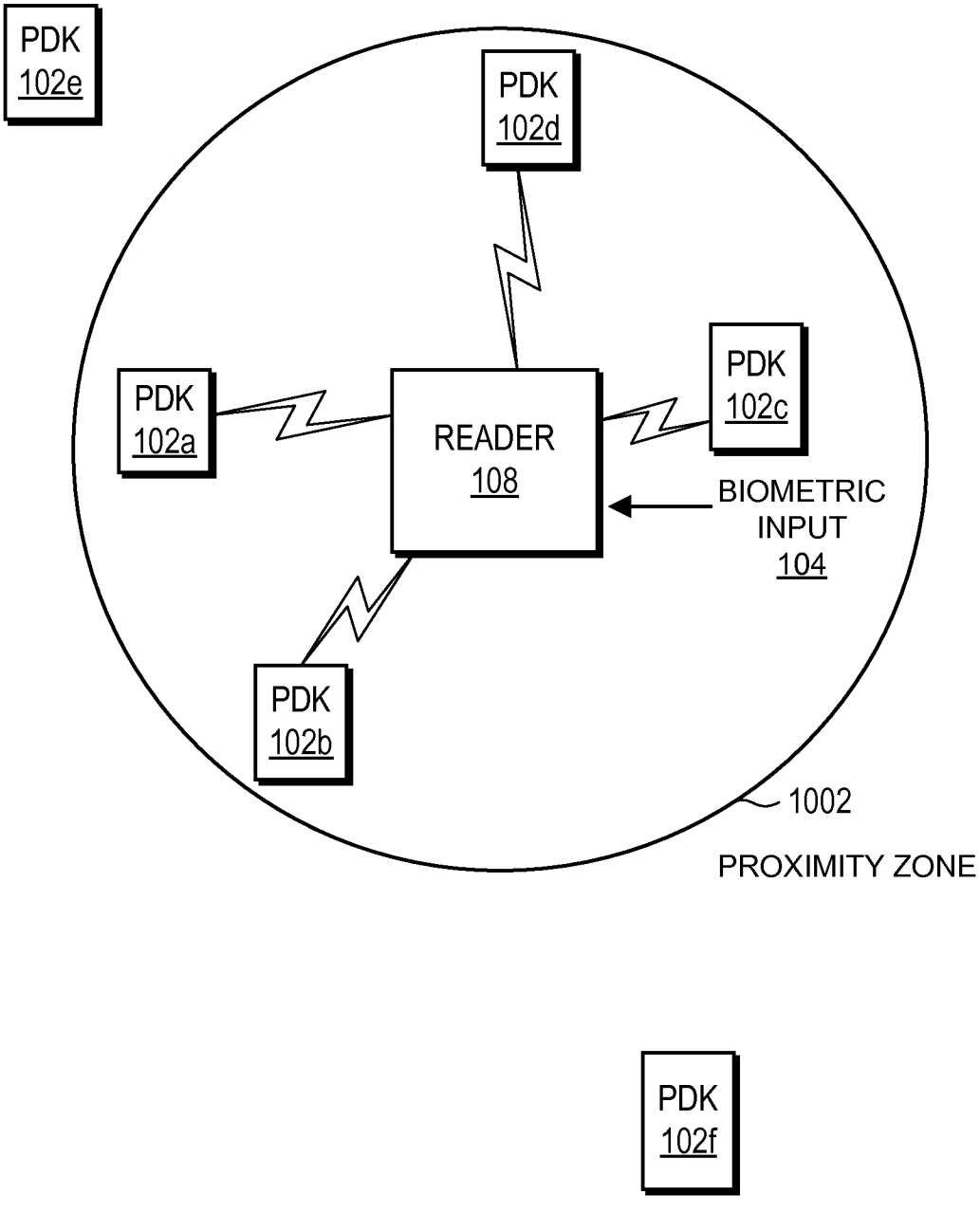
PDK
102e
PDK
102d
PDK
102a
READER
108
PDK
102c
BIOMETRIC
INPUT
104
PDK
102b
1002
PROXIMITY ZONE
PDK
102f

FIG. 10

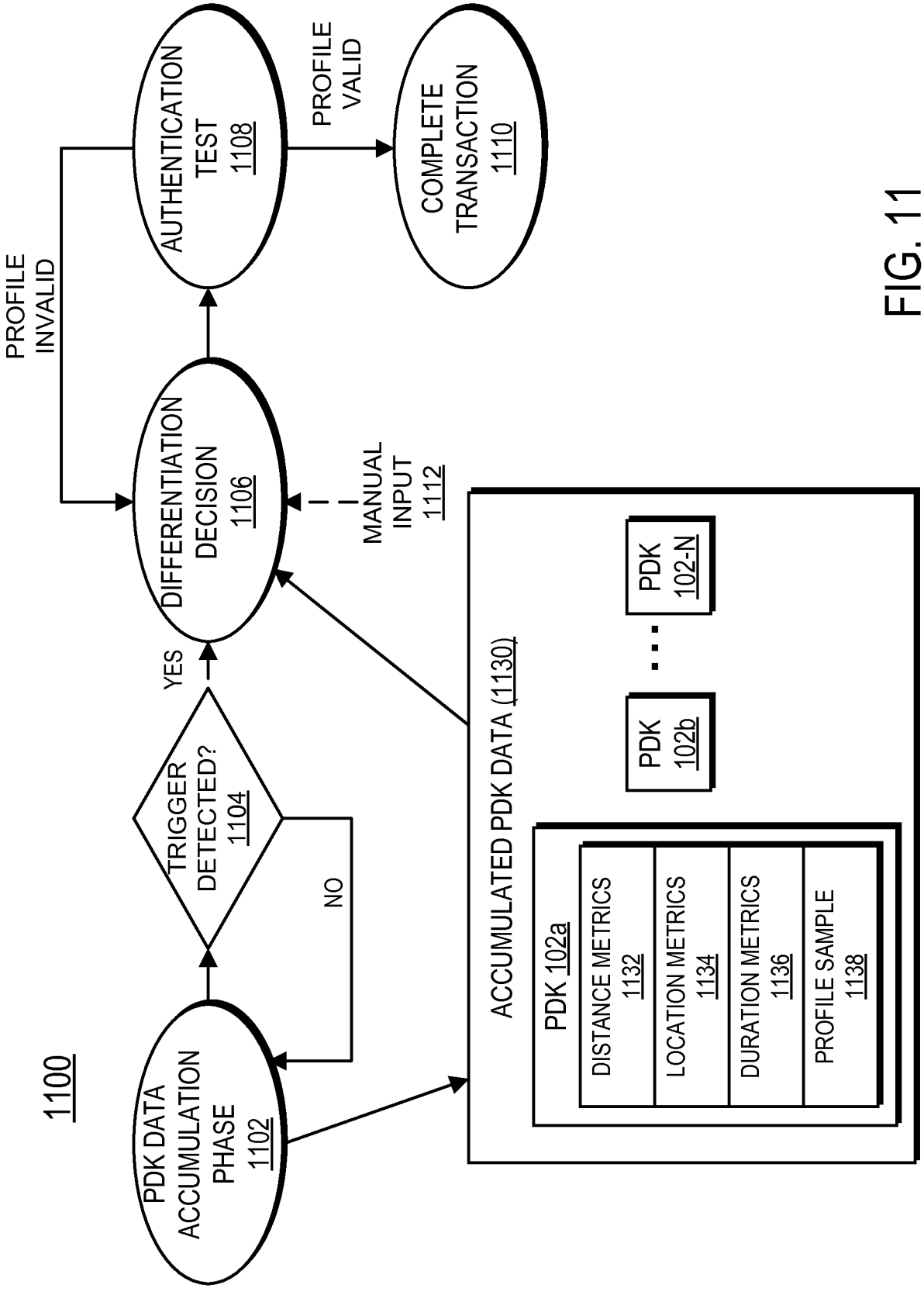
1100
PDK DATA ACCUMULATION PHASE 1102
TRIGGER DETECTED? 1104
YES
NO
DIFFERENTIATION DECISION 1106
MANUAL INPUT 1112
AUTHENTICATION TEST 1108
PROFILE INVALID
PROFILE VALID
COMPLETE TRANSACTION 1110
ACCUMULATED PDK DATA (1130)
PDK 102a
DISTANCE METRICS 1132
LOCATION METRICS 1134
DURATION METRICS 1136
PROFILE SAMPLE 1138
PDK 102b
PDK 102-N

