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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 September 2014 (25.09.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/151892 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04W 12/06* (2009.01)

(21) International Application Number:
PCT/US2014/026625

(22) International Filing Date:
13 March 2014 (13.03.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/837,703 15 March 2013 (15.03.2013) US

(71) Applicant: **QUALCOMM INCORPORATED** [US/US]; ATTN: International IP Administration, 5775 Morehouse Drive, San Diego, California 92121-1714 (US).

(72) Inventors: **TINNAKORNSRISUPHAP, Peerapol**; 5775 Morehouse Drive, San Diego, California 92121 (US). **BENOIT, Olivier Jean**; 5775 Morehouse Drive, San Diego, California 92121 (US). **KUMAR, Rajesh**; 5775 Morehouse Drive, San Diego, California 92121 (US).

(74) Agents: **LEWIN, Mario J.** et al.; 15201 Mason Road, Suite 1000-312, Cypress, Texas 77433 (US).

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

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

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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

(54) Title: SEAMLESS DEVICE CONFIGURATION IN A COMMUNICATION NETWORK

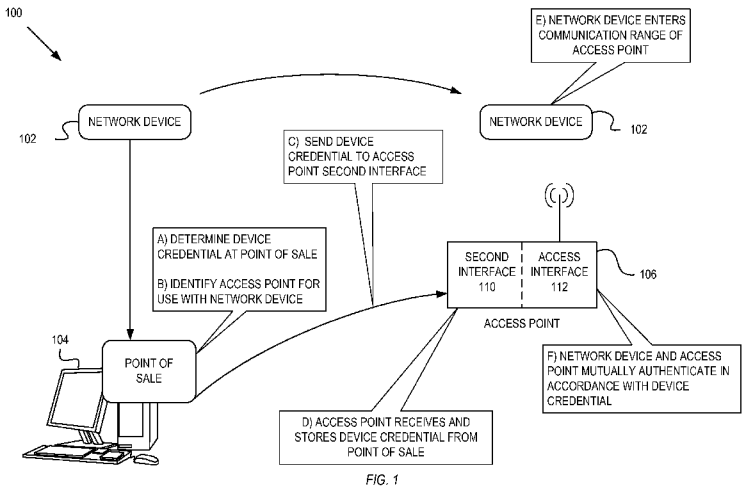

FIG. 1

(57) Abstract: Seamless device configuration techniques between a network device and an access point are disclosed. In one example, a device credential associated with the network device is sent to the access point before the network device communicates with the access point. The device credential can be used to verify the identity of the network device and can authenticate the network device with the access point without requiring user interaction. In another example, a central authority can maintain a database of network devices, access points and associated users. The central authority can determine when one or more network devices can seamlessly be configured for use with a particular access point. The central authority can send the device credential associated with the one or more network devices to the access point before the network device communicates with the access point.

WO 2014/151892 A1

SEAMLESS DEVICE CONFIGURATION IN A COMMUNICATION NETWORK

RELATED APPLICATIONS

[0001] This application claims the priority benefit of U.S. Application Serial No. 13/837,703 filed Mar 15, 2013.

BACKGROUND

[0002] Embodiments of the inventive subject matter generally relate to the field of communication systems and, more particularly, to configuring communication devices for use within a communication network.

[0003] Often, a user of a network device can be required to authenticate to an access point to gain access to network resources available through the access point. The authentication procedure can use security credentials provided by the user to control access and prevent unauthorized usage. Typical authentication steps can include entering codes or other information by the user as the network device comes within communication range of the access point. These configuration steps can seem overly complicated to some users and may discourage the use of networks and their resources altogether.

SUMMARY

[0004] Disclosed herein are various embodiments of seamless device configuration of a network device for use in a communication network. In some embodiments, a method comprises: receiving, at a terminal in a first network, a device credential associated with a network device; identifying an authentication recipient in a second network to receive the device credential; and sending, from the terminal to the identified authentication recipient, the device credential, wherein the device credential is used to authenticate the network device for operation with an access point prior to the network device communicating with the access point.

[0005] In some embodiments, the authentication recipient is a cellular modem integrated within the access point.

[0006] In some embodiments, the access point receives the device credential through a short message service (SMS) message.

[0007] In some embodiments, the method further comprises verifying a source of the SMS message and ignoring the SMS message when the source is not from a known retailer.

[0008] In some embodiments, the authentication recipient is identified by a phone number.

[0009] In some embodiments, the authentication recipient is a cellular phone.

[0010] In some embodiments, the cellular phone forwards the device credential to the access point.

[0011] In some embodiments, the forwarding occurs after detecting an input at the cellular phone indicative of approval that the network device associated with the device credential shall be allowed to authenticate with the access point.

[0012] In some embodiments, the device credential is stored in the network device when the network device is manufactured.

[0013] In some embodiments, the device credential is a Personal Identification Number or Device Password associated with the network device at a time of manufacture.

[0014] In some embodiments, the identifying the authentication recipient comprises using a scanner to read a quick response (QR) code placed on a package of the network device.

[0015] In some embodiments, the identifying the authentication recipient comprises using a scanner to read a barcode placed on a package of the network device.

[0016] In some embodiments, the device credential is included in a near field communication (NFC) tag.

[0017] In some embodiments, the method further comprises receiving a validation phrase in response to sending the device credential.

[0018] In some embodiments, the device credential is an encrypted device credential.

[0019] In some embodiments, the method further comprises sending, from the terminal to a decryption device, the encrypted device credential, wherein the decryption device decrypts the

encrypted device credential and provides the decrypted device credential to the authentication recipient.

[0020] In some embodiments, the method further comprises sending an identity of the authentication recipient to the decryption device.

[0021] In some embodiments, the authentication recipient is identified with a phone number.

[0022] In some embodiments, the sending, from the terminal to the decryption device, the encrypted device credential further comprises detecting an input at the authentication recipient indicative of approval that the network device associated with the decrypted device credential shall be allowed to authenticate with the access point.

[0023] In some embodiments, a method comprises: generating, at a terminal in a first network, a one-time password; sending the one-time password to a network device in a second network, wherein one-time password is stored in the network device; identifying an authentication recipient; and sending the one-time password to the authentication recipient, wherein the one-time password is used to authenticate the network device for operation with an access point prior to the network device communicating with the access point.

[0024] In some embodiments, the authentication recipient is identified by a phone number.

[0025] In some embodiments, the access point receives the one-time password through a short message service (SMS) message.

[0026] In some embodiments, the authentication recipient is a cellular phone.

[0027] In some embodiments, the cellular phone forwards the one-time password to the access point.

[0028] In some embodiments, the forwarding occurs after detecting an input at the cellular phone indicative of approval that the network device associated with the one-time password shall be allowed to authenticate with the access point.

[0029] In some embodiments, a method comprises: receiving, at an access point in a first network, a device credential associated with a network device, wherein the device credential is determined at a point of sale terminal when the network device is sold; and authenticating, the

network device for use in a second network with the access point prior to the network device communicating with the access point.

[0030] In some embodiments, the receiving, at the access point in the first network, the device credential associated with the network device, further comprises receiving the device credential from an authentication recipient.

[0031] In some embodiments, the authentication recipient is a cell phone.

[0032] In some embodiments, the receiving, at the access point in the first network, the device credential associated with the network device, further comprises receiving the device credential through a short message service (SMS) message.

[0033] In some embodiments, the receiving, at the access point in the first network, the device credential associated with the network device, further comprises receiving the device credential from the point of sale terminal.

[0034] In some embodiments, the device credential is a PIN code.

[0035] In some embodiments, a method comprises: receiving, at a computing server from a point of sale terminal in a first network, a first device credential associated with an access point; associating a first user identifier with the access point; receiving, at the computing server from a terminal in a second network, a second device credential associated with a network device; associating a second user identifier with the network device; and sending the second device credential to the access point to authenticate the network device with the access point when the first user identifier is associated with the second user identifier prior to the network device communicating with the access point.

[0036] In some embodiments, the associating the second user identifier with the network device, further comprises receiving the second user identifier from a second point of sale terminal.

[0037] In some embodiments, the first device credential is a serial number.

[0038] In some embodiments, the method further comprises sending, the first device credential to a manufacturer of the access point in response to receiving the first device credential; and receiving a public encryption key associated with the access point.

[0039] In some embodiments, the sending the second device credential to the access point further comprises sending the second device credential through a secure connection to the access point.

[0040] In some embodiments, the method further comprises storing a private encryption key in the access point.

[0041] In some embodiments, the second device credential is a personal identification number (PIN) code.

[0042] In some embodiments, the method further comprises storing the first device credential, the first user identifier, the second device credential and the second user identifier in a database at the computing server.

[0043] In some embodiments, the first user identifier and the second user identifier are associated with different users.

[0044] In some embodiments, a system comprises: a terminal configured to receive, in a first network, a device credential associated with a network device; an authentication recipient, in a second network, configured to receive the device credential from the terminal; and an access point configured to receive the device credential from the authentication recipient and authenticate the network device for operation with the access point prior to the network device communicating with the access point.

[0045] In some embodiments, the authentication recipient is further configured to provide the device credential to the access point after detecting an input indicative of approval that the network device associated with the device credential shall be allowed to authenticate with the access point.

[0046] In some embodiments, the authentication recipient is further configured to forward the device credential to the access point through a short message service (SMS) message.

[0047] In some embodiments, the access point comprises a cellular modem configured to receive the SMS message from the authentication recipient.

[0048] In some embodiments, the device credential is encrypted.

[0049] In some embodiments, the system further comprises a decryption device, wherein the terminal is further configured to send the encrypted device credential to the decryption device and the decryption device decrypts the encrypted device credential and provides a decrypted device credential to the authentication recipient.

[0050] In some embodiments, the authentication recipient is further configured to provide the decrypted device credential to the access point after detecting an input indicative of approval that the network device associated with the decrypted device credential shall be allowed to authenticate with the access point

[0051] In some embodiments, a non-transitory machine-readable storage media having instructions stored therein, which when executed by one or more processors causes the one or more processors to perform operations that comprise: receiving, at a terminal in a first network, a device credential associated with a network device; identifying an authentication recipient in a second network to receive the device credential; and sending, from the terminal to the identified authentication recipient, the device credential, wherein the device credential is used to authenticate the network device for operation with an access point prior to the network device communicating with the access point.

[0052] In some embodiments, the non-transitory machine-readable storage media further comprises forwarding the device credential from the authentication recipient to the access point.

[0053] In some embodiments, the forwarding the device credential from the authentication recipient to the access point further comprises detecting an input at the authentication recipient indicative of approval that the network device associated with the device credential shall be allowed to authenticate with the access point.

[0054] In some embodiments, the sending, from the terminal to the identified authentication recipient, the device credential further comprises forwarding the device credential through a short message service message (SMS).

[0055] In some embodiments, the device credential is encrypted.

[0056] In some embodiments, the non-transitory machine-readable storage media further comprises sending, from the terminal to a decryption device, the encrypted device credential, wherein the decryption device decrypts the encrypted device credential and provides the decrypted device credential to the authentication recipient.

[0057] In some embodiments, the sending, from the terminal to a decryption device, the encrypted device credential further comprises detecting an input at the authentication recipient indicative of approval that the network device associated with the decrypted device credential shall be allowed to authenticate with the access point.

BRIEF DESCRIPTION OF THE DRAWINGS

[0058] The present embodiments may be better understood, and numerous objects, features, and advantages made apparent to those skilled in the art by referencing the accompanying drawings.

[0059] **Figure 1** is a system diagram illustrating one embodiment of a seamless device configuration method used in a communication network.

[0060] **Figures 2A – 2B** are system diagrams illustrating embodiments of a seamless device configuration method used in a communication network.

[0061] **Figure 3A – 3B** show flow diagrams illustrating exemplary operations for seamless device configuration in a communication network.

[0062] **Figure 4** is a system diagram illustrating yet another embodiment of a seamless device configuration method used in a communication network.

[0063] **Figure 5** is a flow diagram illustrating another embodiment of example operations for seamless device configuration in a communication network.

[0064] **Figures 6A-6C** a system diagram illustrating still another embodiment of a seamless device configuration method in a communication network.

[0065] **Figure 7** is a flow diagram illustrating yet another embodiment of example operations for seamless device configuration in a communication network.

[0066] **Figure 8** is a block diagram of an exemplary embodiment of an electronic device including a wireless interface for network communications.

DESCRIPTION OF EMBODIMENT(S)

[0067] The description that follows includes exemplary systems, methods, techniques, instruction sequences and computer program products that embody techniques of the present inventive subject matter. However, it is understood that the described embodiments may be practiced without these specific details. For instance, although examples refer to wireless networks, other types of networks are contemplated such as wire-based networks such as coaxial cable, twisted pair, power line or other technically feasible networks. In other instances, well-known instruction instances, protocols, structures and techniques have not been shown in detail in order not to obfuscate the description.

[0068] Often, participation in a communication network by a network device through an access point is controlled so that access to network resources available through the access point is also controlled. Controlled access can prevent unintended or unauthorized access. Traditional access control methods allow a user device and network device to "authenticate" with an access point. Authentication allows the user to verify that a particular device is authorized to access a network. Typical authentication steps include entering codes or other credentials by the user as the network device comes within communication range of the access point. These configuration steps can seem overly complicated and time consuming to some users and may discourage the use of networks and their resources altogether.

[0069] Seamless device configuration can reduce or eliminate any required user interaction and simplify user access while maintaining a controlled access environment. One embodiment of a method for seamless configuration of network devices for use with a communication network can authenticate a network device with an access point prior to the network device being connected to the access point. Authentication can enable the network device to access resources connected to networks accessible through the access point such as data storage, printers, cloud-based resources, internet access, etc. A device credential associated with the network device can be stored within the access point before the network device is within communication range of the

access point. The access point can also store device credentials associated with other network devices. The access point can use the device credential to authenticate the network device without sharing (transmitting) the device credential. For example, the access point can proves its possession of the device credential to the network device using operations based on, at least in part, Diffie-Hellman, Simultaneous Authentication of Equals (SAE), Wi-Fi Protected Setup (WPS) or any other technically feasible authentication protocol based on the device credential. If the access point does not authenticate the network device, then the access point can refuse network access for the network device. In this manner, permission to gain access to the access point can be transparent to the user, without the user having to enter codes or passwords.

[0070] The device credential can be entered and stored into the access point directly through a communication interface at the access point, or the device credential can be entered indirectly through a trusted device, such as a smart phone. That is, for indirect entry, the device credential can first be sent to a trusted device, other than the access point. The trusted device can forward the device credential to the access point. In one embodiment, the trusted device can forward the device credential after access is approved by the user or a third party.

