

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
2 April 2009 (02.04.2009)

PCT

(10) International Publication Number  
**WO 2009/043048 A1**

(51) International Patent Classification:  
*H04Q 7/20* (2006.01)

(74) Agents: **KLOKE, Daniel, C.** et al.; Sheppard, Mullin, Richter & Hampton LLP, 990 Marsh Road, Menlo Park, CA 94025 (US).

(21) International Application Number:  
PCT/US2008/078191

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

(22) International Filing Date:  
29 September 2008 (29.09.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
60/976,344 28 September 2007 (28.09.2007) US

(71) Applicant (for all designated States except US): **DEVICESCPE SOFTWARE, INC.** [US/US]; 900 Cherry Avenue, 6th Floor, San Bruno, CA 94066 (US).

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

(72) Inventors; and

(75) Inventors/Applicants (for US only): **WYNN, Simon** [GB/US]; C/o Devicescape Software, Inc., 900 Cherry Avenue, 6th Floor, San Bruno, CA 94066 (US). **FRASER, David** [US/US]; C/o Devicescape Software, Inc., 900 Cherry Avenue, 6th Floor, San Bruno, CA 94066 (US).

Published:  
— with international search report

(54) Title: SYSTEMS AND METHODS FOR WIRELESS NETWORK SELECTION

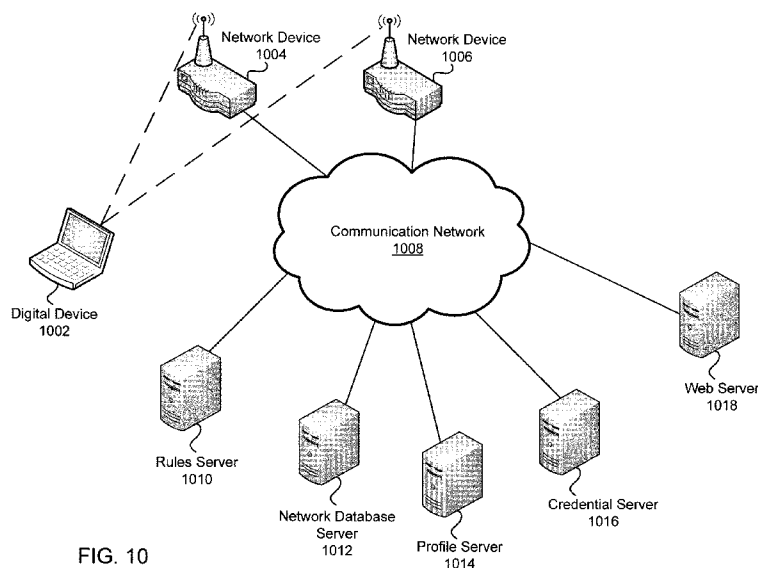


FIG. 10

(57) Abstract: Systems and methods for selecting a wireless network are disclosed. In some embodiments, a method comprises receiving a first network device identifier for a first network device and a second network device identifier for a second network device, obtaining a first network profile comprising a first attribute, the first network profile based on the first network device identifier, obtaining a second network profile comprising a second attribute, the second network profile based on the second network device identifier, and selecting either the first network device identifier or the second network device identifier based on an attribute analysis of the first attribute and the second attribute.

WO 2009/043048 A1

**SYSTEMS AND METHODS FOR WIRELESS NETWORK SELECTION**

By: Simon Wynn and David Fraser

**CROSS-REFERENCE TO RELATED APPLICATION**

**[001]** The present application claims benefit of U.S. Provisional Patent Application No. 60/976,344 filed September 28, 2007, and entitled "Systems and Methods for Opportunistic Access to Free and Open Wireless Networks" which is incorporated herein by reference.

**[002]** The present application is also a continuation-in-part of U.S. Nonprovisional Patent Application No. 11/899,739, filed September 6, 2007, entitled "Systems and Methods for Providing Network Credentials" which claims benefit of U.S. Provisional Patent Application No. 60/824,756 filed Sep. 6, 2006, and entitled "Network Credential Discovery Using DNS," which are hereby incorporated by reference. The present application is also related to co-pending U.S. patent application Ser. No. 11/899,697, entitled "System and Method for Acquiring Network Credentials," filed Sep. 6, 2007, and co-pending U.S. patent application Ser. No. 11/899,638, entitled "Systems and Methods for Obtaining Network Access," filed Sep. 6, 2007, both of which are incorporated by reference.