FIG. 11

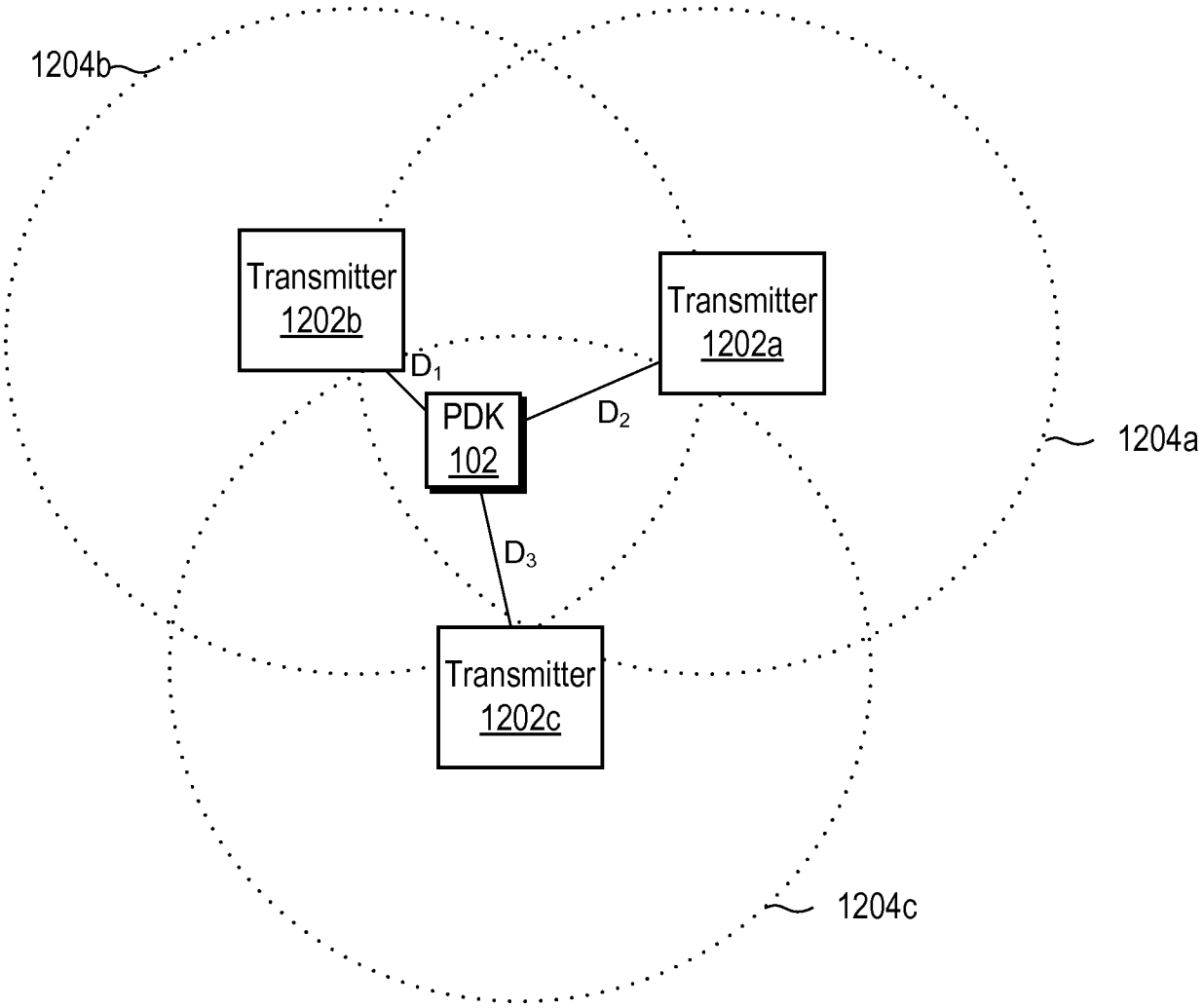
1204b
Transmitter
1202b
Transmitter
1202a
D1
PDK
102
D2
1204a
D3
Transmitter
1202c
1204c