[0071] In another embodiment, instead of a device credential, a one-time password can be assigned to the network device. The one-time password can be stored directly or indirectly in the access point as described above. The access point can authenticate the network device using the one-time password. For example, the access point can prove its possession of the device credential to the network device using operations based on, at least in part, Diffie-Hellman, Simultaneous Authentication of Equals (SAE), Wi-Fi Protected Setup (WPS) or any other technically feasible authentication protocol based on the device credential. The one-time password can be more secure than the device credential because the one-time password can be generated, assigned and transmitted through secure channels, making it more difficult to clone or spoof.

[0072] In yet another embodiment, a Central Authority can track the association of network devices, access points and users. For example, when the user purchases an access point, an access point device identifier can be associated with a user (such as through a user ID). The association can be stored in a database by the Central Authority. When a network device is purchased by the user, a network device credential associated with the network device can be associated with the user and again stored by the Central Authority in the database. The Central

Authority can determine when a network device can be seamlessly authenticated with an access point by matching user IDs associated with the network devices with user IDs associated with access points. The Central Authority can send the network device credential to be stored in the access point. When the network device seeks to connect to the access point, the access point and network device can mutually authenticate using the device credential. For example, the access point can prove its possession of the device credential to the network device using operations based on, at least in part, Diffie-Hellman, Simultaneous Authentication of Equals (SAE), Wi-Fi Protected Setup (WPS) or any other technically feasible authentication protocol based on the device credential.

[0073] **Figure 1** is a system diagram 100 illustrating one embodiment of a seamless device configuration method used in a communication network. In an overview of the system diagram 100 shown in Figure 1, a device credential can be associated with network device 102. The device credential can be stored within network device 102 and can also be transmitted directly to a network gateway such as access point 106. When network device 102 seeks to access a communication network served by access point 106, access point 106 can authenticate network device 102 when network device 102 proves its possession of the device credential to access point 106.

[0074] Network device 102 can be a network device and can take the form of any technically feasible device that can transfer data through a communication network. Exemplary network devices 102 can be smart phones, laptops, netbooks, tablet computers, smart thermostats, smart home appliances (furnaces, stereos, network capable televisions, etc.) and the like. For example, network devices 102 can be devices with wireless interfaces such as interfaces that conform to ZigBee®, IEEE 802.11 standards or Bluetooth ® enabled devices. In other embodiments, network device 102 can take the form of a wired device such as one that communicates over Ethernet or a device that includes an interface that can conform with a powerline communications protocol such as those described by the HomePlug Alliance®.

[0075] At stage A, a device credential of network device 102 can be determined. In one embodiment, the device credential can be determined when the network device is sold. Examples of device credentials can be a serial number or a personal identification number (PIN) code or any technically feasible code or string that can be used to identify network device 102. For example, when network device 102 is sold at a terminal, such as a point of sale terminal 104,

the device credential can be read from packaging surrounding network device 102. In one embodiment, the device credential can be assigned to network device 102 when the device is manufactured. In another embodiment, the device credential can be encoded and printed as a quick response (QR) code, barcode or other machine readable code (not shown) on the packaging of network device 102. For example, the device credential can be determined by simply reading the QR code with a camera, smart phone, scanner or other QR code reader. Using a machine readable code, such as a QR code, can help to determine the device credential relatively quickly and can reduce human error associated with obtaining or reading the device credential. In yet another embodiment, a near field communication (NFC) tag (not shown) containing the device credential can be provided by the manufacture and attached to, or located proximate to network device 102. The NFC tag can be read by a NFC tag reader to determine the device credential. Using the NFC tag can also reduce errors in determining device credentials of network device 102.

[0076] At stage B, access point 106 can be identified by the user or purchaser of network device 102. Access point 106 can function as a gateway or entry point for a network. By identifying access point 106, the user or purchaser can indicate that he/she desires network device 102 to access a network and/or network resources through access point 106. Access point 106 can include access interface 112. Access interface 112 can provide a communication interface to network device 102. Access interface 112 can be implemented a wireless interface such as a WiFi interface conforming to IEEE 802.11 specifications, ZigBee, WiMAX, Bluetooth and others. In another embodiment, access interface 112 can be any technically feasible wired interface such as Ethernet, power line communications (PLC) such as those specified by the HomePlug Alliance and others.

[0077] Access point 106 can also include second interface 110. In some embodiments, second interface 110 can provide an independent communication interface to access point 106. For example, second interface 110 can be implemented with a cellular radio or modem. In this manner, access point 106 can be identified with a phone number and can receive SMS (short message service) messages. In other embodiments, second interface 110 can be provided with other interfaces such as a wired connection to other networks, such as a cloud network, or other network related resources such as Internet based networks.

[0078] In some embodiments, access point 106 can support a short message service (SMS) client through an Internet connection. The SMS client can be associated with a phone number and can receive SMS messages without the need for a cellular radio. Thus, access point 106 can again be identified with a phone number, even when access point 106 does not include a cellular radio. In still other embodiments, access point 106 can be identified with an email address.

[0079] At stage C, the device credential (as described in stage A) is sent to access point 106. For example, the device credential can be sent by a seller or retailer involved at point of sale terminal 104 when network device 102 is purchased and the access point 106 is identified. In one embodiment, the device credential can be sent via a SMS message addressed to the phone number associated with access point 106. The SMS message can be received by second interface 110 of access point 106, particularly when second interface 110 includes a cellular modem or interface. In other embodiments, the SMS message can be sent to a SMS client associated with access point 106, such as a SMS client running on a processor included in access point 106.

[0080] As described above, the device credential can be sent at a time of sale of network device 102. For example, the sale can be provided by a seller operating a "brick and mortar" type of retail store. In another embodiment, the sale of network device 102 can by through an online seller. In both cases, the seller can send the device credential to an identified access point 106 through an SMS message.

[0081] In one embodiment, second interface 110 of access point 106 can be identified with a descriptor device. The descriptor device can ease the task of identifying access point 106 for the user by providing a user friendly tool for providing the phone number associated with access point 106 to a registrar so that the device credential can be sent to access point 106. One example of a descriptor device can be a card with a magnetic stripe that can be provided to the user/owner of access point 106 (when access point 106 is purchased or deployed) and can include the phone number associated with access point 106. In this manner, access point 106 can be identified by reading the magnetic stripe on the card. The magnetic stripe card can reduce errors that may be associated with identifying access point 106. In another embodiment, an NFC device including the phone number associated with access point 106 can be provided to the user/owner of access point 106. The provided NFC device can be used to provide the phone number to identify access point 106. Descriptor devices can simplify stage B related processes

by providing a simpler and more error free method for determining the phone number associated with access point 106.

[0082] At stage D, access point 106 can receive the device credential and store the device credential within access point 106. The device credential can be received through second interface 110 or access interface 112. In one embodiment, the recipient of the device credential can be referred to as an authentication recipient. For example, if the device credential is sent as an SMS message, then access point 106 can receive the SMS message through second interface 110 when second interface includes a cellular radio or modem. In another example, a SMS message can be received through second interface 110 when a SMS client is provided within second interface 110. The device credential can be stored in memory within access point 106 such as random access memory (RAM), flash RAM, EEPROM, or any other persistent or semi-persistent storage device.

[0083] In one embodiment, before accepting the contents of the SMS message, the source of the SMS message can optionally be verified. For example, if the SMS message is received from a trustworthy source, such as a known retailer, then access point 106 can accept the contents of the SMS message. Known retailers can be determined by comparing the sending SMS phone numbers against a list of verified retailers. The source of the SMS message can be determined by reviewing the sending phone number associated with the SMS message. Verifying the sender of the SMS message can help prevent false or spoofed messages from being accepted by access point 106.

[0084] In some embodiments, access point 106 can send a validation phrase back to the sender of the SMS message. The validation phrase can include a phrase or numbers to acknowledge successful receipt of the SMS message including the device credential information. The validation phrase can be used to help determine when the SMS message including the network device credential has been sent to an incorrect phone number. For example, when the user identifies access point 106 with a phone number associated with access point 106, a SMS message can be sent to access point 106. If the validation phrase returned from access point 106 is not a phrase that is expected, then the purchase can determine that the device credential may have sent to an incorrect phone number. The sender of the SMS message can take appropriate steps to correct the issue.

[0085] At stage E, network device 102 can enter communication range of access point 106. For example, if network device 102 is a wireless device, network device 102 can be moved to a position such that radio signals can be transmitted and received between network device 102 and access point 106. Alternatively, if network device 102 is a wired device, then network device 102 can be within communication range when network device 102 is coupled to access point 106 through a wire, powerline or cable.

[0086] At stage F, network device 102 and access point 106 can mutually authenticate using device credential. For example, network device 102 can prove its possession of the device credential to access point 106 (using device credentials stored within access point 106). Device credentials can be received and stored in access point 106 as described in stage D above. Proof of possession of the device credential can be based on, at least in part, Diffie-Hellman, Simultaneous Authentication of Equals (SAE), Wi-Fi Protected Setup (WPS) or any other technically feasible authentication protocol based on the device credential.

[0087] If possession of the device credential is verified (proven), then network device 102 can be authenticated with access point 106. When network device 102 is authenticated, network device 102 can access networks coupled directly or indirectly to access point 106. In one embodiment, network device 102 can communicate with access point 106 through access interface 112 while second interface 110 can access and communicate directly or indirectly with other networks.

[0088] Figure 1 can be referred to as a direct method since the device credential is provided directly to access point 106. The direct method can be straightforward and require little, if any, user interaction. An indirect method can offer an increased level of security by sending the device credential to a trusted device for verification prior to forwarding to access point 106. The indirect method is described below in conjunction with Figure 2.

[0089] **Figures 2A** and **2B** are system diagrams 200 and 250 illustrating embodiments of a seamless device configuration method used in a communication network. System diagram 200 shows a system without encrypted device credentials. System diagram 250 differs slightly from system diagram 200 since system diagram 250 includes encrypted device credentials.

[0090] Beginning with System diagram 200 in Figure 2A, at stage A, the device credential associated with network device 102 is determined. This is similar to stage A as described in

Figure 1 above. At stage B, user device 202 can be identified for receiving the device credential. User device 202 can be a trusted device such as a smart phone, tablet computer or any other technically feasible device that can receive the device credential and can communicate with access point 106 as described below in conjunction with stages C and D. User device 202 can be referred to as an authentication recipient because device credentials can be received thereby. In one embodiment, user device 202 can be identified with a phone number. For example, user device 202 can include a cellular phone or modem or can include a SMS client running on a processor included in user device 202 that can be configured to respond to a phone number. In another embodiment, user device 202 can be identified with an email address. Descriptor devices as described in conjunction with stage A of Figure 1 can also be used to identify user device 202.

[0091] At stage C, the device credential determined in stage A can be sent to user device 202. As described above in Figure 1, the device credential can be sent by a seller or retailer involved at point of sale terminal 104 when network device 102 is purchased. The device credential can be sent via a SMS message addressed to the phone number associated with user device 202 (particularly when user device 202 can be identified with a phone number). In another embodiment, the device credential can be sent through an email message, Uniform Resource Locator (URL), social media notification messages, operating system notification messages, or any other technically feasible messaging protocol to user device 202.

[0092] At stage D, the device credential can be forwarded to access point 106 from user device 202. In one embodiment, the forwarding is not automatic, but rather can involve user interaction to review the device credential at user device 202 and actively forward the device credential to access point 106. The user receiving the device credential at user device 202 needs not be the owner or user of network device 102, but instead can be an owner, user or administrator of access point 106. Actions at user device 202 (the forwarding of the device credential) can configure access point 106 to authorize the user of network device 102 to have access to access point 106 as well as networks directly or indirectly coupled to access point 106. Since the device credential is sent indirectly to access point 106 through user device 202, an extra layer of security can be realized by requiring an active action on the part of a third party to actively forward the device credential to access point 106.

[0093] In one embodiment, user device 202 can forward the device credential to access point 106 through access interface 112. For example, if access interface 112 is a WiFi interface, and user device 202 also includes a WiFi interface and has previously authenticated with access point 106, then user device 202 can forward the device credential to access point 106 through access interface 112. In another embodiment, both user device 202 and access point 106 can include a cellular radio or modem (i.e., second interface 110 can include the cellular radio or modem) that can be used to forward and receive the device credential. For example, user device 202 can forward the device credential via a SMS message that can be received through second interface 110 of access point 106.

[0094] At stage E, network device 102 can enter communication range of access point 106. At stage F, network device 102 and access point 106 can mutually authenticate using device credential. In some implementations, stages E and F can be similar to the like named stages described in Figure 1 above.

[0095] Turning to system diagram 250 in Figure 2B, at stage A, the encrypted device credential associated with network device 102 is determined. This can be similar to stage A as described in Figure 1. However, in this embodiment, the device credential can be encrypted. Encrypting the device credential can add a level of security by obfuscating the device credential, particularly when the device credential is available on packaging surrounding network device 102 or can be read from barcode or QR code. In one embodiment, the device credential can be encrypted with asymmetric encryption such as an encryption method that uses public and private encryption keys. In another embodiment, the device credential can be encrypted with symmetric encryption method using a shared encryption key.

[0096] At stage B, user device 202 can be identified for receiving the device credential. In one embodiment, user device 202 can be identified with a phone number. In another embodiment, user device 202 can be identified with an email address. At stage C, the encrypted device credential and a user device 202 identifier (determined in stage B) can be sent to server 255. In one embodiment, server 255 can verify a sender identity of the encrypted device credential to help prevent from using server 255 from unauthorized or malicious use. For example, server 255 can verify that the encrypted device credential was sent by a known point of sale terminal 104 or an associated trusted server. At stage D, server 255 can decrypt the encrypted device credential and then send the decrypted device credential to user device 202.

Server 255 can decrypt the device credential with an appropriate decryption method (symmetric or asymmetric, determined, at least in part, by a selected encryption method). In one embodiment, server 255 can send the decrypted device credential to a phone number used to identify user device 202 in stage B. In another embodiment, the decrypted device credential can be sent through an email message, Uniform Resource Locator (URL), social media notification messages, operating system notification messages, or any other technically feasible messaging protocol to user device 202. At stage E, the decrypted device credential can be forwarded to access point 106 from user device 202. Actions at user device 202 (the forwarding of the device credential) can configure access point 106 to authorize the user of network device 102 to have access to access point 106 as well as networks directly or indirectly coupled to access point 106. As described above, user device 202 can forward the decrypted device credential through access.