**BACKGROUND****1. Field of the Invention**

**[003]** The present invention generally relates to accessing communication networks. More particularly, the invention relates to the selection of one or more wireless communication networks.

**2. Description of Related Art**

**[004]** The increasing use of the networks to access information has resulted in a greater dependence on network communication for a variety of activities. With this dependence comes the growing expectation that network access will be ubiquitous. Network access for mobile users has been particularly enhanced by improvements in wireless technology. Various cellular (e.g. GSM, CDMA and the like), Wi-Fi (i.e. IEEE 802.11), WiMAX (i.e. IEEE 802.16), and other technologies have enabled a wide range of access options for a

potential network user. Many wireless access points or "hotspots" are accessible only with local geographic regions--in some cases as small as a specific business or other address. In addition, strategically placed hotspots may provide public or private network access for a diverse group of people.

**[005]** The owners or managers of hotspots often require password and the like to enable user access. As a result, a user of multiple hotspots may have to store, remember, or otherwise manage a large number of passwords. Many users may store their passwords on a laptop computer they use to access the hotspot. However, not all devices capable of accessing hotspots are laptop computers; cellular phones, personal digital assistants (PDAs), and many other devices are now capable of wireless access. Unfortunately, users often cannot easily enter the password on the device or store the password within the device. For example, some devices capable of wireless access may not have a keyboard. Even when a device includes a keyboard, the keyboard is often small and may be of limited functionality, especially for users with limited finger dexterity.

**[006]** When users store passwords on a laptop computer, the user must first access the laptop computer and store the correct password within the computer. When a password changes, the user is required to update the password within the computer. Additionally, having the username and password stored in the device presents a security problem should the device be lost or stolen.

**[007]** Further, users are typically required to enter a password, username, and navigate a website to obtain network access. This process is time consuming and the user may enter the wrong information and be forced to re-enter data.

**[008]** When users enter a password manually, they are less apt to remember difficult passwords. As a result, simple password access is susceptible to hacking and may compromise the user's network access, the hotspot, and/or the user's personal information. Moreover, the user's network access may be stolen if the user's simple password is hacked or simply guessed.

**[009]** Connecting to wireless networks has traditionally been a complex process for users of wireless devices for other reasons. Typically, the user enters an area where two or more Wi-Fi networks are present, selects the Wi-Fi function on their laptop, and views a series of 'scan results' listing the available Wi-Fi networks. In one example, the listing of

available Wi-Fi networks comprises a list of Wi-Fi network SSID identifiers. Users must often identify which Wi-Fi networks do not have encryption or other security mechanisms (e.g., a login page). To add to user frustration, some of the wireless networks may be functional while others may be misconfigured in such a way that renders the network unuseable.

**[0010]** The user typically makes an arbitrary decision which Wi-Fi network to connect to based on the listing. In making a decision of which Wi-Fi network to connect, the user typically does not know whether the selected Wi-Fi network will provide adequate quality of service or even if the network will be able to provide an IP address via Dynamic Host Configuration Protocol (DHCP).

### SUMMARY OF THE INVENTION

**[0011]** Exemplary methods and systems for providing network credentials for network access are described. The exemplary method comprises receiving a credential request from a digital device over a network device, identifying a network record based on at least some information within the credential request, retrieving a network credential from a plurality of network credentials based on the network record, and transmitting a credential request response containing the network credential from the plurality of network credentials to the digital device.

**[0012]** The method may further comprise decrypting the credential request, authenticating the credential request, and encrypting the credential request response. Further, the method may also comprise retrieving an encryption key based on the digital device. The credential request may be received over a standard protocol of the network device. The standard protocol may be DNS.

**[0013]** The credential request may comprise a location identifier. The method may further comprise receiving a confirmed access response from the digital device.

**[0014]** An exemplary system for providing network credentials may comprise a credential request module and a credential request response module. The credential request module may be configured to receive a credential request from a digital device over a network device. The credential request response module may be configured to identify a network record based on at least some information within the credential request, retrieve a network credential from a plurality of network credentials based on the network record, and transmit a credential request response containing the network to the digital device.

**[0015]** An exemplary computer readable medium may have embodied thereon a program. The program may be executable by a processor for performing a method for providing network credentials. The method may comprise receiving a credential request from a digital device over a network device, identifying a network record based on at least some information within the credential request, retrieving a network credential from a plurality of network credentials based on the network record, and transmitting a credential request response containing the network credential from the plurality of network credentials to the digital device.