FIG. 12

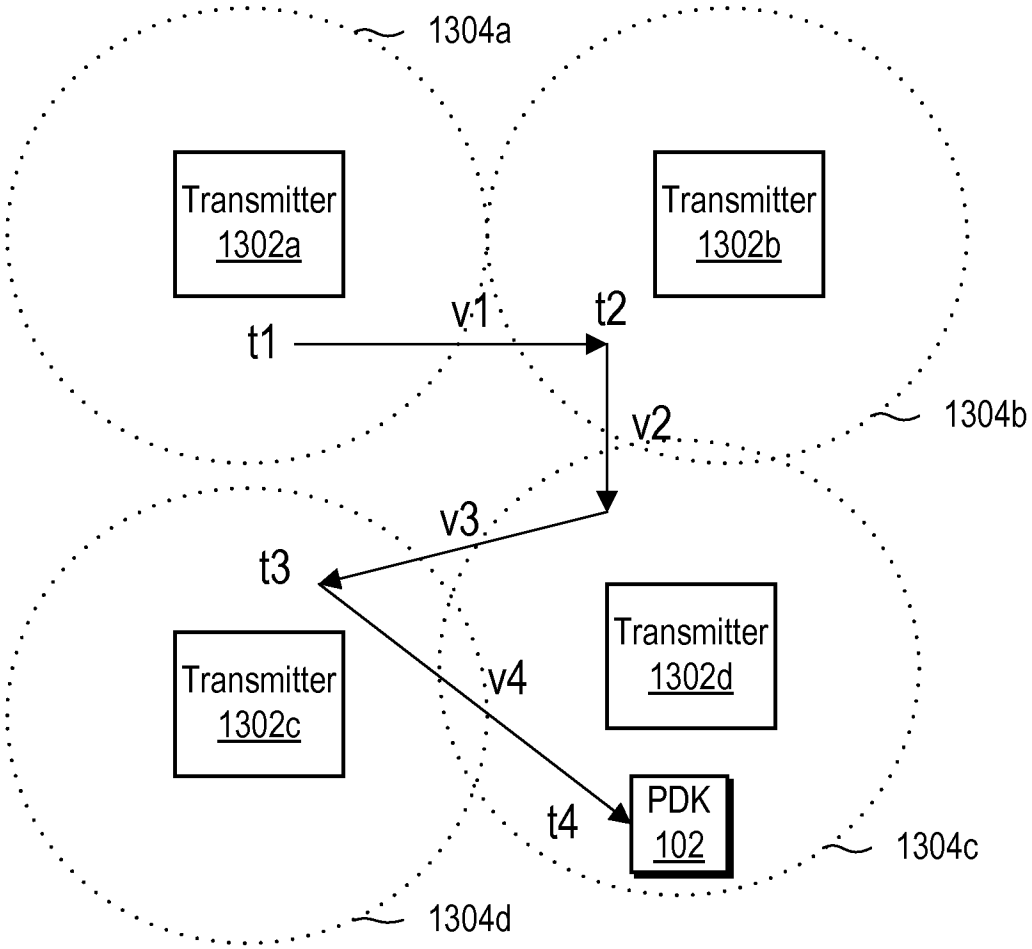
1304a
Transmitter
1302a
Transmitter
1302b
v1
t2
t1
v2
1304b
v3
t3
Transmitter
1302d
Transmitter
1302c
v4
PDK
102
t4
1304c
1304d

FIG. 13

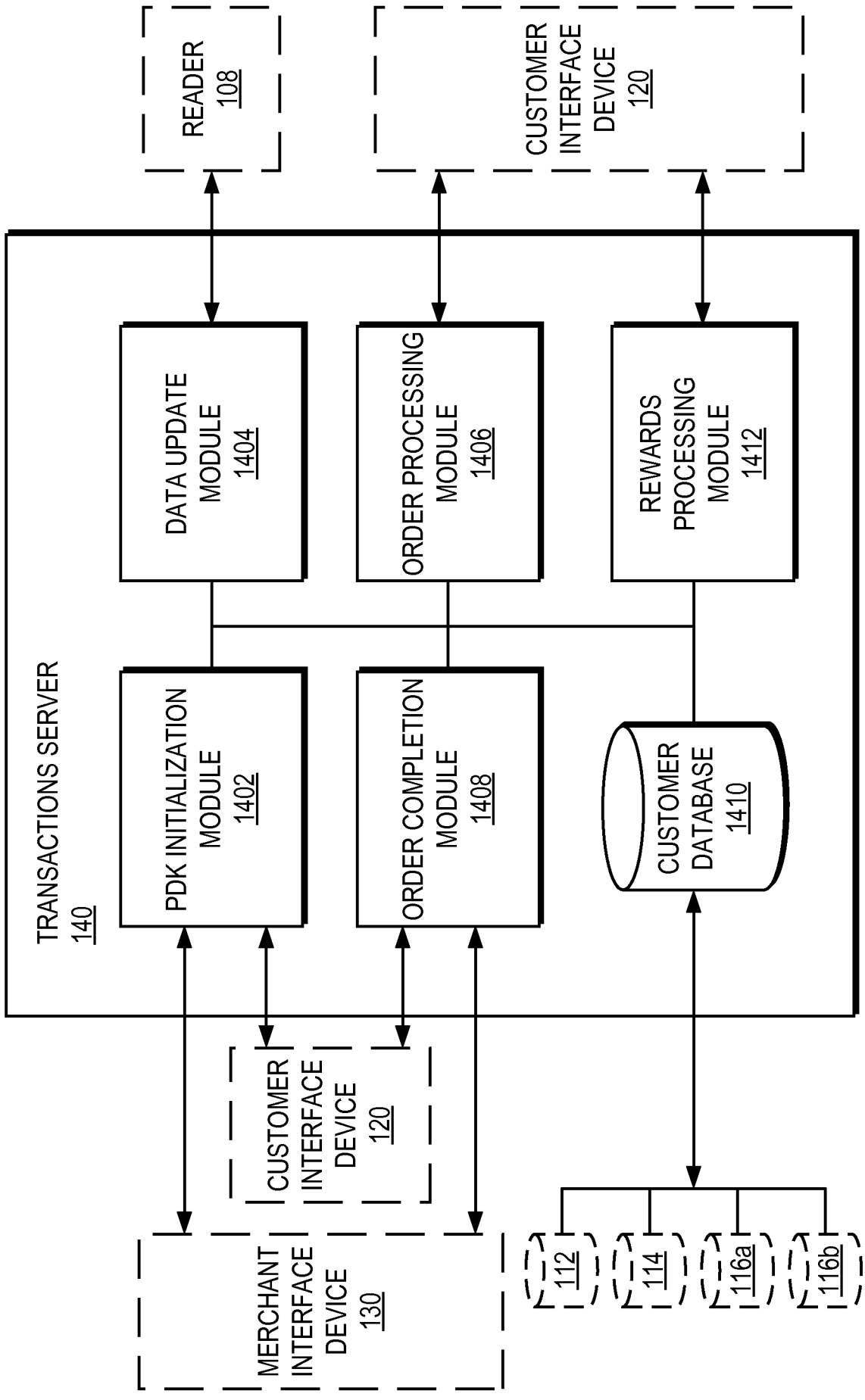
READER
108
CUSTOMER INTERFACE DEVICE
120
TRANSACTIONS SERVER
140
DATA UPDATE MODULE
1404
ORDER PROCESSING MODULE
1406
REWARDS PROCESSING MODULE
1412
PDK INITIALIZATION MODULE
1402
ORDER COMPLETION MODULE
1408
CUSTOMER DATABASE
1410
CUSTOMER INTERFACE DEVICE
120
MERCHANT INTERFACE DEVICE
130
112
114
116a
116b