[0097] At stage F, network device 102 can enter communication range of access point 106. At stage G, network device 102 can authenticate with access point 106 using device credentials stored within access point 106. In one embodiment, this can be similar to stage F as described above in Figure 1. In one embodiment, network device 102 can communicate with access point 106 through access interface 112 while second interface 110 can access and communicate directly or indirectly with other networks.

[0098] **Figures 3A and 3B** show flow diagram 300 illustrating exemplary operations for seamless device configuration in a communication network. The method of Figure 3 is described with reference to the systems and components described in Figures 1 and 2 (for illustration purposes and not as a limitation). The example operations can be carried out by one or more components in system 100 or 200, such as terminal 104, a processor within network device 102, access point 106 or by user device 202. Beginning with block 302, the device credential associated with network device 102 can be determined. As described above, the device credential can be a serial number, PIN code or any technically feasible code or string that can identify network device 102. In some embodiments, the device credential can be a machine readable code such as a QR code, bar code or NFC tag that can be scanned to retrieve the device credential.

[0099] Proceeding to block 303, if the device credential is sent directly to access point 106, then the flow proceeds to block 304 where access point 106 is identified. As described above, access point 106 can be identified with a phone number, email address or any other technically

feasible means. The flow can proceed to block 306 where the determined device credential is sent to the identified access point 106. In one embodiment, the device credential is sent via a SMS message to access point 106. Access point 106 can include a cellular radio or modem that can be configured to receive SMS messages or access point 106 can include a SMS client running on a processor that can receive SMS messages. In another embodiment, access point 106 can receive the device credential through an email message.

[00100] Proceeding to block 308, the device credential is stored in access point 106. Access point 106 can include memory such as RAM, flash RAM, EEPROM, or any other persistent or semi-persistent storage device that can be used to store the received device credential. Proceeding to block 310, network device 102 can enter communication range of access point 106. If network device 102 and access point 106 both include wireless interfaces, then when network device 102 can be moved to a position such that radio signals can be transmitted and received between network device 102 and access point 106. In another embodiment, if network device 102 and access point 106 both include a wire-based interface such as cable-based Ethernet or PLC, then network device 102 can be within communication range of access point 106 when a wire-based connection is established between them.

[00101] Proceeding to block 312, access point 106 and network device 102 can mutually authenticate using the device credential. In some embodiments, network device 102 can prove its possession of the device credential to access point 106 and the flow ends.

[00102] Returning to block 303, if the device credential is sent indirectly to access point 106, then the flow proceeds to block 316 of Figure 3B where user device 202 can be identified. In one embodiment, user device 202 can be identified with a phone number, particularly when user device 202 is a smart phone. In another embodiment, user device 202 is identified with an email address. User device 202 can be any technically feasible device that can receive messages and can communicate with access point 106 such as a laptop, tablet computer or similar device. Proceeding to block 317, if the device credential is not encrypted, then flow proceeds to block 318 where the device credential can be sent to the identified user device 202. In one embodiment, the device credential can be sent via a SMS message. In another embodiment, the device credential can be sent through an email message.

[00103] Proceeding to block 320, a user, administrator or owner associated with access point 106 can forward the device credential from user device 202 to access point 106 and the flow can proceed to block 308 as described above.

[00104] Returning to block 317, if the device credential is encrypted, then flow proceeds to block 319. In block 319, server 255 can decrypt the encrypted device credential. Decryption can be asymmetric or symmetric decryption based, in part, on the encryption used when the device credential was formed as was described in stage A of Figure 3B. After the device credential is decrypted, the flow can proceed to block 318.

[00105] Although block 303 is shown in flow diagram 300, in some implementations the operations described in conjunction with block 303 can be omitted. For example in a first embodiment, operations according to blocks 302, 304, 306, 308, and 310 can be performed while in a second embodiment, operations according to blocks 302, 316, 317, 319, 318, 320, 308, and 310 can be performed. In both the first and second embodiments described above, decision block 303 would not actively be performed.

[00106] **Figure 4** is a system diagram 400 illustrating yet another embodiment of a seamless device configuration method used in a communication network. In an overview of system diagram 400, a one-time password can be generated and provided to network device 102 and to access point 106 replacing the use of the device credential described in Figures 1 and 2. Using a one-time password can be more secure than the device credential because the one-time password can be generated, assigned and transmitted through secure channels to the network device 102 and access point 106 making it relatively more difficult to clone or spoof.

[00107] At stage A, a one-time password can be generated. The one-time password can include letters, numbers or symbols and can be of a predetermined or variable length. In one embodiment, the one-time password can be generated by the point of sale terminal 104. In another embodiment, the one-time password can be generated by the purchaser or user of network device 102. For example, the purchaser or user can have an application that can run on a smart phone, tablet computer or other technically feasible device that can generate the one-time password. In one embodiment, the one-time password can be displayed as a barcode by a smart phone application.

[00108] At stage B, the one-time password is stored in network device 102. In one embodiment, network device 102 can be connected to an activation platform to receive the one-time password. For example, the connection between network device 102 and the activation platform can be a cable, such as a USB cable or the connection can be a secure (encrypted) link. By using a secure (encrypted) connection, the integrity and security of the one-time password is enhanced. In other embodiments, the one-time password can be sent to network device 102 through a Secure Digital (SD) card, or using NFC protocols and devices. The one-time password can be stored in a memory included in network device 102. The memory can be RAM, flash RAM, EEPROM, or any other persistent or semi-persistent storage device.

[00109] At stage C, user device 202 can be identified. User device 202 can be used to indirectly send the one-time password to access point 106 in a similar manner as described above in conjunction with Figure 2. User device 202 can include a cellular phone or modem or can include a SMS client running on a processor that can be identified with a phone number. In another embodiment, user device 202 can be identified with an email address. Device descriptors as described in conjunction with Figure 1 can also be used to identify user device 202.

[00110] At stage D, the one-time password can be sent to user device 202. As illustrated in Figure 4, in one embodiment point of sale terminal 104 can generate and send the one-time password to user device 202. In another embodiment, if the one-time password is generated by an application running on a device such as a smart phone or tablet computer, then the one-time password can be sent from the device (smart phone, tablet computer, etc.) directly to the user device 202.

[00111] At stage E the one-time password can be forwarded to and stored within access point 106 from user device 202. This can be similar to stage D described above in conjunction with Figure 2. User device 202 can forward one-time password to access point 106 through access interface 112. For example, if access interface 112 is a WiFi interface, and user device 202 also includes a WiFi interface and has previously authenticated with access point 106, then user device 202 can forward the one-time password to access point 106 through access interface 112. Alternatively, if both user device 202 and access point 106 includes a cellular radio or modem included in second interface 110, then user device 202 can forward the one-time password to access point 106 through an SMS message.

[00112] Similar to stage D described in conjunction with Figure 2, forwarding of the one-time password is not automatic, but rather involves user interaction to review the one-time password at user device 202 and actively forward the one-time password to access point 106. The user receiving the one-time password at user device 202 need not be the owner or user of network device 102, but instead can be an owner, user or administrator of access point 106. Actions at user device 202 can be seen as actions to authorize the user of network device 102 to have access to access point 106 as well as networks directly or indirectly coupled to access point 106. Since the one-time password is sent indirectly to access point 106 through user device 202, an extra layer of security can be realized by requiring an active action on the part of a third party to actively forward the one-time password to access point 106.

[00113] At stage F, network device 102 can enter communication range of access point 106. This stage can be similar to as described for stage E in Figures 1 or 2 above. At stage G, network device 102 and access point 106 can mutually authenticate. For example, network device can authenticate with access point 106 when network device 102 proves its possession of the one-time password to access point 106. This stage can be similar to as described for stage F in Figures 1 or 2 above.

[00114] **Figure 5** is a flow diagram 500 illustrating another embodiment of example operations for seamless device configuration in a communication network. The method of Figure 5 is described with reference to the systems and components described in Figure 4 (for illustration purposes and not as a limitation). The example operations can be carried out by one or more components in system 400 such as terminal 104, a processor within network device 102 or access point 106 or by user device 202.

[00115] Beginning in block 502, the one-time password can be generated. In one embodiment, the one-time password can be generated by a user through an application running on a smart phone or other technically feasible device. In another embodiment, the one-time password can be generated on a terminal involved during the sale of network device 102, such as point of sale terminal 104. Proceeding to block 504, the one-time password can be sent to and stored in network device 102. In one embodiment, the one-time password is sent through a secure connection to network device 102. In another embodiment, the one-time password is sent to network device 102 through a SD card or NFC device. The one-time password can be stored

in a memory included in network device 102. The memory can be RAM, flash RAM, EEPROM, or any other persistent or semi-persistent storage device.

[00116] Proceeding to block 506, the one-time password can be sent to user device 202. As described above, user device 202 can be a smart phone, tablet computer or any other technically feasible device. Proceeding to block 508, the one-time password can be forwarded from user device 202 to access point 106. This step can enable a confirmation of the access for network device 102. In block 510, access point 106 can receive and store one-time password within access point 106. For example, one-time password can be stored in a memory included within access point 106. Proceeding to block 512, network device can enter communication range of access point 106. Finally, in block 514, network device 102 and access point 106 can mutually authenticate using one-time password stored within access point 106 and the flow ends. In one embodiment, this can be similar to stage F as described above in Figure 1.

[00117] The embodiments shown in Figures 4 and 5 describe an indirect storing of the one-time password into access point 106 similar to the indirect methods shown and described in Figures 2 and 3. In another embodiment, the one-time password can be directly stored into access point 106 by simply sending the one-time password directly to access point 106 instead of going through the intermediate device of user device 202. For example, after the one-time password is generated, in block 506, the one-time password can be sent directly to access point 106 and block 508 can be omitted altogether.

[00118] **Figures 6A-6C** is a system diagram 600 illustrating still another embodiment of a seamless device configuration method in a communication network. In an overview of system diagram 600, a central authority can be used to maintain a database of access points, network devices and users. The central authority can associate a network device with an access point when the users associated with these devices can themselves be associated with each other. For example if a user identifier (user ID) associated with a particular access point matches (or is linked to) a user ID associated with a particular network device, and then the central authority can enable the access point to authenticate the network device. In one embodiment, the central authority can send a device credential (such as a PIN code, for example) associated with the network device to the access point. The access point can authenticate the network device when the network device proves its possession of the device credential to the access point. The central

authority can send the device credential to the access point before the network device enters within a communication range of the access point.

[00119] Turning to **Figure 6A**, at stage A, access point manufacturer 602 can assign a serial number 632 and public and private encryption keys (634 and 636 respectively) to access point 106. The use of encryption keys 634, 636 are not essential for the practice of the embodiment described herein; however as will be described below, the encryption keys 634, 636 can enhance protection by protecting access point 106 from unauthorized access. In one embodiment, the private encryption key 636 and serial number 632 can be stored within access point 106. Access point manufacturer 602 can maintain a list (not shown) including the serial numbers of access point 106, and the related public 634 and private 636 encryption keys. After the manufacture of access point 106, access point 106 can be shipped to a seller, reseller, online merchant, etc.

[00120] When access point 106 is sold to a user, such as user 608, database 606 maintained by central authority 604 can be updated. To this end, at stage B, the seller of access point 106 can send access point serial number 632, and user ID 630 of user 608 to central authority 604. Access point 106 can be sold at a terminal, such as point of sale terminal 104, or can be sold online. Access point serial number 632 can be determined by examining the packaging or case of access point 106, or in other embodiments, by scanning a label such as a barcode label or a QR code sticker (not shown). Central authority 604 can store user ID 630 and access point serial number 632 in database 606. At stage C, central authority 604 can send the determined access point serial number 632 to access point manufacturer 602. In return, at stage D, access point manufacturer 602 can respond with a public encryption key 634 associated with access point 106. At stage E, database 606 can be updated to include access point serial number 632, user ID 630 and the public encryption key 634 associated with access point 106.

[00121] Turning to **Figure 6B**, at stage F, network device manufacturer 610 can assign a serial number 640 and a device credential such as PIN code 620 to network device 102. As described above, in other embodiments, other device credentials can be used. The PIN code 620 can be stored within network device 102. In one embodiment, network device manufacturer 610 can maintain a list (not shown) associating PIN codes 620 with network device serial numbers 640. After the manufacture of network device 102, network device 102 can be shipped to a seller, reseller, online merchant, etc.

[00122] When network device 102 is sold, database 606 can be updated with the users' user ID 638 and serial number 640 of network device. 102. To that end, at stage G, the seller can send user ID 638 associated with user 608 and network device serial number 640 to central authority 604. Network device serial number 640 can be determined by examining the packaging or case of network device 102, or in other embodiments, by scanning a label such as a barcode label or a QR code sticker (not shown). At stage H, central authority 604 can send serial number 640 to network device manufacturer 610. In return, at stage J, network device manufacturer 610 can respond with PIN code 620 for network device 102. Central authority 604 can store the PIN code 620, network device serial number 640, and user ID 638 associated with network device 102 in database 606.

[00123] Turning to **Figure 6C**, the central authority 604 can examine database 606 and can associate network device 102 with access point 106 by noting a common user ID (user IDs 630 and 638). For example if access point user ID 630 is found that matches network device user ID 638, then the central authority 604 can associate network device 102 with access point 106. In another embodiment, user IDs 630 and 638 need not match exactly. That is, a single user ID can be replaced by a list of "equivalent" user IDs that can be viewed by central authority 604 as being the same as one single user ID. In this manner, a group of users can easily be referred to and can be associated with access point 106 or network device 102 for seamless device configuration.

[00124] When central authority 604 determines that network device 102 should be associated with access point 106, at stage L, central authority 604 can send PIN code 620 to access point 106. In one embodiment, central authority 604 can send PIN code 620 using encryption such as the public encryption key 634 stored in database 606. Since access point 106 includes private encryption key 636, PIN code 620 can be sent securely (encrypted) from central authority 604 to access point 106. At stage M, network device 102 can be positioned within communication range of access point 106 and can communicate with access point 106. At stage N, access point 106 and network device 102 can mutually authenticate using PIN code 620. For example, access point 106 can authenticate network device 102 when network device 102 proves its possession of the PIN code 620 to access point 106 and the method ends. Proof of possession of the PIN code 620 can be based on, at least in part, Diffie-Hellman, Simultaneous Authentication of Equals (SAE), Wi-Fi Protected Setup (WPS) or any other technically feasible authentication protocol.

Although PIN code 620 is used to authenticate network device 102 to access point 106 in this example, any other technically feasible device credential (as described above) can be used.