**[0016]** Systems and methods for selecting a wireless network are disclosed. In some embodiments, a method comprises receiving a first network device identifier for a first network device and a second network device identifier for a second network device, obtaining a first network profile comprising a first attribute, the first network profile based on the first network device identifier, obtaining a second network profile comprising a second attribute, the second network profile based on the second network device identifier, and selecting either the first network device identifier or the second network device identifier based on an attribute analysis of the first attribute and the second attribute.

**[0017]** In various embodiments, the first network device identifier and the second network device identifier are received from a digital device by a server. The method may further comprise providing a wireless network selection based on the selection. The method may also further comprise providing a credential request response based on the selection.

**[0018]** In some embodiments, the network selection identifier comprises the first network device identifier. The network selection identifier may also comprise a sorted list including the first network device identifier and the second network device identifier wherein the list is sorted based on the attribute analysis of the first attribute and the second attribute. An attribute may comprise a performance metric, a shared indicator, and a service identifier.

**[0019]** The method may further comprise comparing the first attribute and the second attribute to minimum requirements wherein selecting either the first network identifier or the second network device identifier is also based, at least in part, on the comparison of the attributes to the minimum requirements. The method may also further comprise comparing the first attribute and the second attribute to personalized settings wherein selecting either the first network identifier or the second network device identifier is also based, at least in part, on the comparison of the attributes to personalized settings. The method may also further comprise receiving a user identifier and retrieving the personalized settings from a user account based on the user identifier.

**[0020]** In various embodiments, a system comprises a digital device and a server. The digital device may be coupled to a communication network and configured to transmit a first network device identifier for a first network device and a second network device identifier for a second network device over the communication network. The server may also be coupled to the communication network and configured to receive the first network device identifier and the second network device identifier from the digital device, to obtain a first network

profile comprising a first attribute, the first network profile based on the first network device identifier, to obtain a second network profile comprising a second attribute, the second network profile based on the second network device identifier, and to select either the first network device identifier or the second network device identifier based on an attribute analysis of the first attribute and the second attribute.

**[0021]** A computer readable storage medium may be configured to store instructions, the instructions comprising a method, the method comprising the steps of receiving a first network device identifier for a first network device and a second network device identifier for a second network device, obtaining a first network profile comprising a first attribute, the first network profile based on the first network device identifier, obtaining a second network profile comprising a second attribute, the second network profile based on the second network device identifier, and selecting either the first network device identifier or the second network device identifier based on an attribute analysis of the first attribute and the second attribute.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022] FIG. 1 is a diagram of an environment in which embodiments of the present invention may be practiced.

[0023] FIG. 2 is a block diagram of an exemplary credential server.

[0024] FIG. 3 is a flow diagram of an exemplary process for providing network access to the digital device.

[0025] FIG. 4 is a block diagram of an exemplary credential request.

[0026] FIG. 5 is a block diagram of an exemplary credential request response.

[0027] FIG. 6 is a flow diagram of the exemplary method for providing network credentials.

[0028] FIG. 7 is another flow diagram of the exemplary method for providing network credentials.

[0029] FIG. 8 is a flow diagram of an exemplary method for receiving and storing network credentials.

[0030] FIG. 9 is a block diagram of an exemplary credential server.

[0031] FIG. 10 is a diagram of another environment in which embodiments of the present invention may be practiced.

[0032] FIG. 11 is a flow diagram of an exemplary process for providing a selection of a wireless network.

[0033] FIG. 12 is a flow diagram of an exemplary process for selecting a wireless network.

[0034] FIG. 13 is a diagram for selecting a wireless network and accessing the selected wireless network.



### DETAILED DESCRIPTION OF THE INVENTION

**[0035]** Embodiments of the present invention provide systems and methods for providing network credentials. In exemplary embodiments, a credential server receives a request for network credentials from a digital device at a hotspot. The request may be formatted as a standard protocol which is relayed from the hotspot to the credential server. The credential server may identify a network record based on at least some information contained within the request and transmit network credentials associated with the network record to the digital device. The digital device may receive the network credentials and provide them to network device in order to obtain network access.

**[0036]** In various embodiments, a rules server may identify a preferred network from a plurality of available networks that the digital device may connect based on a variety of network attributes. In one example, a digital device may scan a physical region for available networks and generate a list of available wireless networks. The list may be provided to a rules server which identifies and retrieves a network profile for each wireless network on the list. The rules server may then compare each network profile (e.g., via attributes contained within each profile) to select a preferred network from the list. The rules server may then transmit the wireless network selection to the digital device which may then access the network.