FIG. 14

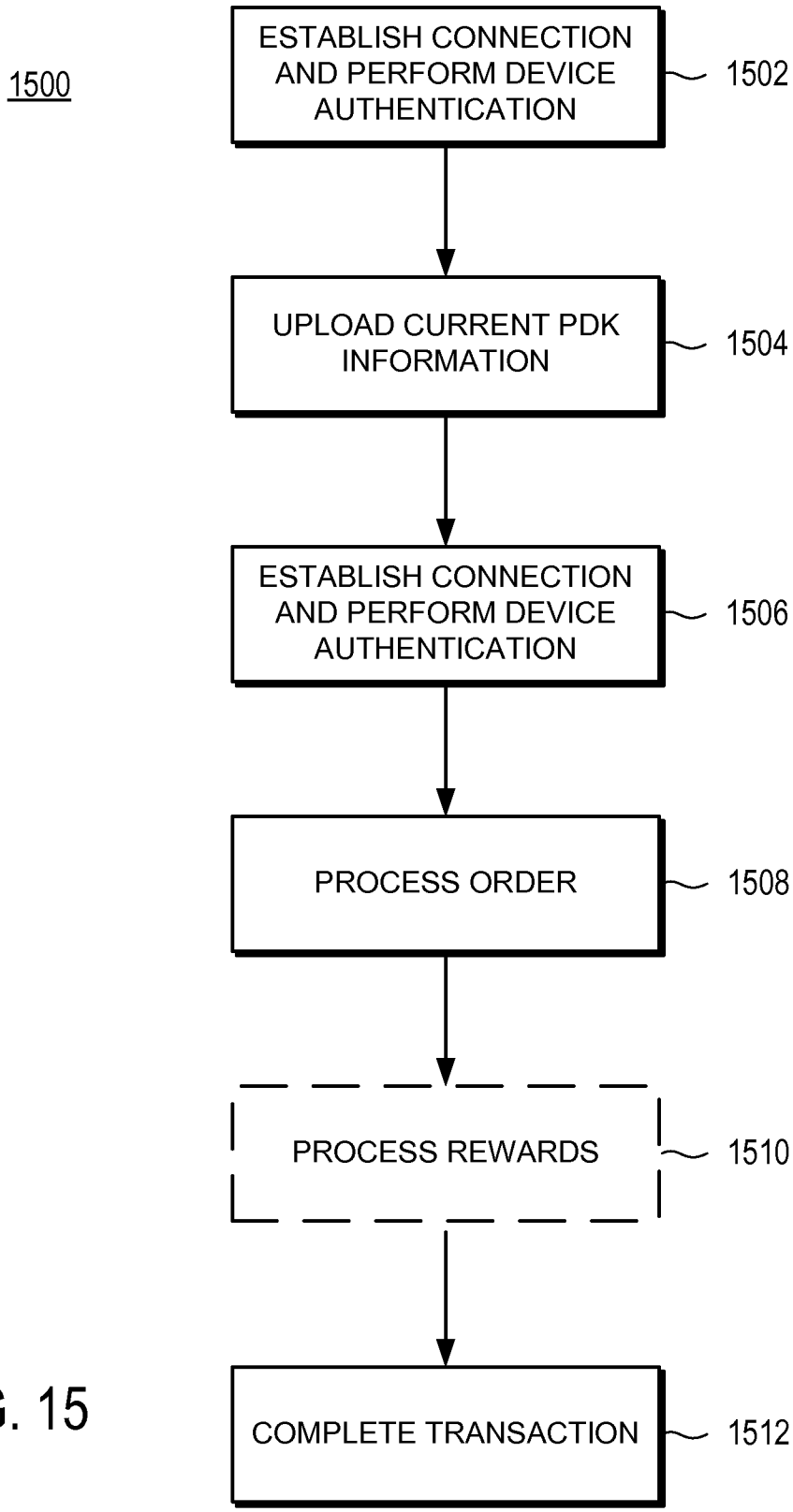
1500
ESTABLISH CONNECTION AND PERFORM DEVICE AUTHENTICATION
1502
UPLOAD CURRENT PDK INFORMATION
1504
ESTABLISH CONNECTION AND PERFORM DEVICE AUTHENTICATION
1506
PROCESS ORDER
1508
PROCESS REWARDS
1510
COMPLETE TRANSACTION
1512

FIG. 15

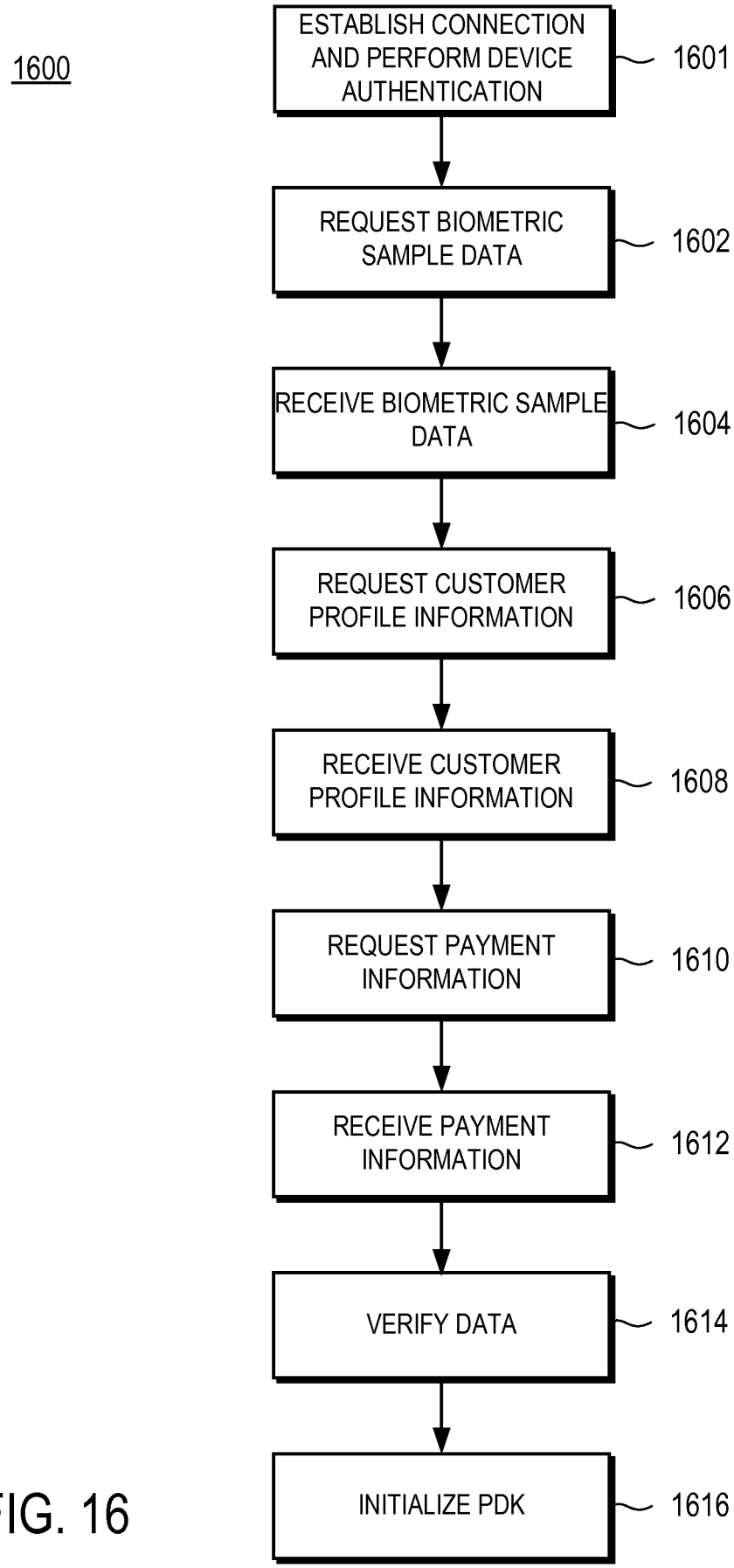
1600
ESTABLISH CONNECTION AND PERFORM DEVICE AUTHENTICATION
1601
REQUEST BIOMETRIC SAMPLE DATA
1602
RECEIVE BIOMETRIC SAMPLE DATA
1604
REQUEST CUSTOMER PROFILE INFORMATION
1606
RECEIVE CUSTOMER PROFILE INFORMATION
1608
REQUEST PAYMENT INFORMATION
1610
RECEIVE PAYMENT INFORMATION
1612
VERIFY DATA
1614
INITIALIZE PDK
1616