[00125] Although Figures 6A-6C describe using public/private key encryption for secure communications between central authority 604 and access point 106, other forms of encryption can be used (symmetric key, or shared key for example). In yet another embodiment, encryption can be ignored and communications between central authority 604 and access point 106 can be clear channel (open with no encryption) communications.

[00126] **Figure 7** is a flow diagram 700 illustrating yet another embodiment of example operations for seamless device configuration in a communication network. The method of Figure 7 is described with reference to the systems and components described in Figures 6A – 6C (for illustration purposes and not as a limitation). The example operations can be carried out by one or more components in system 700 such as terminal 104, a processor within network device 102 or access point 106.

[00127] Beginning in block 702, access point manufacturer 602 can assign serial number 632 and public 634 and private 636 encryption keys to access point 106. In one embodiment, serial number 632 can uniquely identify access point 106. Public 634 and private 636 encryption keys can be used for asymmetric encryption for secure transmission of messages. The private encryption key 636 can be stored within access point 106.

[00128] Proceeding to block 704, central authority 604 can receive a user ID 630 and a serial number 632 associated with access point 106. The user ID 630 and serial number 632 can be sent to central authority 604 when access point 106 is sold, either through an online sale or a sale occurring at a store at a terminal, such as a point of sale terminal 104. The user ID 630 can be assigned to identify a particular user 608 or group of users (not shown).

[00129] Proceeding to block 706, central authority 604 can send serial number 632 to access point manufacturer 602. Communications between central authority 604 and access point manufacturer 602 can be conducted on any technically feasible network, such as the Internet. Proceeding to block 708, central authority 604 can receive the public encryption key 634 from access point manufacturer 602. In one embodiment, the public encryption key 634 can be received in response to access point manufacturer 602 receiving serial number 632 sent in block 706. The public encryption key 634 can enable secure communications with access point 106 to

occur, if desired. Central authority 604 can store user ID 630, access point serial number 632 and access point public encryption key 634 in database 606.

[00130] Proceeding to block 710, network device manufacturer 610 can assign serial number 640 and PIN code 620 to network device 102. In one embodiment, PIN code 620 can also be stored within network device 102. Proceeding to block 712, central authority 604 can receive user ID 638 and serial number 640 associated with network device 102. The user ID 638 and serial number 640 can be sent to central authority 604 when network device 102 is sold, either through an online sale or a sale occurring at a terminal, such as point of sale terminal 104. Proceeding to block 714, central authority 604 can send network device serial number 640 to network device manufacturer 610. Proceeding to block 716, central authority 604 can receive PIN code 620 associated with network device 102. In one embodiment, PIN code 620 can be received from network device manufacturer 610 in response to receiving serial number 640 of network device 102. Central authority 604 can store user ID 638, network device serial number 640 and PIN code 620 in database 606.

[00131] Proceeding to block 718, central authority 604 can associate network device 102 with access point 106, by processing database 606. In one embodiment, the association between network device 102 and access point 106 can be determined by a common user ID associated with both devices. In another embodiment, two or more user IDs can be grouped together and treated as a single user ID. That is, a single user ID can be replaced by a list of "equivalent" user IDs that can be viewed by central authority 604 as being the same as one single user ID. In this manner, a group of users can easily be referred to and can be associated with access point 106 or network device 102.

[00132] Proceeding to block 720, central authority 604 can send PIN code 620 to access point 106 before network device 102 communicates with access point 106. PIN code 620 can be stored within access point 106. In one embodiment, PIN code 620 can be sent securely to access point 106 using asymmetric public/private key based encryption using the public encryption key 634 stored in central authority 604 and private encryption key 636 stored in access point 106. Proceeding to block 722, network device 102 and access point 106 can mutually authenticate using PIN code 620 and the flow can end.

[00133] It should be understood that Figures 1 – 7 and the operations described herein are examples meant to aid in understanding embodiments and should not be used to limit embodiments or limit scope of the claims. Embodiments may perform additional operations, fewer operations, operations in a different order, operations in parallel, and some operations differently.

[00134] As will be appreciated by one skilled in the art, aspects of the present inventive subject matter may be embodied as a system, method, or computer program product. Accordingly, aspects of the present inventive subject matter may take the form of an entirely hardware embodiment, a software embodiment (including firmware, resident software, micro-code, etc.) or an embodiment combining software and hardware aspects that may all generally be referred to herein as a "circuit," "module" or "system." Furthermore, aspects of the present inventive subject matter may take the form of a computer program product embodied in one or more computer readable medium(s) having computer readable program code embodied thereon.

[00135] Any combination of one or more computer readable medium(s) may be utilized. The computer readable medium may be a computer readable signal medium or a computer readable storage medium. A computer readable storage medium may be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples (a non-exhaustive list) of the computer readable storage medium would include the following: an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of the foregoing. In the context of this document, a computer readable storage medium may be any tangible medium that can contain, or store a program for use by or in connection with an instruction execution system, apparatus, or device.

[00136] A computer readable signal medium may include a propagated data signal with computer readable program code embodied therein, for example, in baseband or as part of a carrier wave. Such a propagated signal may take any of a variety of forms, including, but not limited to, electro-magnetic, optical, or any suitable combination thereof. A computer readable signal medium may be any computer readable medium that is not a computer readable storage

medium and that can communicate, propagate, or transport a program for use by or in connection with an instruction execution system, apparatus, or device.

[00137] Program code embodied on a computer readable medium may be transmitted using any appropriate medium, including but not limited to wireless, wireline, optical fiber cable, RF, etc., or any suitable combination of the foregoing.

[00138] Computer program code for carrying out operations for aspects of the present inventive subject matter may be written in any combination of one or more programming languages, including an object oriented programming language such as Java, Smalltalk, C++ or the like and conventional procedural programming languages, such as the "C" programming language or similar programming languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

[00139] Aspects of the present inventive subject matter are described with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and computer program products according to embodiments of the inventive subject matter. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[00140] These computer program instructions may also be stored in a computer readable medium that can direct a computer, other programmable data processing apparatus, or other devices to function in a particular manner, such that the instructions stored in the computer

readable medium produce an article of manufacture including instructions which implement the function/act specified in the flowchart and/or block diagram block or blocks.

[00141] The computer program instructions may also be loaded onto a computer, other programmable data processing apparatus, or other devices to cause a series of operational steps to be performed on the computer, other programmable apparatus or other devices to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide processes for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[00142] **Figure 8** is a block diagram of an exemplary embodiment of an electronic device 800 including a wireless interface 808 for network communications. In some implementations, the electronic device 800 may be one of a laptop computer, a tablet computer, a mobile phone, a powerline communication device, a smart appliance (PDA), or other electronic systems. The electronic device 800 can include processor unit 802 (possibly including multiple processors, multiple cores, multiple nodes, and/or implementing multi-threading, etc.). The electronic device 800 can also include memory unit 806. Memory unit 806 may be system memory (e.g., one or more of cache, SRAM, DRAM, zero capacitor RAM, Twin Transistor RAM, eDRAM, EDO RAM, DDR RAM, EEPROM, NRAM, RRAM, SONOS, PRAM, etc.) or any one or more of the above already described possible realizations of machine-readable media. Electronic device 800 can also include bus 810 (e.g., PCI, ISA, PCI-Express, HyperTransport®, InfiniBand®, NuBus, AHB, AXI, etc.), and a network interfaces 804 can include wire-based interfaces (e.g., an Ethernet interface, a powerline communication interface, etc.). Wireless interfaces 808 can include at least one of a wireless network interface (e.g., a WLAN interface, a Bluetooth interface, a WiMAX interface, a ZigBee interface, a Wireless USB interface, etc.), In some implementations, electronic device 800 may support multiple network interfaces - each of which is configured to couple the electronic device 800 to a different communication network.

[00143] The memory unit 806 embodies functionality to implement embodiments described above. The memory unit 806 may include one or more functionalities that facilitate seamless device configuration. For example, memory unit 806 can implement one or more aspects of terminal 104, access point 106 or central authority 604 as described above.

[00144] The memory unit 806 can embody functionality to implement embodiments described in Figures 1 – 7 above. In one embodiment, memory unit 806 can include one or more functionalities that facilitate sending and receiving PIN codes, identifier codes, serial numbers, encryption keys, and the like. Memory unit 806 can also facilitate maintaining a database, and authenticating a device, such as a network device 102. Memory unit 806 can also be used to provide persistent storage of data such as database 606. Any one of these functionalities may be partially (or entirely) implemented in hardware and/or on the processor unit 802. For example, some functionality may be implemented with an application specific integrated circuit, in logic implemented in the processor unit 802, in a co-processor on a peripheral device or card, etc. Further, realizations may include fewer or additional components not illustrated in Figure 8 (e.g., video cards, audio cards, additional network interfaces, peripheral devices, etc.). Processor unit 802, memory unit 806, network interface 804 and wireless interface 808 are coupled to bus 810. Although illustrated as being coupled to the bus 810, memory unit 806 may be coupled to processor unit 802.

[00145] While the embodiments are described with reference to various implementations and exploitations, it will be understood that these embodiments are illustrative and that the scope of the inventive subject matter is not limited to them. In general, techniques for seamless device configuration as described herein may be implemented with facilities consistent with any hardware system or hardware systems. Many variations, modifications, additions, and improvements are possible.

[00146] Plural instances may be provided for components, operations or structures described herein as a single instance. Finally, boundaries between various components, operations and data stores are somewhat arbitrary, and particular operations are illustrated in the context of specific illustrative configurations. Other allocations of functionality are envisioned and may fall within the scope of the inventive subject matter. In general, structures and functionality presented as separate components in the exemplary configurations may be implemented as a combined structure or component. Similarly, structures and functionality presented as a single component may be implemented as separate components. These and other variations, modifications, additions, and improvements may fall within the scope of the inventive subject matter.

CLAIMS

1. A method, comprising:

receiving, at a terminal in a first network, a device credential associated with a network device;

identifying an authentication recipient in a second network to receive the device credential; and

sending, from the terminal to the identified authentication recipient, the device credential, wherein the device credential is used to authenticate the network device for operation with an access point prior to the network device communicating with the access point.

2. The method of claim 1, wherein the authentication recipient is a cellular modem integrated within the access point.

3. The method of claim 2, wherein the access point receives the device credential through a short message service (SMS) message.

4. The method of claim 3, further comprising verifying a source of the SMS message and ignoring the SMS message when the source is not from a known retailer.

5. The method of claim 1, wherein the authentication recipient is identified by a phone number.

6. The method of claim 1, wherein the authentication recipient is a cellular phone.

7. The method of claim 6, wherein the cellular phone forwards the device credential to the access point.

8. The method of claim 7, wherein the forwarding occurs after detecting an input at the cellular phone indicative of approval that the network device associated with the device credential shall be allowed to authenticate with the access point.

9. The method of claim 1, wherein the device credential is stored in the network device when the network device is manufactured.

10. The method of claim 1, wherein the device credential is a Personal Identification Number or Device Password associated with the network device at a time of manufacture.

11. The method of claim 1, wherein the identifying the authentication recipient comprises using a scanner to read a quick response (QR) code placed on a package of the network device.

12. The method of claim 1, wherein the identifying the authentication recipient comprises using a scanner to read a barcode placed on a package of the network device.

13. The method of claim 1, wherein the device credential is included in a near field communication (NFC) tag.

14. The method of claim 1, further comprising receiving a validation phrase in response to sending the device credential.

15. The method of claim 1, wherein the device credential is an encrypted device credential.

16. The method of claim 15, further comprising sending, from the terminal to a decryption device, the encrypted device credential, wherein the decryption device decrypts the encrypted device credential and provides the decrypted device credential to the authentication recipient.

17. The method of claim 16, further comprising sending an identity of the authentication recipient to the decryption device.

18. The method of claim 16, wherein the authentication recipient is identified with a phone number.

19. The method of claim 16, wherein the sending, from the terminal to the decryption device, the encrypted device credential further comprises detecting an input at the authentication recipient indicative of approval that the network device associated with the decrypted device credential shall be allowed to authenticate with the access point.

20. A method comprising:
generating, at a terminal in a first network, a one-time password;
sending the one-time password to a network device in a second network, wherein one-time password is stored in the network device;
identifying an authentication recipient; and
sending the one-time password to the authentication recipient, wherein the one-time password is used to authenticate the network device for operation with an access point prior to the network device communicating with the access point.

21. The method of claim 20, wherein the authentication recipient is identified by a phone number.

22. The method of claim 21, wherein the access point receives the one-time password through a short message service (SMS) message.

23. The method of claim 20, wherein the authentication recipient is a cellular phone.

24. The method of claim 23, wherein the cellular phone forwards the one-time password to the access point.

25. The method of claim 24, wherein the forwarding occurs after detecting an input at the cellular phone indicative of approval that the network device associated with the one-time password shall be allowed to authenticate with the access point.

26. A method comprising:
receiving, at an access point in a first network, a device credential associated with a network device, wherein the device credential is determined at a point of sale terminal when the network device is sold; and

authenticating, the network device for use in a second network with the access point prior to the network device communicating with the access point.

27. The method of claim 26, wherein the receiving, at the access point in the first network, the device credential associated with the network device, further comprises receiving the device credential from an authentication recipient.

28. The method of claim 27, wherein the authentication recipient is a cell phone.

29. The method of claim 26, wherein the receiving, at the access point in the first network, the device credential associated with the network device, further comprises receiving the device credential through a short message service (SMS) message.

30. The method of claim 26, wherein the receiving, at the access point in the first network, the device credential associated with the network device, further comprises receiving the device credential from the point of sale terminal.

31. The method of claim 26, wherein the device credential is a PIN code.

32. A method comprising:

receiving, at a computing server from a point of sale terminal in a first network, a first device credential associated with an access point;

associating a first user identifier with the access point;

receiving, at the computing server from a terminal in a second network, a second device credential associated with a network device;

associating a second user identifier with the network device; and

sending the second device credential to the access point to authenticate the network device with the access point when the first user identifier is associated with the second user identifier prior to the network device communicating with the access point.

33. The method of claim 32, wherein the associating the second user identifier with the network device, further comprises receiving the second user identifier from a second point of sale terminal.

34. The method of claim 32, wherein the first device credential is a serial number.

35. A method of claim 32, further comprising:
sending, the first device credential to a manufacturer of the access point in response to receiving the first device credential; and
receiving a public encryption key associated with the access point.

36. The method of claim 35, wherein the sending the second device credential to the access point further comprises sending the second device credential through a secure connection to the access point.