**[0037]** In some embodiments, the digital device accesses the selected wireless network using credentials provided by the credential server. In one example, when the rules server selects the preferred wireless network, the rules server (or another server in communication with the rules server) may simultaneously (or nearly simultaneously) provide a credential request response including network credentials associated with the selected wireless network.

**[0038]** FIG. 1 illustrates a diagram of an environment 100 in which embodiments of the present invention may be practiced. In exemplary embodiments, a user with a digital device 102 enters a hotspot. The digital device 102 may automatically transmit a credential request as a standard protocol over a network device 104. The credential request may be forwarded to a credential server 116 which, based on the information contained within the credential request, transmits a credential request response back to the digital device 102. The credential request response contains network credentials which the digital device 102 may provide to the network device 104, the authentication server 108, or the access controller 112 to obtain access to the communication network 114.

**[0039]** In various embodiments, a hotspot comprises the network device 104, the authentication server 108, the DNS server 110, and the access controller 112 which are coupled to the local area network 106 (e.g., a "walled garden"). The network device 104 may comprise an access point which allows the digital device 102 to communicate with the authentication server 108, the DNS server 110, and the access controller 112 over the local area network 106. The digital device 102 may comprise a laptop, mobile phone, camera, personal digital assistant, or any other computing device. The authentication server 108 is a server that requires network credentials from the digital device 102 before allowing the digital device 102 access the communication network 114. The DNS server 110 provides DNS services over the local area network 106 and may relay requests to other DNS servers (not shown) across the communication network 114. The access controller 112 is an access device such as a router or bridge that can allow communication between devices operationally coupled to the network device 104 with devices coupled to the communication network 114.

**[0040]** Although the hotspot in FIG. 1 depicts separate servers coupled to the local area network 106, those skilled in the art will appreciate that there may be any number of devices (e.g., servers, digital devices, access controllers, and network devices) coupled to the local area network 106. In some embodiments, the local area network 106 is optional. In one example, the authentication server 108, the DNS server 110, and the access controller 112 are coupled directly to the network device 104. In various embodiments, the authentication server 108, the DNS server 110, and the access controller 112 may be combined within one or more servers or one or more digital devices. Further, although FIG. 1 depicts wireless access, the digital device 102 may be coupled to the network device 104 wirelessly or over wires (e.g., such as 10baseT).

**[0041]** In order to access the communication network 114, the authentication server 108 may require the digital device 102 to provide one or more network credentials for access to the hotspot. The network credential may comprise, for example, a username and password for an account associated with the hotspot. In alternative embodiments, network credentials other than a user name and password may be utilized.

**[0042]** According to exemplary embodiments, the digital device 102 may dynamically acquire the network credentials from the credential server 116. The digital device 102 may send a credential request comprising an identity of the digital device 102 (or the user of the

digital device 102) and details about the network device 104 (e.g., name of the network device 104 or Wi-Fi service provider) to the credential server 116.

**[0043]** In one example, when the digital device 102 enters the hotspot, the network device 104 may provide an IP address to which DNS queries may be submitted, for example, via DHCP (Dynamic Host Configuration Protocol). The credential request may be formatted as a standard protocol. In an example, the credential request may be formatted as a DNS request. The credential request may be a text record request (e.g., TXT), which comprises a standard record type such that the network infrastructure (e.g., the access controller 112) will not block the request. More details regarding the process for acquiring network credentials are provided in co-pending U.S. patent application Ser. No. 11/899,697, entitled "System and Method for Acquiring Network Credentials," filed Sep. 6, 2007, and incorporated by reference herein.

**[0044]** In some embodiments, the credential request is received by the DNS server 110 which may forward the credential request to the credential server 116 for the network credential. In exemplary embodiments, the credential server 116 may perform a lookup to determine the proper network credential(s) to send back to the DNS server 110 which forwards the network credential back to the requesting digital device 102. In various embodiments, the proper network credential(s) are sent from the credential server 116 to the digital device 102 over the same path as the transmission of the credential request.

**[0045]** Although only one DNS server 110 is depicted within FIG. 1, the credential request may be forwarded through any number of servers, including but not limited to DNS servers, prior to being received by the credential server 116. In other embodiments, the credential request is forwarded directly from the network device 104 to the credential server 116.

**[0046]** In some embodiments, a credential request response from the credential server 116 may comprise the username, password, and/or login procedure information. The login procedural information may comprise, for example, HTML form element names, a submission URL, or a submission protocol. In some embodiments, the network credential response may be encrypted by the credential server 116 using an encryption key associated with the digital device 102 prior to transmission back to the digital device 102.