FIG. 16

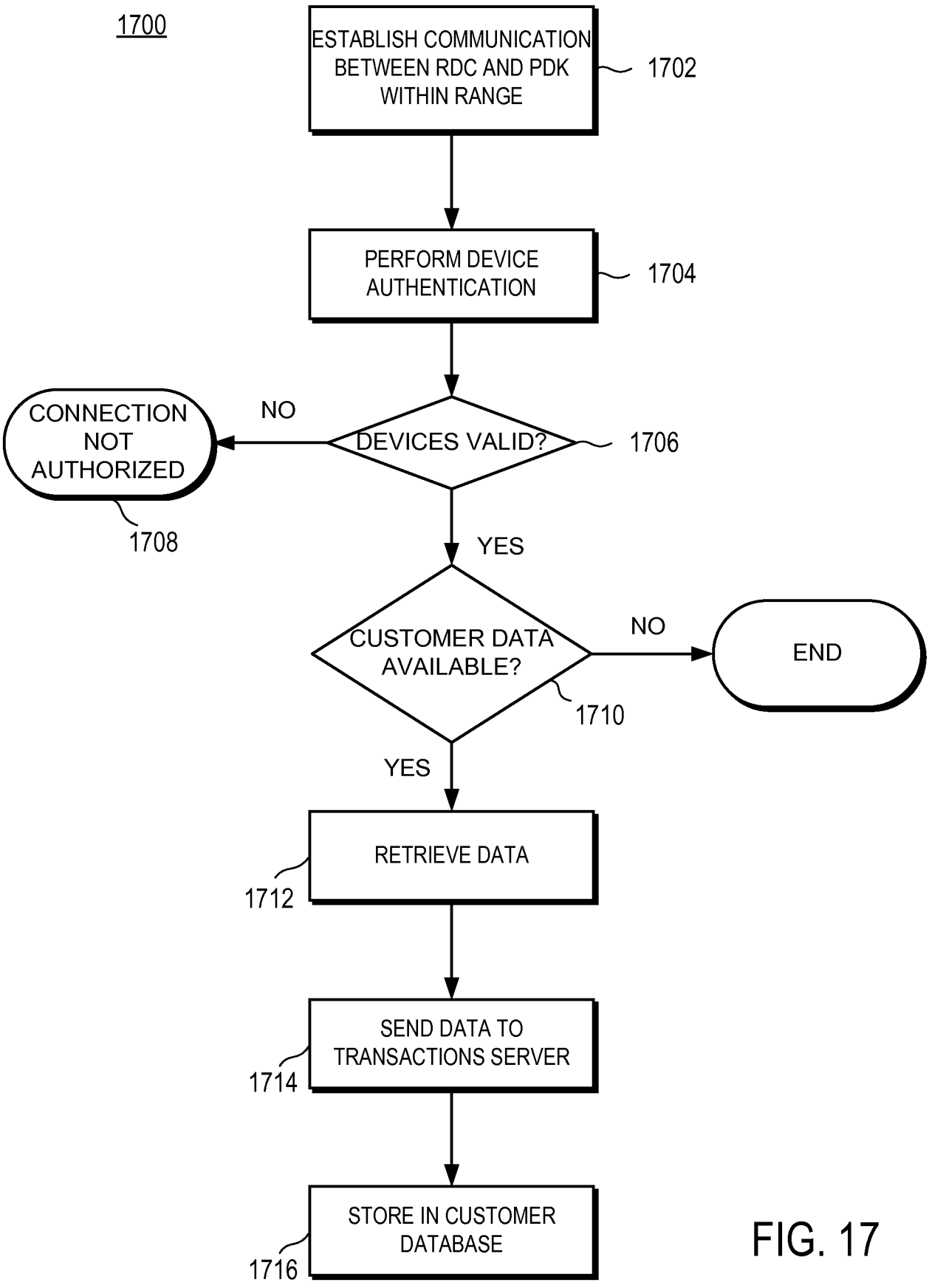
1700
ESTABLISH COMMUNICATION BETWEEN RDC AND PDK WITHIN RANGE
1702
PERFORM DEVICE AUTHENTICATION
1704
DEVICES VALID?
1706
NO
CONNECTION NOT AUTHORIZED
1708
YES
CUSTOMER DATA AVAILABLE?
1710
NO
END
YES
RETRIEVE DATA
1712
SEND DATA TO TRANSACTIONS SERVER
1714
STORE IN CUSTOMER DATABASE
1716