37. The method of claim 35, further comprising storing a private encryption key in the access point.

38. The method of claim 32, wherein the second device credential is a personal identification number (PIN) code.

39. The method of claim 32, further comprising storing the first device credential, the first user identifier, the second device credential and the second user identifier in a database at the computing server.

40. The method of claim 32, wherein the first user identifier and the second user identifier are associated with different users.

41. A system comprising:
a terminal configured to receive, in a first network, a device credential associated with a network device;
an authentication recipient, in a second network, configured to receive the device credential from the terminal; and
an access point configured to receive the device credential from the authentication recipient and authenticate the network device for operation with the access point prior to the network device communicating with the access point.

42. The system of claim 41, wherein the authentication recipient is further configured to provide the device credential to the access point after detecting an input indicative of approval that the network device associated with the device credential shall be allowed to authenticate with the access point.

43. The system of claim 41, wherein the authentication recipient is further configured to forward the device credential to the access point through a short message service (SMS) message.

44. The system of claim 43, wherein the access point comprises a cellular modem configured to receive the SMS message from the authentication recipient.

45. The system of claim 41, wherein the device credential is encrypted.

46. The system of claim 45, further comprising a decryption device, wherein the terminal is further configured to send the encrypted device credential to the decryption device and the decryption device decrypts the encrypted device credential and provides a decrypted device credential to the authentication recipient.

47. The system of claim 46, wherein the authentication recipient is further configured to provide the decrypted device credential to the access point after detecting an input indicative of approval that the network device associated with the decrypted device credential shall be allowed to authenticate with the access point

48. A non-transitory machine-readable storage media having instructions stored therein, which when executed by one or more processors causes the one or more processors to perform operations that comprise:

receiving, at a terminal in a first network, a device credential associated with a network device;

identifying an authentication recipient in a second network to receive the device credential; and

sending, from the terminal to the identified authentication recipient, the device credential, wherein the device credential is used to authenticate the network device for operation with an access point prior to the network device communicating with the access point.

49. The non-transitory machine-readable storage media of claim 48, further comprises forwarding the device credential from the authentication recipient to the access point.

50. The non-transitory machine-readable storage media of claim 49, wherein the forwarding the device credential from the authentication recipient to the access point further comprises detecting an input at the authentication recipient indicative of approval that the network device associated with the device credential shall be allowed to authenticate with the access point.

51. The non-transitory machine-readable storage media of 48, wherein the sending, from the terminal to the identified authentication recipient, the device credential further comprises forwarding the device credential through a short message service message (SMS).

52. The non-transitory machine-readable storage media of claim 48, wherein the device credential is encrypted.

53. The non-transitory machine-readable storage media of claim 52, further comprising sending, from the terminal to a decryption device, the encrypted device credential, wherein the decryption device decrypts the encrypted device credential and provides the decrypted device credential to the authentication recipient.

54. The non-transitory machine-readable storage media of claim 53, wherein the sending, from the terminal to a decryption device, the encrypted device credential further comprises detecting an input at the authentication recipient indicative of approval that the network device associated with the decrypted device credential shall be allowed to authenticate with the access point.

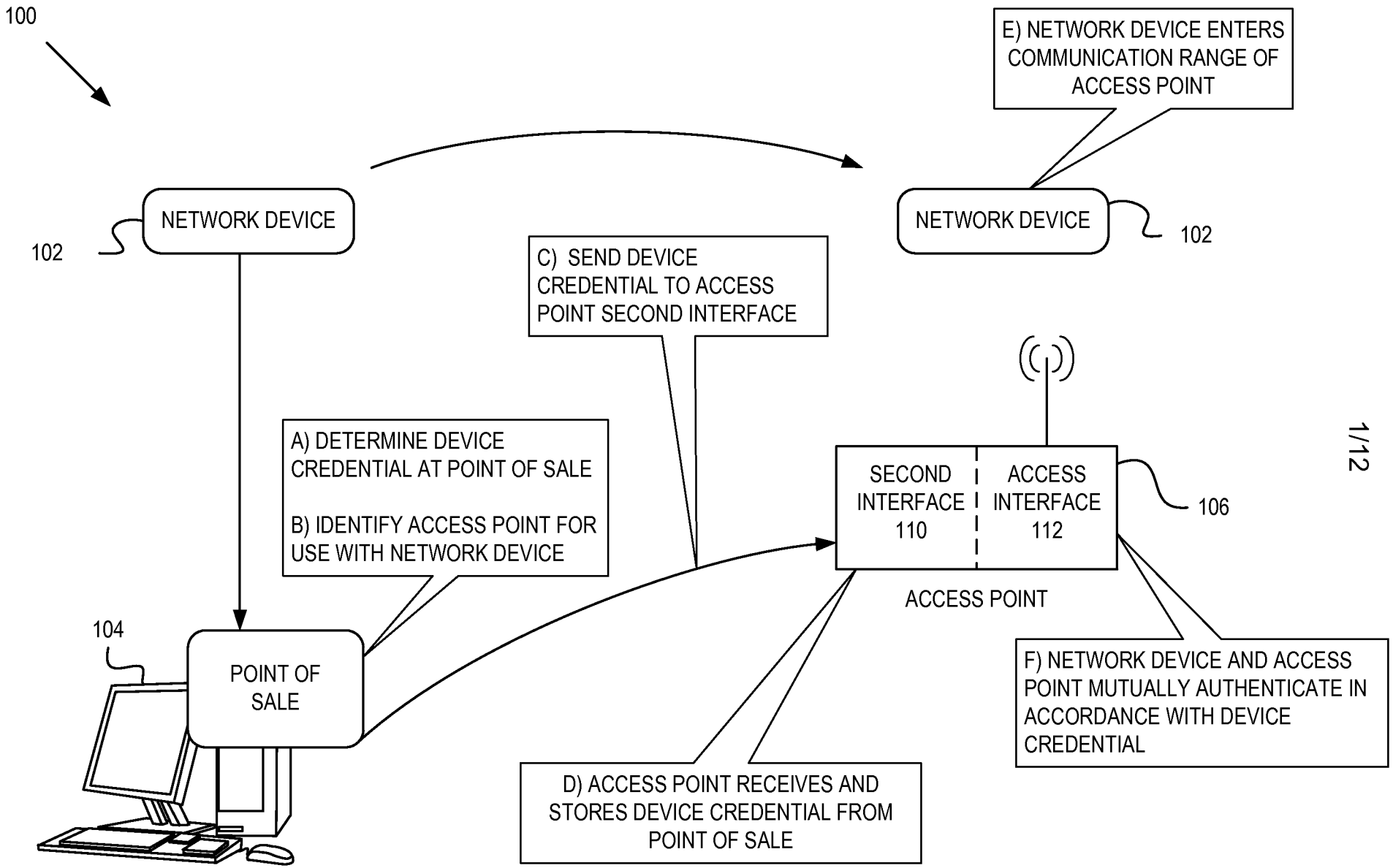
100
NETWORK DEVICE
102
E) NETWORK DEVICE ENTERS COMMUNICATION RANGE OF ACCESS POINT
NETWORK DEVICE
102
C) SEND DEVICE CREDENTIAL TO ACCESS POINT SECOND INTERFACE
A) DETERMINE DEVICE CREDENTIAL AT POINT OF SALE
B) IDENTIFY ACCESS POINT FOR USE WITH NETWORK DEVICE
SECOND INTERFACE 110
ACCESS INTERFACE 112
106
ACCESS POINT
104
POINT OF SALE
F) NETWORK DEVICE AND ACCESS POINT MUTUALLY AUTHENTICATE IN ACCORDANCE WITH DEVICE CREDENTIAL
D) ACCESS POINT RECEIVES AND STORES DEVICE CREDENTIAL FROM POINT OF SALE

FIG. 1

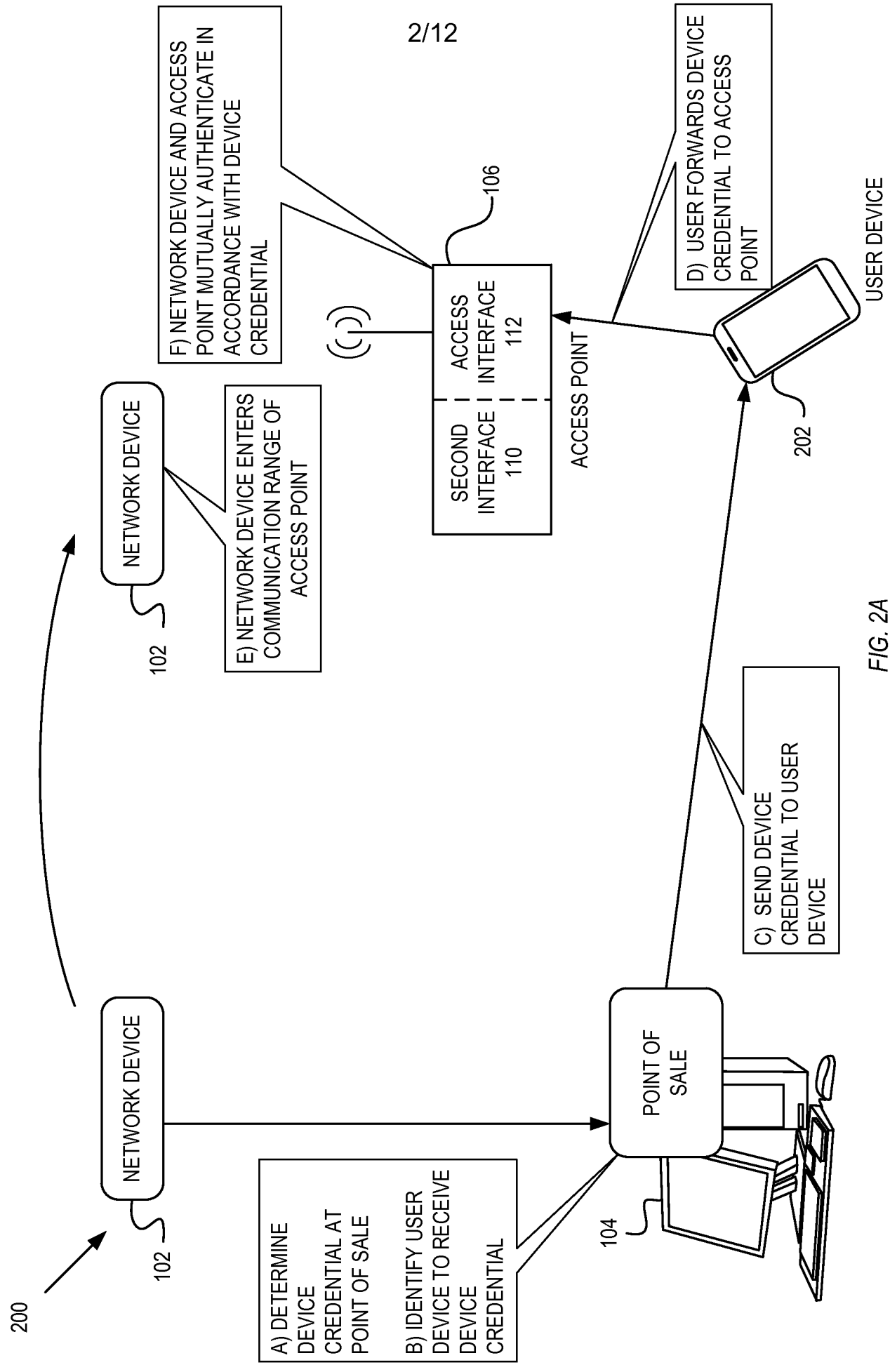
200
NETWORK DEVICE
102
A) DETERMINE DEVICE CREDENTIAL AT POINT OF SALE
B) IDENTIFY USER DEVICE TO RECEIVE DEVICE CREDENTIAL
POINT OF SALE
104
C) SEND DEVICE CREDENTIAL TO USER DEVICE
USER DEVICE
202
D) USER FORWARDS DEVICE CREDENTIAL TO ACCESS POINT
ACCESS POINT
SECOND INTERFACE 110
ACCESS INTERFACE 112
106
E) NETWORK DEVICE ENTERS COMMUNICATION RANGE OF ACCESS POINT
NETWORK DEVICE
102
F) NETWORK DEVICE AND ACCESS POINT MUTUALLY AUTHENTICATE IN ACCORDANCE WITH DEVICE CREDENTIAL

FIG. 2A

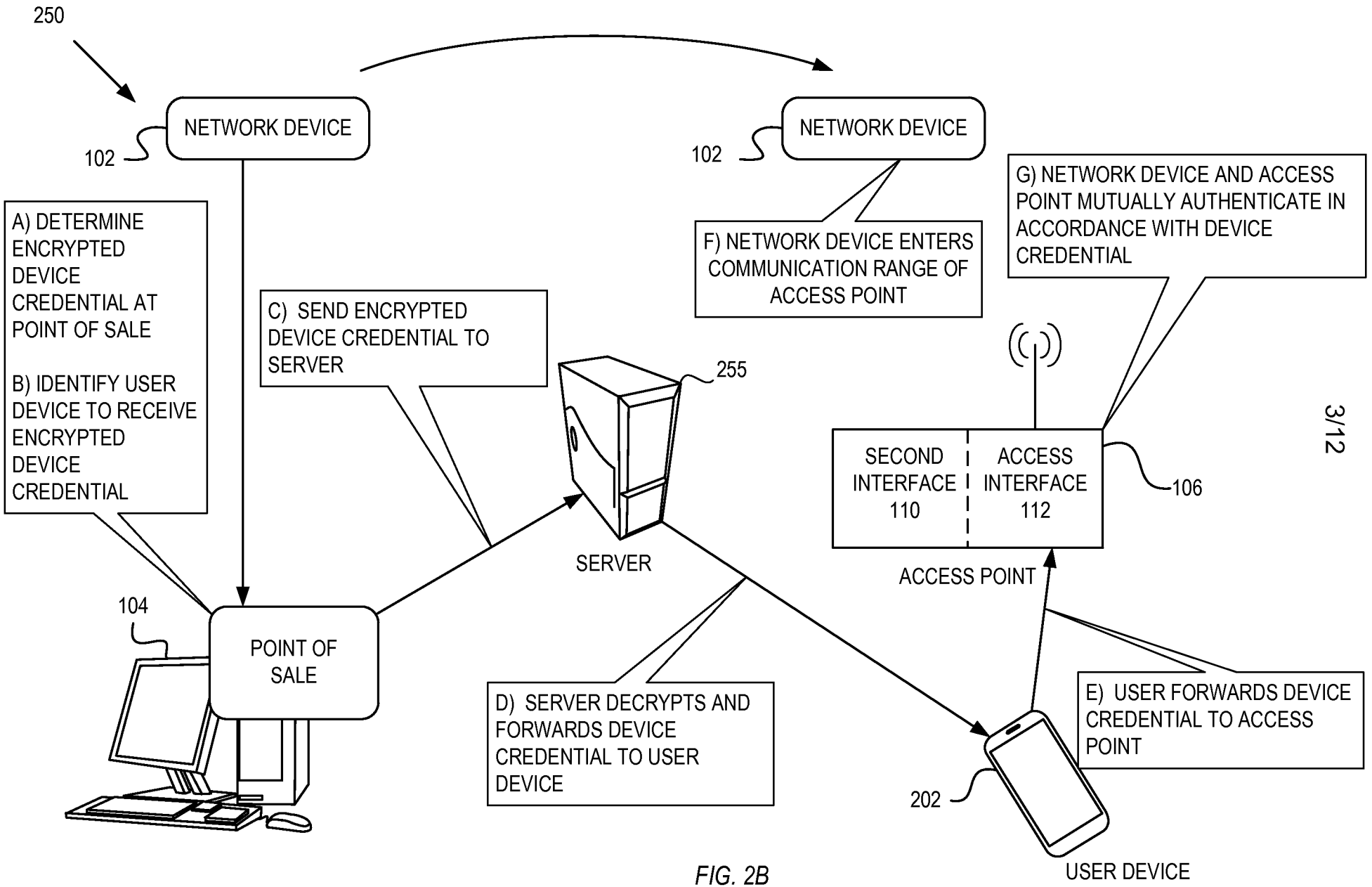
250
NETWORK DEVICE
102
NETWORK DEVICE
102
A) DETERMINE ENCRYPTED DEVICE CREDENTIAL AT POINT OF SALE
B) IDENTIFY USER DEVICE TO RECEIVE ENCRYPTED DEVICE CREDENTIAL
C) SEND ENCRYPTED DEVICE CREDENTIAL TO SERVER
F) NETWORK DEVICE ENTERS COMMUNICATION RANGE OF ACCESS POINT
G) NETWORK DEVICE AND ACCESS POINT MUTUALLY AUTHENTICATE IN ACCORDANCE WITH DEVICE CREDENTIAL
255
SERVER
SECOND INTERFACE 110
ACCESS INTERFACE 112
106
ACCESS POINT
104
POINT OF SALE
D) SERVER DECRYPTS AND FORWARDS DEVICE CREDENTIAL TO USER DEVICE
E) USER FORWARDS DEVICE CREDENTIAL TO ACCESS POINT
202
USER DEVICE

FIG. 2B

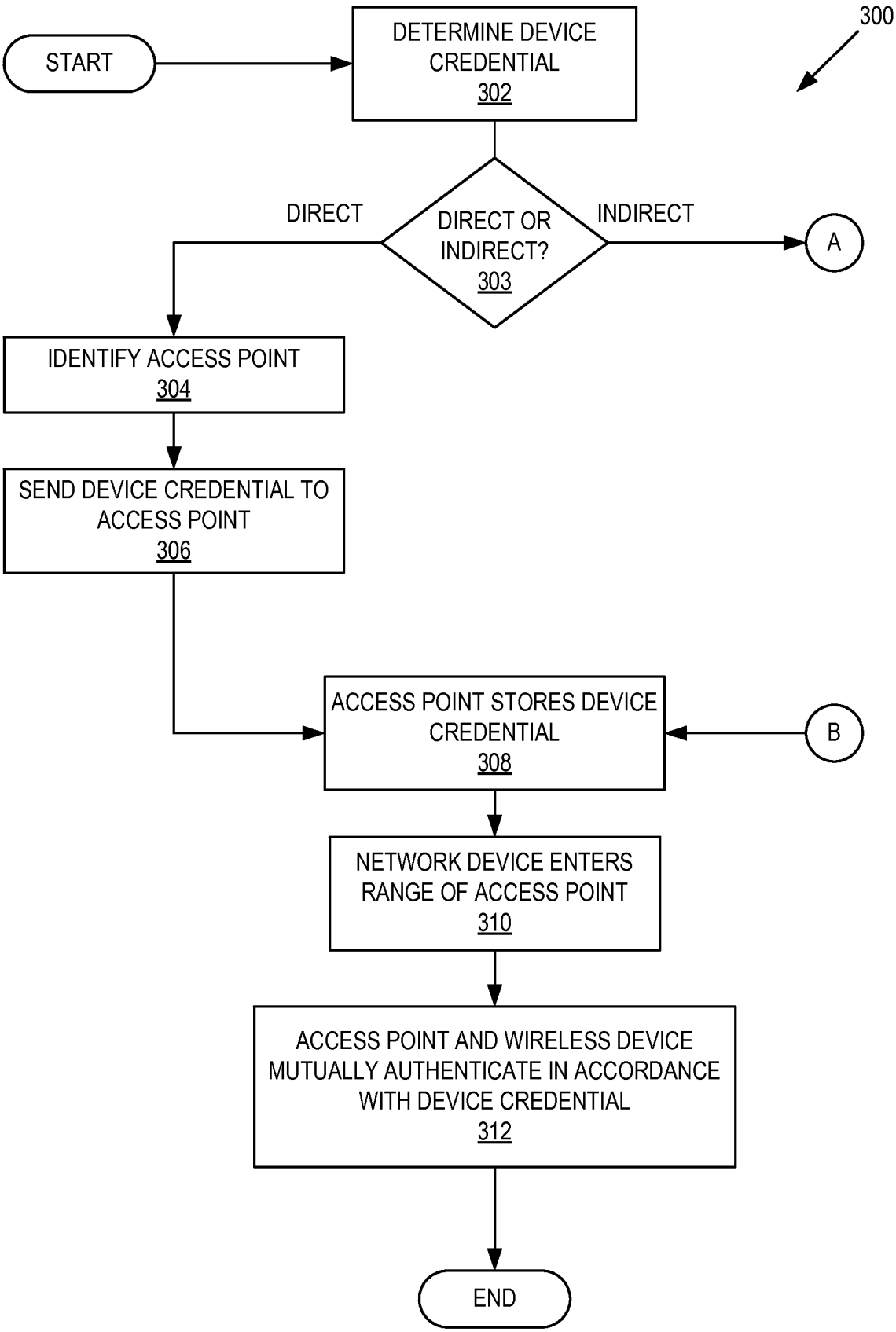
300
START
DETERMINE DEVICE CREDENTIAL
302
DIRECT OR INDIRECT?
303
DIRECT
INDIRECT
A
IDENTIFY ACCESS POINT
304
SEND DEVICE CREDENTIAL TO ACCESS POINT
306
ACCESS POINT STORES DEVICE CREDENTIAL
308
B
NETWORK DEVICE ENTERS RANGE OF ACCESS POINT
310
ACCESS POINT AND WIRELESS DEVICE MUTUALLY AUTHENTICATE IN ACCORDANCE WITH DEVICE CREDENTIAL
312
END

FIG. 3A

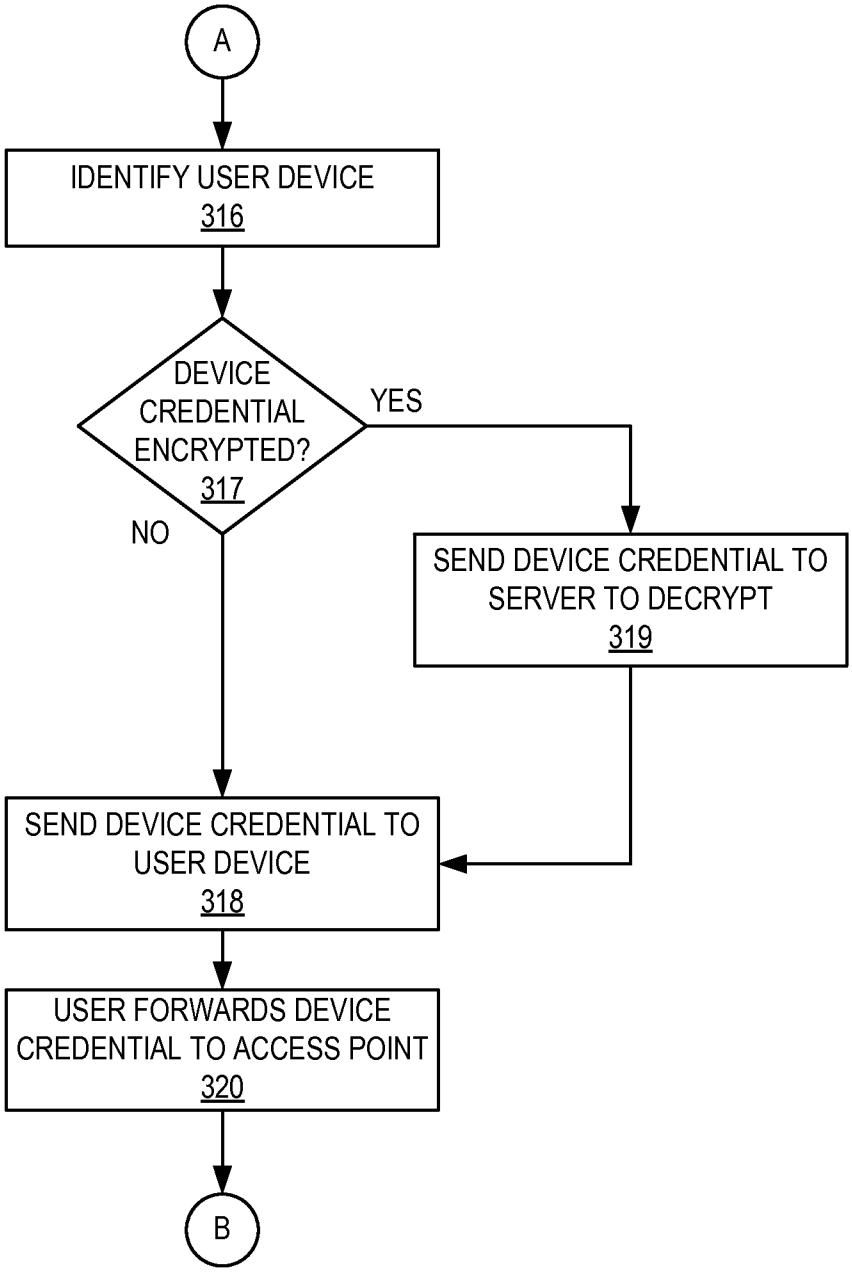
A
IDENTIFY USER DEVICE
316
DEVICE CREDENTIAL ENCRYPTED?
317
YES
NO
SEND DEVICE CREDENTIAL TO SERVER TO DECRYPT
319
SEND DEVICE CREDENTIAL TO USER DEVICE
318
USER FORWARDS DEVICE CREDENTIAL TO ACCESS POINT
320
B

FIG. 3B

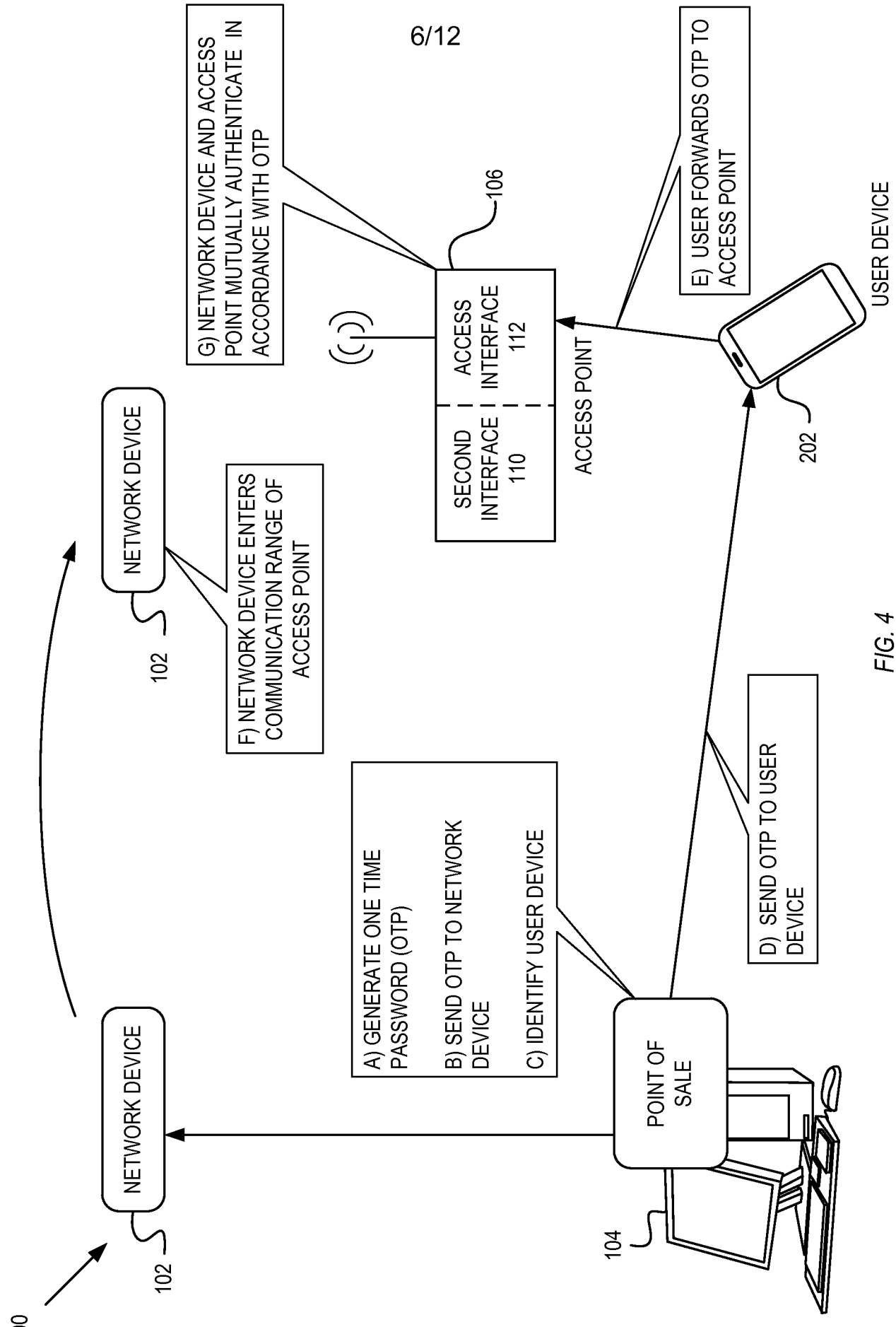
400
NETWORK DEVICE
102
NETWORK DEVICE
102
F) NETWORK DEVICE ENTERS COMMUNICATION RANGE OF ACCESS POINT
G) NETWORK DEVICE AND ACCESS POINT MUTUALLY AUTHENTICATE IN ACCORDANCE WITH OTP
106
ACCESS INTERFACE 112
SECOND INTERFACE 110
ACCESS POINT
E) USER FORWARDS OTP TO ACCESS POINT
USER DEVICE
202
A) GENERATE ONE TIME PASSWORD (OTP)
B) SEND OTP TO NETWORK DEVICE
C) IDENTIFY USER DEVICE
D) SEND OTP TO USER DEVICE
POINT OF SALE
104