FIG. 17

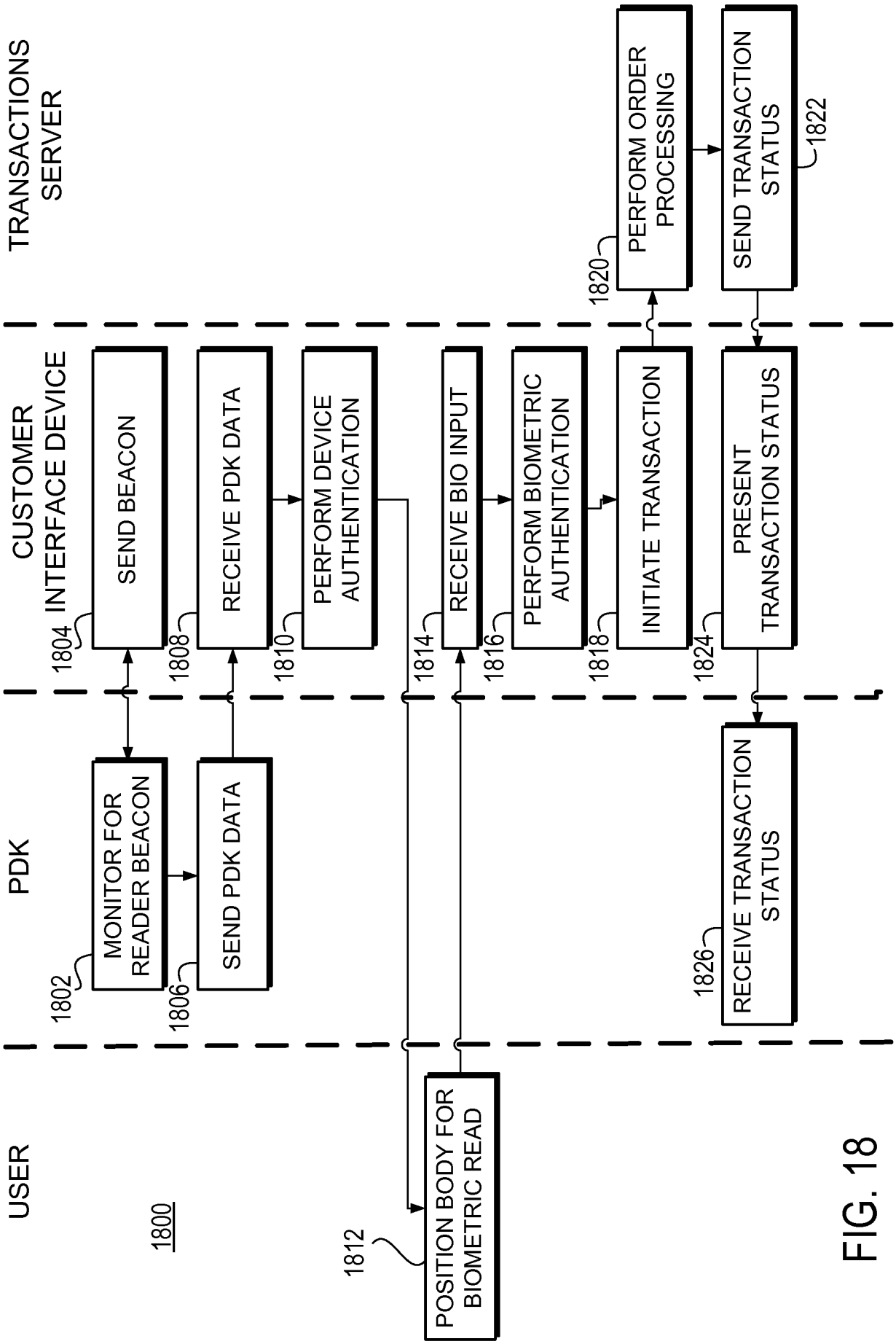
USER
PDK
CUSTOMER INTERFACE DEVICE
TRANSACTIONS SERVER
1800
1802
MONITOR FOR READER BEACON
1804
SEND BEACON
1806
SEND PDK DATA
1808
RECEIVE PDK DATA
1810
PERFORM DEVICE AUTHENTICATION
1812
POSITION BODY FOR BIOMETRIC READ
1814
RECEIVE BIO INPUT
1816
PERFORM BIOMETRIC AUTHENTICATION
1818
INITIATE TRANSACTION
1820
PERFORM ORDER PROCESSING
1822
SEND TRANSACTION STATUS
1824
PRESENT TRANSACTION STATUS
1826
RECEIVE TRANSACTION STATUS

FIG. 18

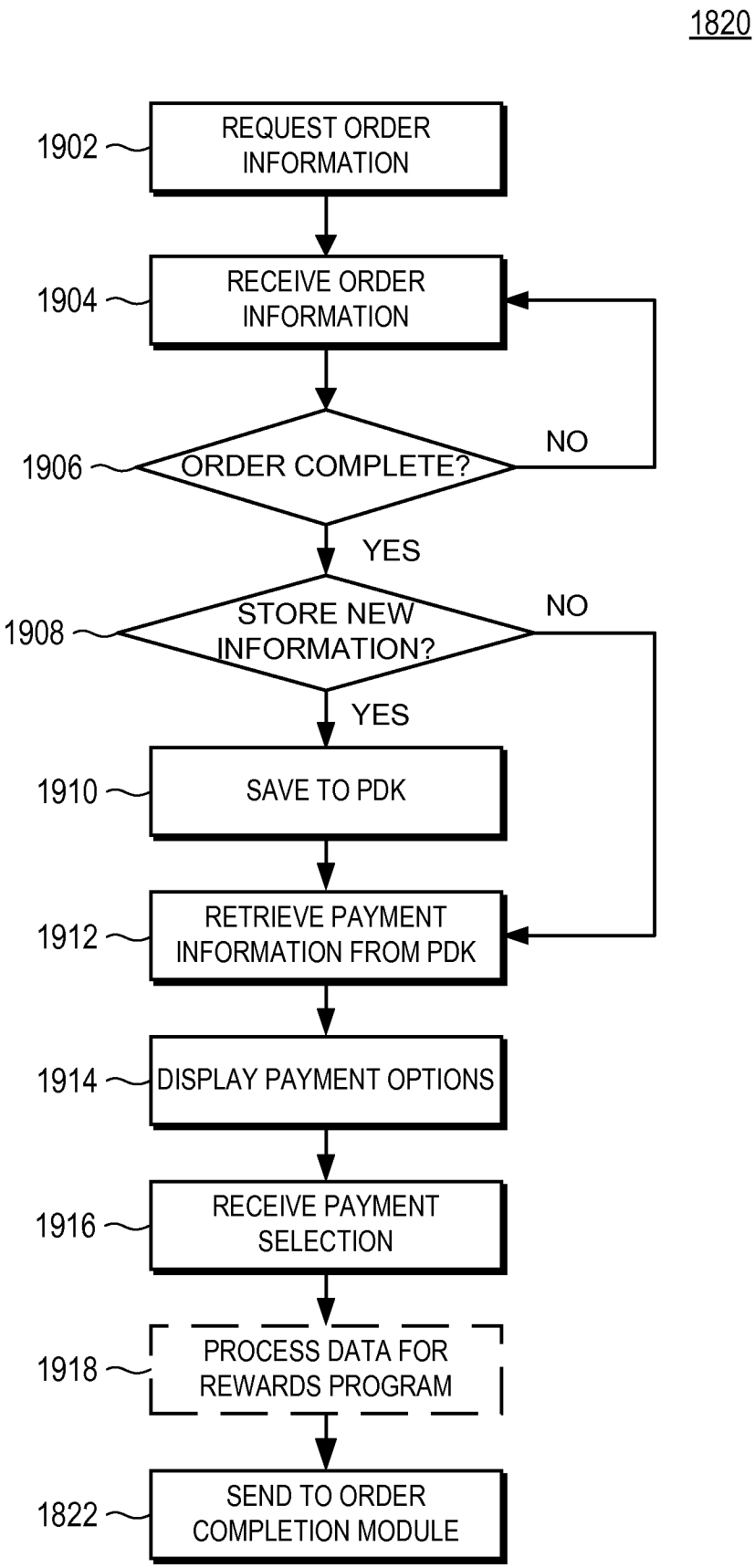
1820
1902
REQUEST ORDER INFORMATION
1904
RECEIVE ORDER INFORMATION
1906
ORDER COMPLETE?
NO
YES
1908
STORE NEW INFORMATION?
NO
YES
1910
SAVE TO PDK
1912
RETRIEVE PAYMENT INFORMATION FROM PDK
1914
DISPLAY PAYMENT OPTIONS
1916
RECEIVE PAYMENT SELECTION
1918
PROCESS DATA FOR REWARDS PROGRAM
1822
SEND TO ORDER COMPLETION MODULE