FIG. 4

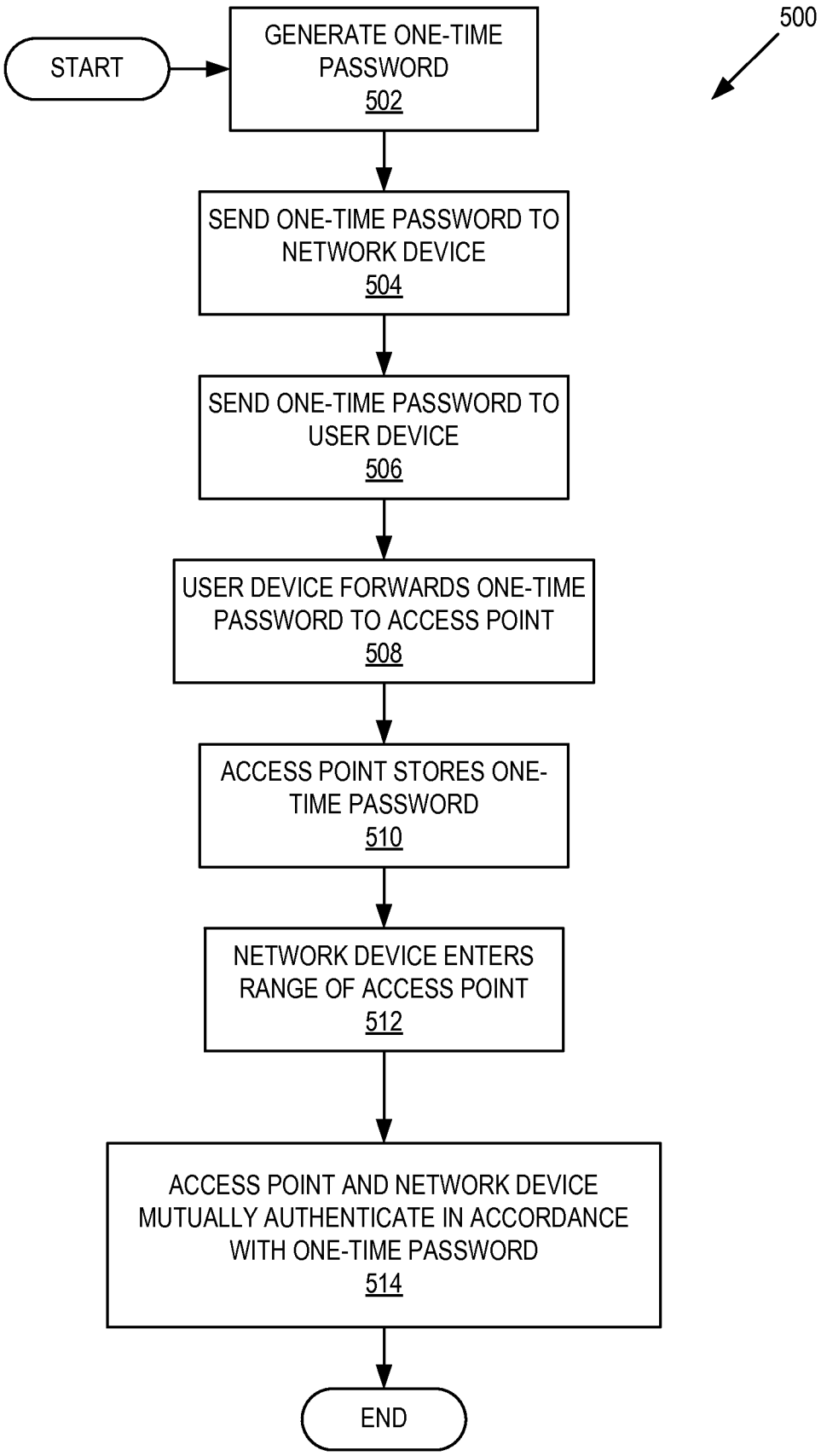
500
START
GENERATE ONE-TIME PASSWORD
502
SEND ONE-TIME PASSWORD TO NETWORK DEVICE
504
SEND ONE-TIME PASSWORD TO USER DEVICE
506
USER DEVICE FORWARDS ONE-TIME PASSWORD TO ACCESS POINT
508
ACCESS POINT STORES ONE-TIME PASSWORD
510
NETWORK DEVICE ENTERS RANGE OF ACCESS POINT
512
ACCESS POINT AND NETWORK DEVICE MUTUALLY AUTHENTICATE IN ACCORDANCE WITH ONE-TIME PASSWORD
514
END

FIG. 5

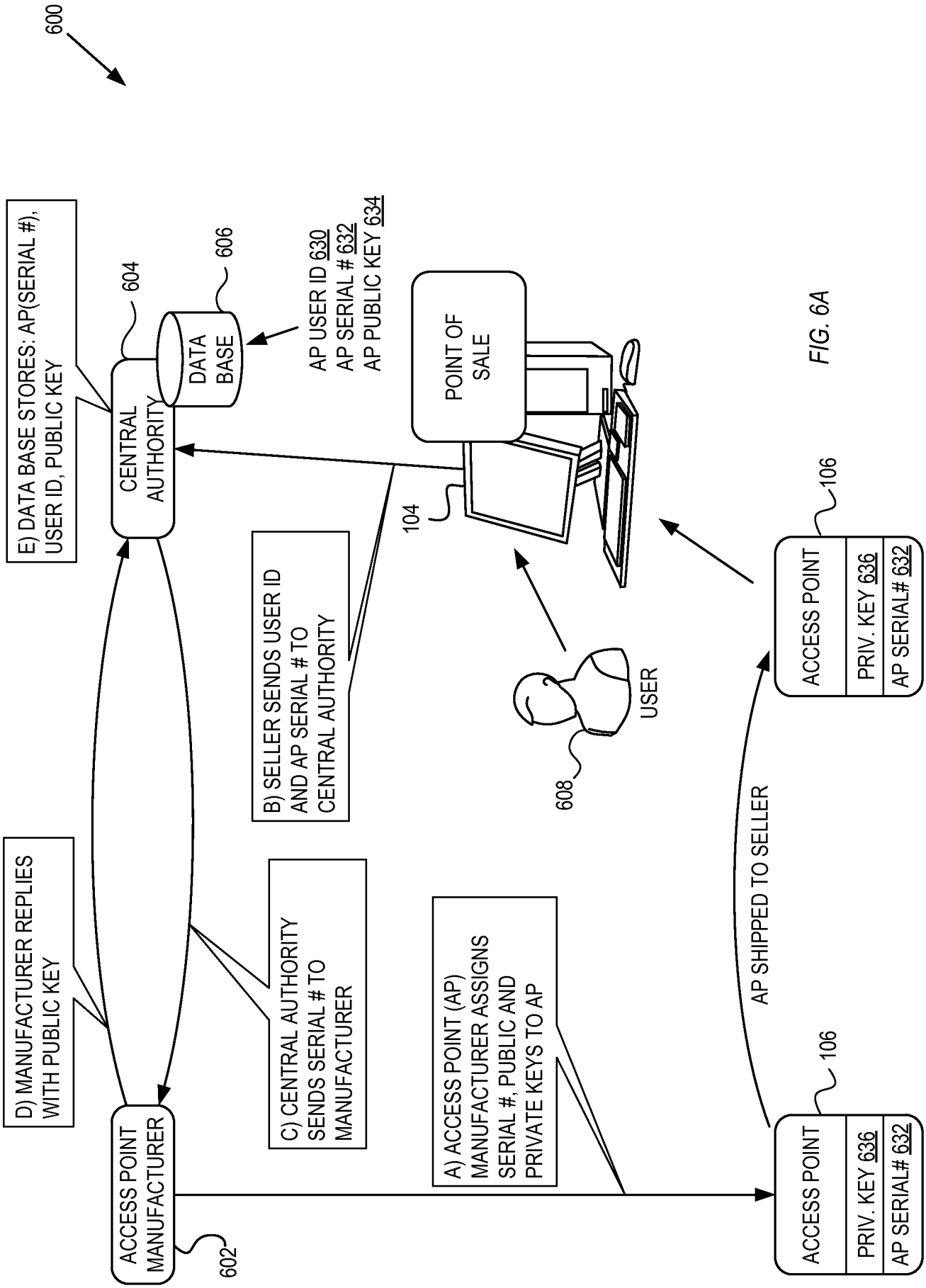
600
E) DATA BASE STORES: AP(SERIAL #), USER ID, PUBLIC KEY
604
606
DATA BASE
AP USER ID 630
AP SERIAL # 632
AP PUBLIC KEY 634
CENTRAL AUTHORITY
POINT OF SALE
104
B) SELLER SENDS USER ID AND AP SERIAL # TO CENTRAL AUTHORITY
608
USER
106
ACCESS POINT
PRIV. KEY 636
AP SERIAL# 632
D) MANUFACTURER REPLIES WITH PUBLIC KEY
C) CENTRAL AUTHORITY SENDS SERIAL # TO MANUFACTURER
A) ACCESS POINT (AP) MANUFACTURER ASSIGNS SERIAL #, PUBLIC AND PRIVATE KEYS TO AP
AP SHIPPED TO SELLER
ACCESS POINT MANUFACTURER
602

FIG. 6A

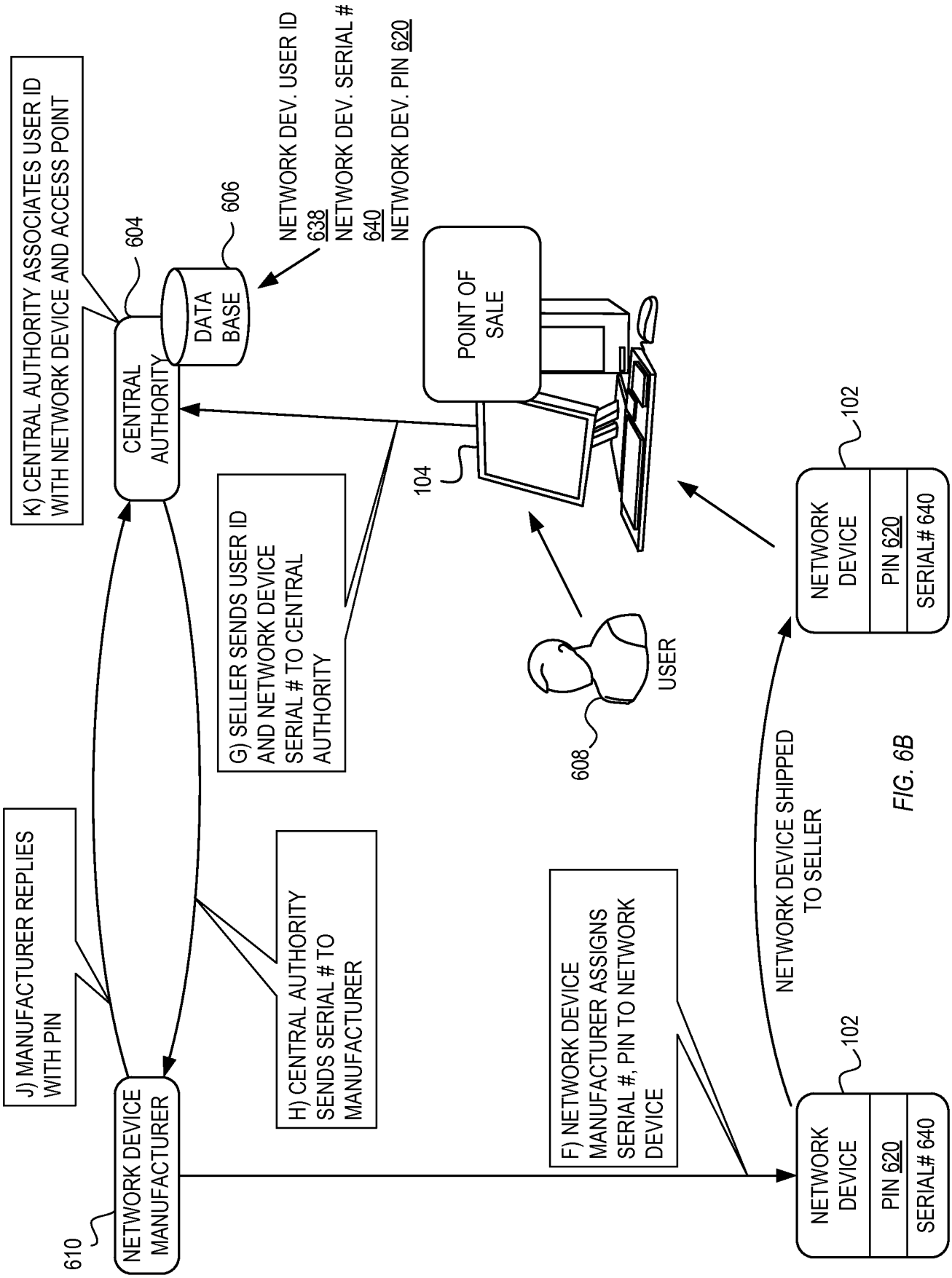
K) CENTRAL AUTHORITY ASSOCIATES USER ID WITH NETWORK DEVICE AND ACCESS POINT
604
606
DATA BASE
NETWORK DEV. USER ID 638
NETWORK DEV. SERIAL # 640
NETWORK DEV. PIN 620
CENTRAL AUTHORITY
POINT OF SALE
102
104
G) SELLER SENDS USER ID AND NETWORK DEVICE SERIAL # TO CENTRAL AUTHORITY
NETWORK DEVICE
PIN 620
SERIAL# 640
USER
608
J) MANUFACTURER REPLIES WITH PIN
H) CENTRAL AUTHORITY SENDS SERIAL # TO MANUFACTURER
F) NETWORK DEVICE MANUFACTURER ASSIGNS SERIAL #, PIN TO NETWORK DEVICE
NETWORK DEVICE SHIPPED TO SELLER
NETWORK DEVICE MANUFACTURER
610
NETWORK DEVICE
PIN 620
SERIAL# 640
102