FIG. 19

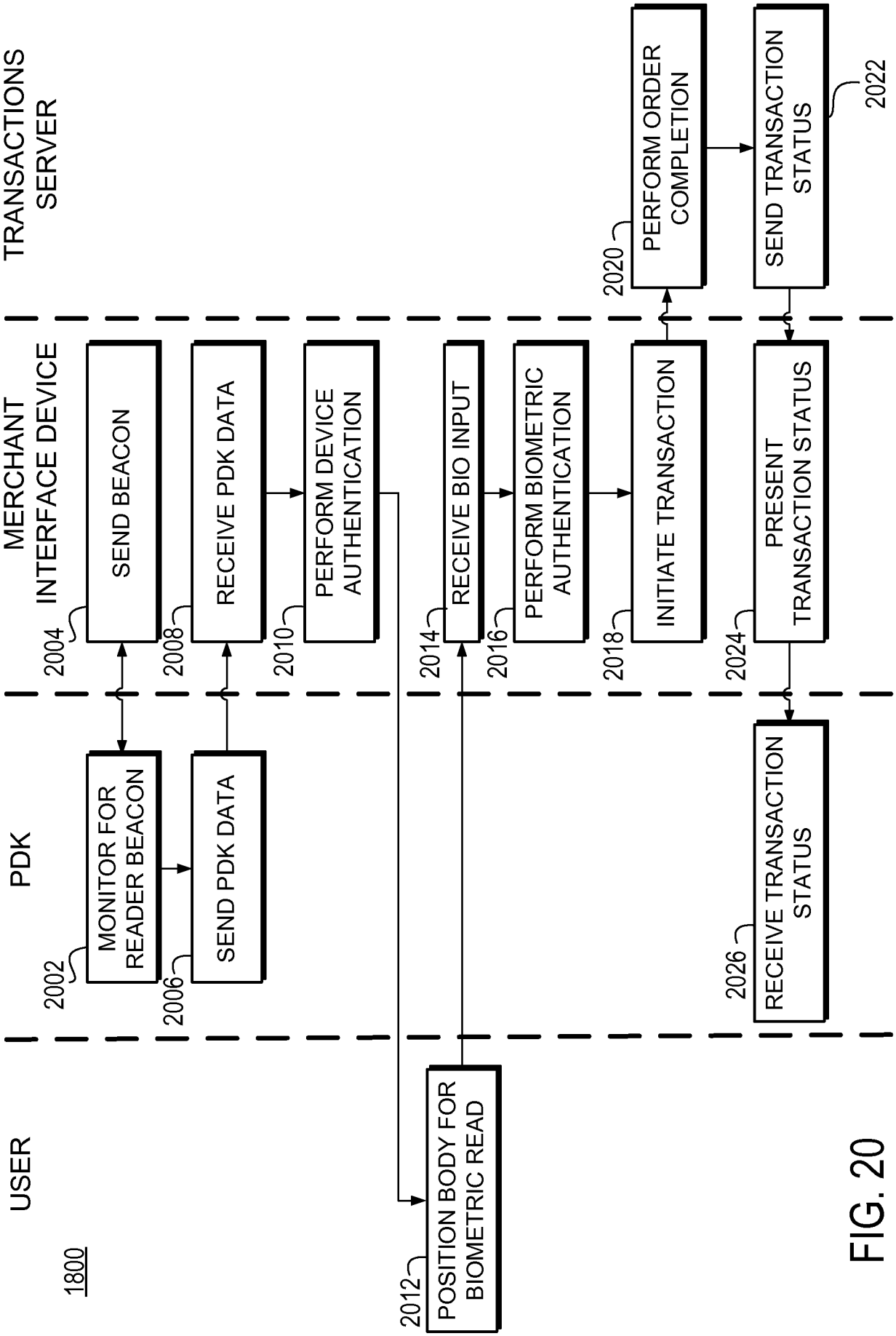
1800
USER
PDK
MERCHANT INTERFACE DEVICE
TRANSACTIONS SERVER
MONITOR FOR READER BEACON
2002
SEND BEACON
2004
SEND PDK DATA
2006
RECEIVE PDK DATA
2008
PERFORM DEVICE AUTHENTICATION
2010
POSITION BODY FOR BIOMETRIC READ
2012
RECEIVE BIO INPUT
2014
PERFORM BIOMETRIC AUTHENTICATION
2016
INITIATE TRANSACTION
2018
PERFORM ORDER COMPLETION
2020
SEND TRANSACTION STATUS
2022
PRESENT TRANSACTION STATUS
2024
RECEIVE TRANSACTION STATUS
2026

FIG. 20

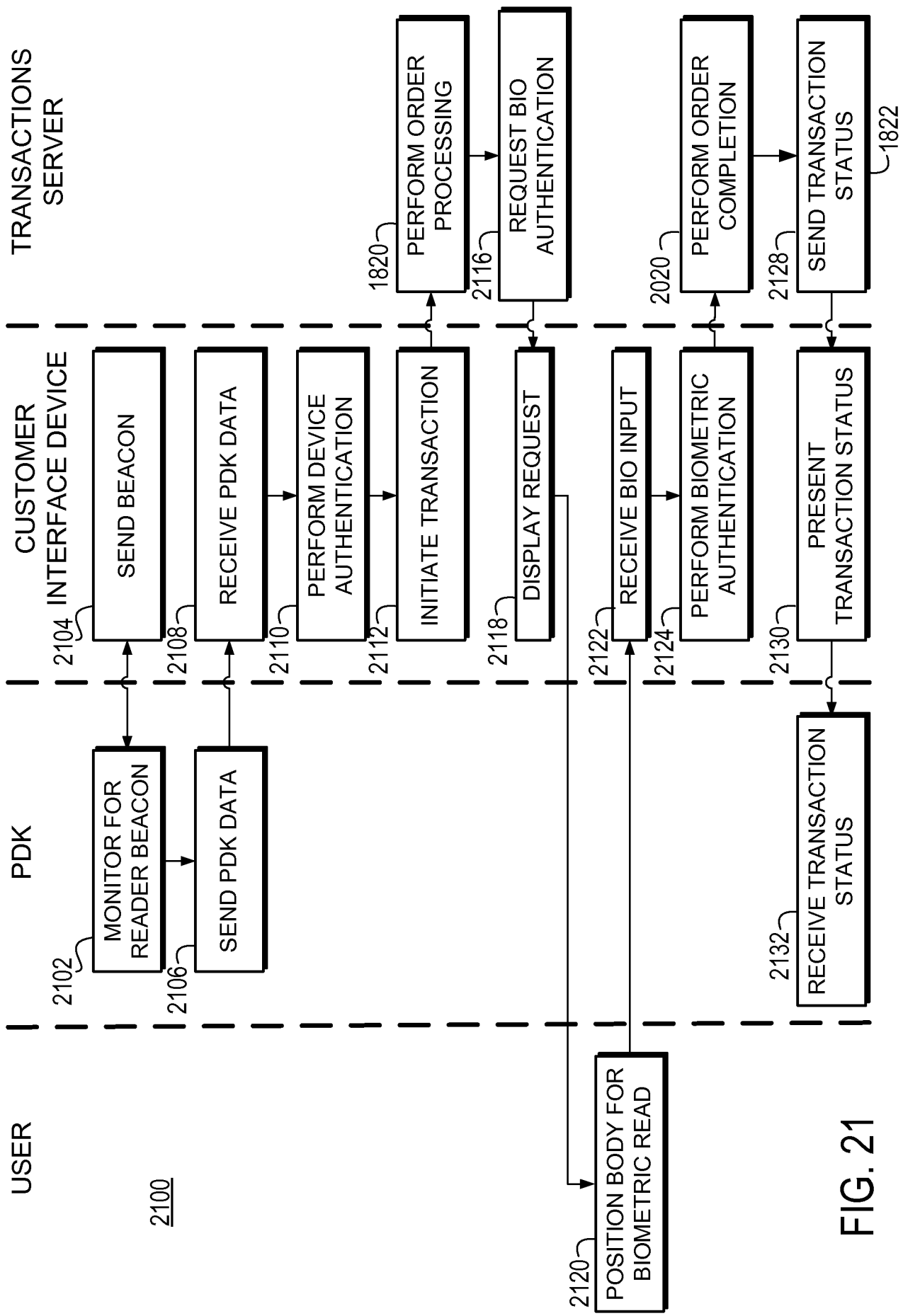
TRANSACTIONS SERVER
CUSTOMER INTERFACE DEVICE
PDK
USER
2100
SEND BEACON
2104
RECEIVE PDK DATA
2108
PERFORM DEVICE AUTHENTICATION
2110
INITIATE TRANSACTION
2112
DISPLAY REQUEST
2118
RECEIVE BIO INPUT
2122
PERFORM BIOMETRIC AUTHENTICATION
2124
PRESENT TRANSACTION STATUS
2130
MONITOR FOR READER BEACON
2102
SEND PDK DATA
2106
RECEIVE TRANSACTION STATUS
2132
POSITION BODY FOR BIOMETRIC READ
2120
PERFORM ORDER PROCESSING
1820
REQUEST BIO AUTHENTICATION
2116
PERFORM ORDER COMPLETION
2020
SEND TRANSACTION STATUS
2128
1822

FIG. 21

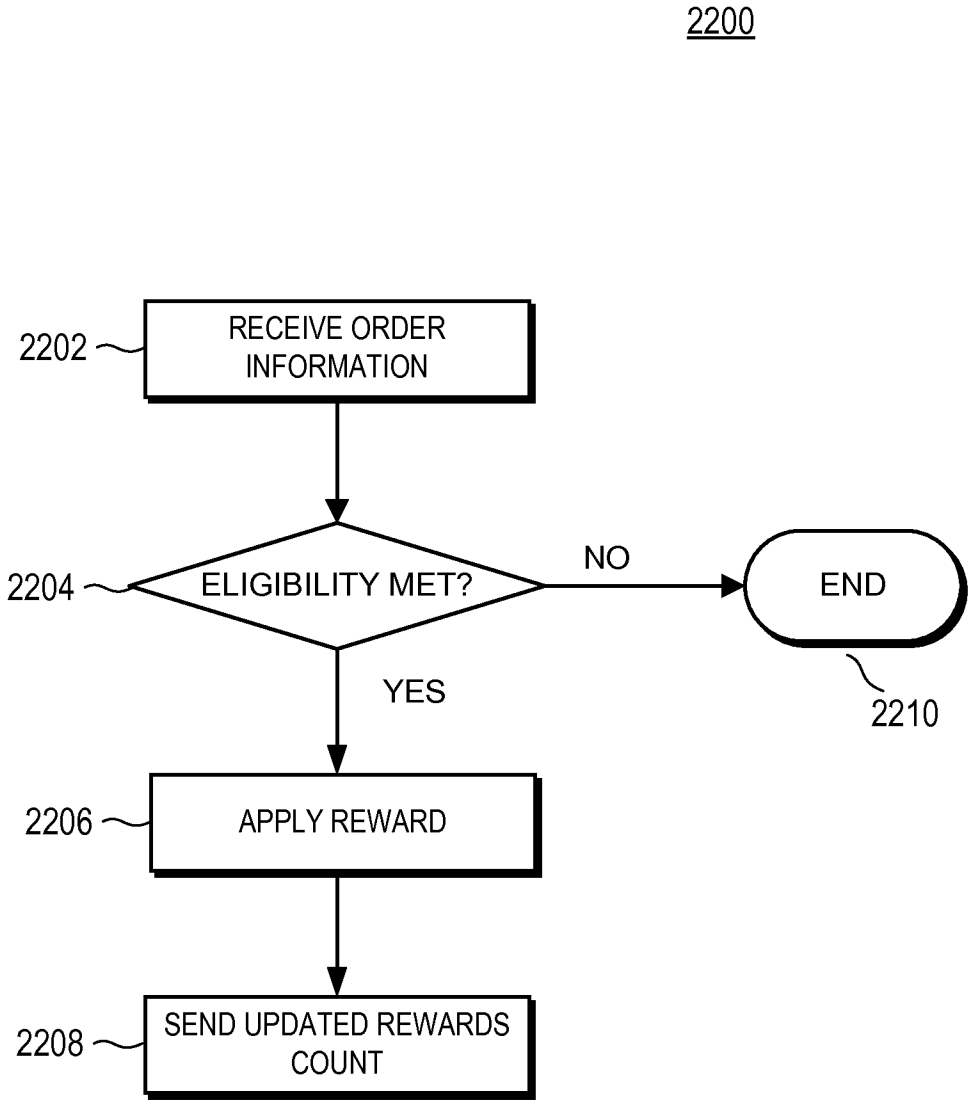
2200
2202
RECEIVE ORDER INFORMATION
2204
ELIGIBILITY MET?
NO
END
2210
YES
2206
APPLY REWARD
2208
SEND UPDATED REWARDS COUNT

FIG. 22