FIG. 6B

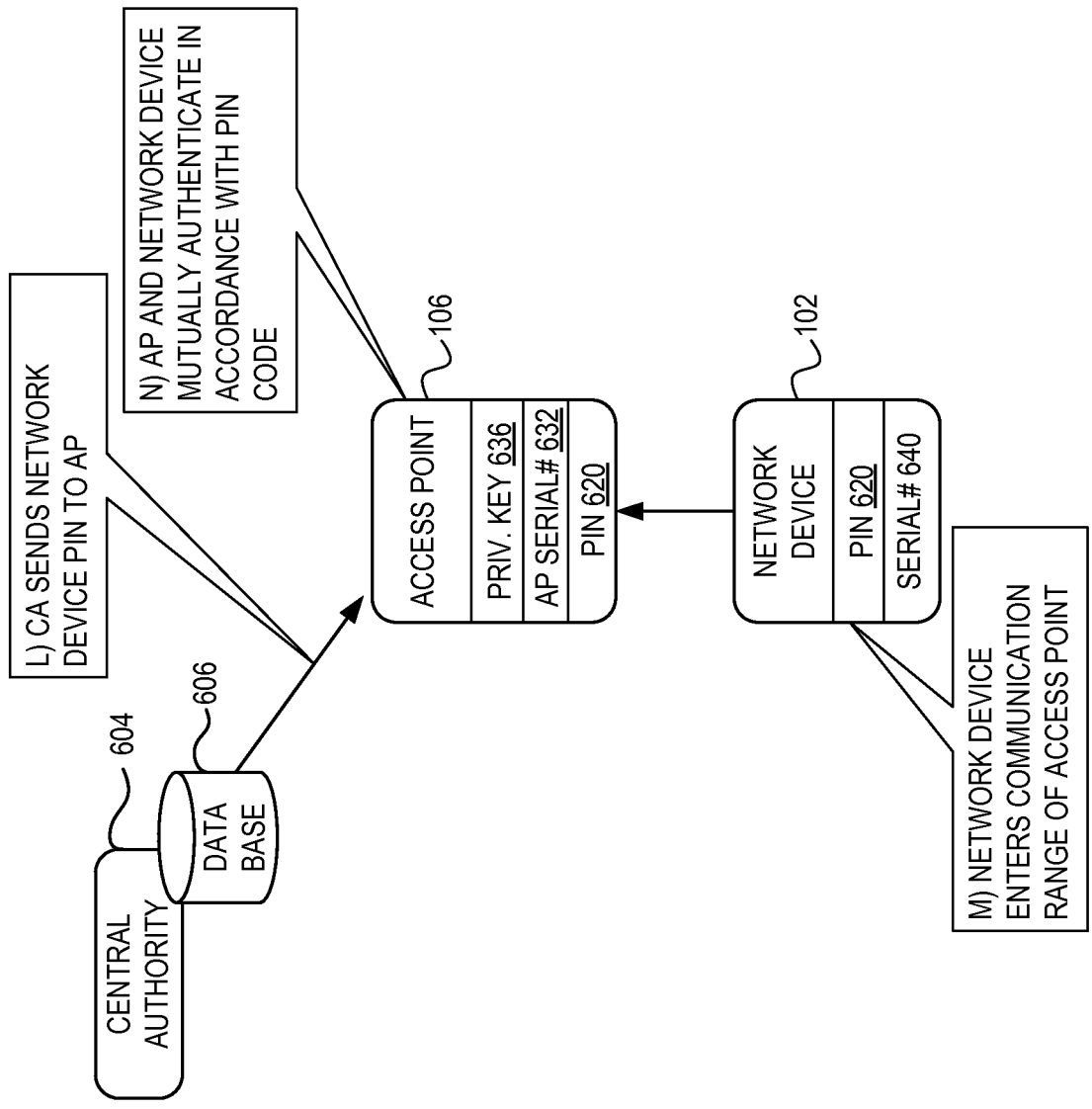
CENTRAL AUTHORITY
604
DATA BASE
606
L) CA SENDS NETWORK DEVICE PIN TO AP
N) AP AND NETWORK DEVICE MUTUALLY AUTHENTICATE IN ACCORDANCE WITH PIN CODE
ACCESS POINT
PRIV. KEY 636
AP SERIAL# 632
PIN 620
106
NETWORK DEVICE
PIN 620
SERIAL# 640
102
M) NETWORK DEVICE ENTERS COMMUNICATION RANGE OF ACCESS POINT

FIG. 6C

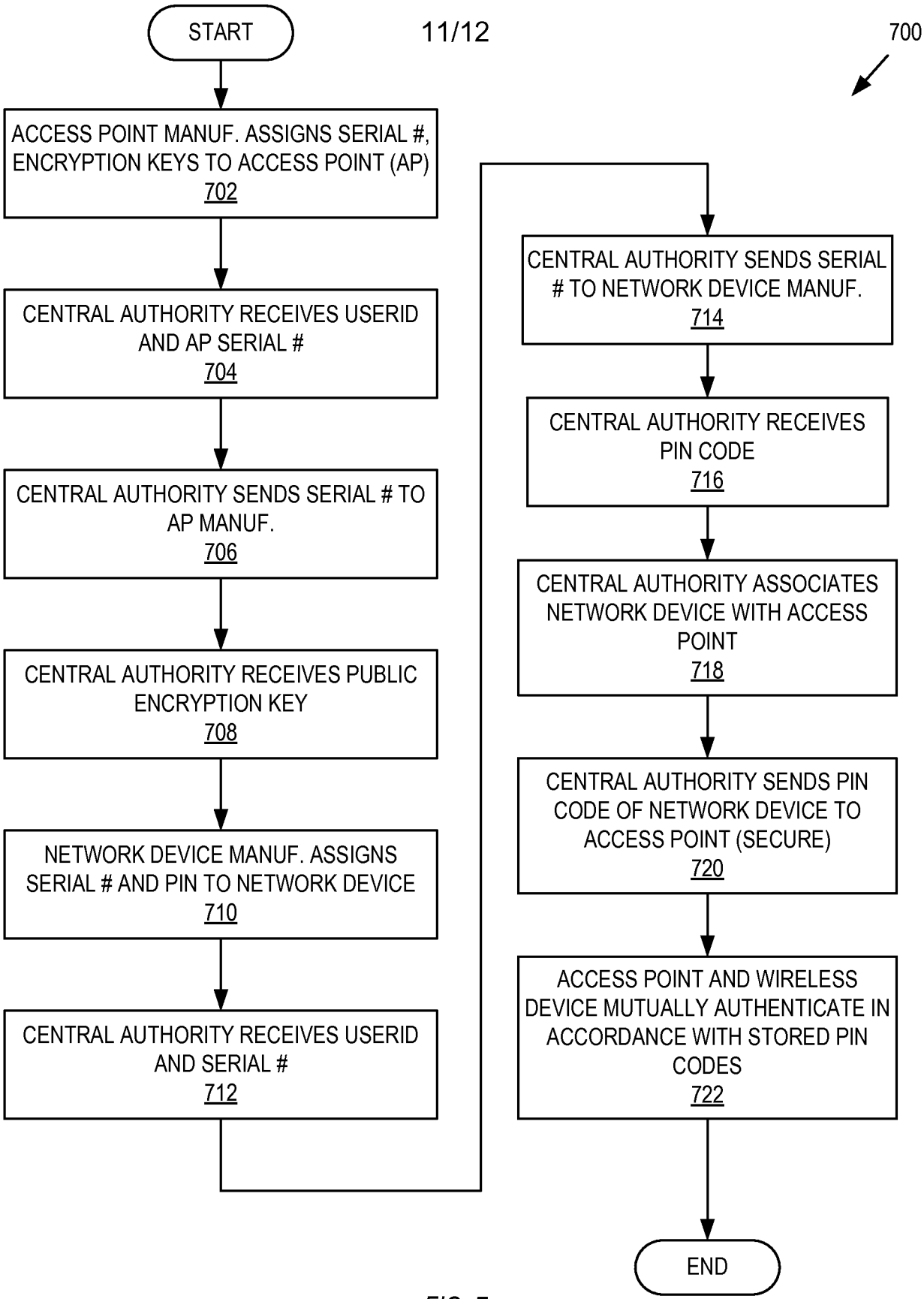
700
START
ACCESS POINT MANUF. ASSIGNS SERIAL #, ENCRYPTION KEYS TO ACCESS POINT (AP)
702
CENTRAL AUTHORITY RECEIVES USERID AND AP SERIAL #
704
CENTRAL AUTHORITY SENDS SERIAL # TO AP MANUF.
706
CENTRAL AUTHORITY RECEIVES PUBLIC ENCRYPTION KEY
708
NETWORK DEVICE MANUF. ASSIGNS SERIAL # AND PIN TO NETWORK DEVICE
710
CENTRAL AUTHORITY RECEIVES USERID AND SERIAL #
712
CENTRAL AUTHORITY SENDS SERIAL # TO NETWORK DEVICE MANUF.
714
CENTRAL AUTHORITY RECEIVES PIN CODE
716
CENTRAL AUTHORITY ASSOCIATES NETWORK DEVICE WITH ACCESS POINT
718
CENTRAL AUTHORITY SENDS PIN CODE OF NETWORK DEVICE TO ACCESS POINT (SECURE)
720
ACCESS POINT AND WIRELESS DEVICE MUTUALLY AUTHENTICATE IN ACCORDANCE WITH STORED PIN CODES
722
END

FIG. 7

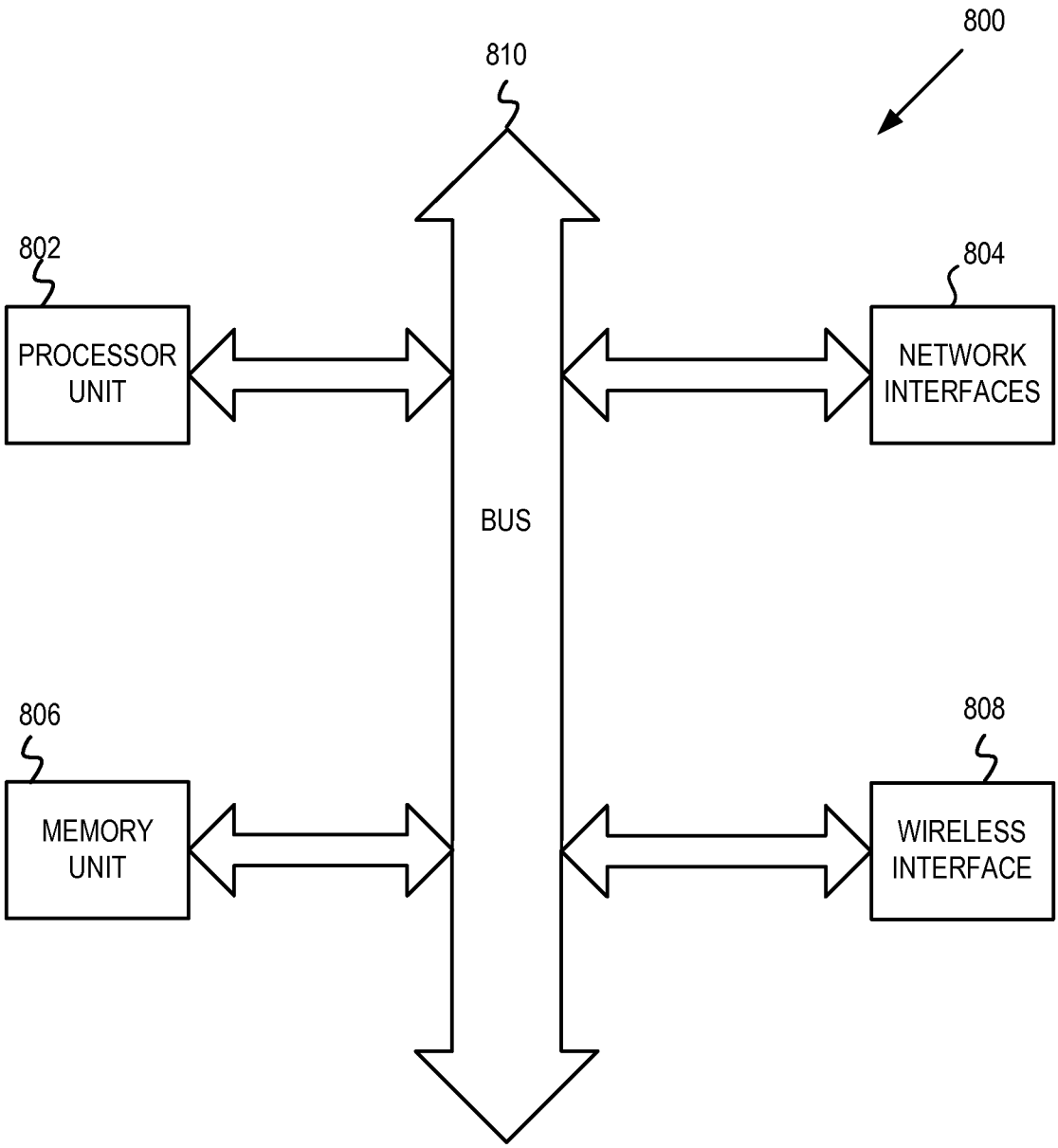
800
810
802
PROCESSOR UNIT
804
NETWORK INTERFACES
BUS
806
MEMORY UNIT
808
WIRELESS INTERFACE

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/026625

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04W12/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/284785 A1 (SALKINTZIS APOSTOLIS K [GR] ET AL) 8 November 2012 (2012-11-08) paragraphs [0031] - [0044]	1-54
X	WO 2010/028681 A1 (ERICSSON TELEFON AB L M [SE]; LINDHOLM FREDRIK [SE]; ROOS PER [SE]) 18 March 2010 (2010-03-18) page 4, lines 2-14	1-54

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 June 2014	26/06/2014

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Veen, Gerardus

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2014/026625

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012284785 A1	08-11-2012	NONE	
WO 2010028681 A1	18-03-2010	CN 102150446 A	10-08-2011
		EP 2347613 A1	27-07-2011
		US 2011191842 A1	04-08-2011
		WO 2010028681 A1	18-03-2010