**[0047]** Once the digital device 102 receives the network credential response, the digital device 102 may submit the network credential (retrieved from the network credential response) to the network device 104 in an authentication response. In exemplary embodiments, the authentication response may be forwarded to an authentication server 108 for verification. In some embodiments, the authentication server 108 may comprise an AAA server or RADIUS server. More details regarding the process for obtaining network access are provided in co-pending U.S. patent application Ser. No. 11/899,638, entitled "System and Method for Obtaining Network Access," filed Sep. 6, 2007, and incorporated by reference herein.

**[0048]** It should be noted that FIG. 1 is exemplary. Alternative embodiments may comprise more, less, or functionally equivalent components and still be within the scope of present embodiments. For example, as previously discussed, the functions of the various servers (e.g., DNS server 110, credential server 116, and authentication server 108) may be combined into one or two servers. That is, for example, the authentication server 108 and the DNS server 110 may comprise the same server, or the functionality of the authentication server 108, the DNS server 110, and the access controller 112 may be combined into a single device.

**[0049]** FIG. 2 is a block diagram of an exemplary credential server 116. The credential server 116 comprises an authentication module 200, a network module 202, a credential request module 204, a credential request response module 206, an encryption/decryption module 208, a network record storage 210, and an encryption key storage 212. A module may comprise, individually or in combination, software, hardware, firmware, or circuitry.

**[0050]** The authentication module 200 may be configured to authenticate the credential request and provide security to the credential request response. In various embodiments, the digital device 102 may encrypt or digitally sign the credential request using an encryption key (e.g., a shared encryption key or an encryption key that is a part of a key pair). The authentication module 200 may authenticate the credential request by decrypting the credential request with the proper encryption key retrieved from the encryption key storage 212. In one example, the digital device 102 generates a hash of the credential request and stores the hash within an encrypted portion of the credential request. The authentication module 200 may decrypt the credential request, generate hash of the credential request

response, and compare the generated hash to the hash contained within the credential request for authentication.

**[0051]** In other embodiments, the digital device 102 may generate a nonce (i.e., a random value) and store the nonce within a portion of the credential request that is digitally signed. The authentication module 200 may decrypt the digital signature to authenticate the credential request and retrieve the nonce. In various embodiments, when the credential request response module 206 generates the credential request response (described hereafter), the authentication module 200 may include the nonce within the credential request response. The authentication module 200 or the encryption/decryption module 208 may then encrypt the credential request response. When the digital device 102 decrypts the credential request response, the digital device 102 may retrieve the nonce from the credential request response and compare the nonce to the nonce that was transmitted within the credential request for further authentication.

**[0052]** The network module 202 may be configured to receive the credential request and transmit the credential request response over the communication network 114.

**[0053]** The credential request module 204 may receive the credential request from the network module 202. The credential request may be a standard protocol. In one example, the credential request is a UDP protocol (e.g., DNS).

**[0054]** In exemplary embodiments, the credential request module 204 may retrieve the DDID and the SSID from the credential request. The DDID may identify the digital device 102, the user of the digital device 102, and/or the user associated with a network record. The SSID may identify the hotspot or the service provider (i.e., operator) of the hotspot.

**[0055]** The credential request module 204 or the credential request response module 206 may identify a network record based on the DDID and the SSID. A network record is a record associated (either directly or indirectly (e.g., a relational database)) with the DDID and the SSID. In one example, a network record contains network credentials necessary to provide network access to a digital device 102 associated with the DDID at the hotspot associated with the SSID. Network records may be stored within the network record storage 210.

**[0056]** The credential request response module 206 may generate the credential request response. In various embodiments, the credential request response module 206 receives the

network credential associated with the DDID and SSID from the network record. In some embodiments, the network credential may comprise a credit card number. In one example, the digital device 102 receives the network credential, retrieves the credit card number, and provides the credit card number to the authentication server 108. In some examples, the authentication server 108 may then charge a fee to a credit card associated with the credit card number or use the information to confirm the identity of the user prior to granting network access.

**[0057]** Further, in various embodiments, the network credentials may comprise login procedural information. In one example, the credentials include a username and password which are to be provided within a form (e.g., an authentication form) retrieved from the authentication server 108 by the digital device 102. In some embodiments, the login procedural information may instruct the digital device 102 to populate specific fields within the form with the network credentials before submitting the completed form to the authentication server 108. Those skilled in the art will appreciate that there are many ways to provide credentials to the authentication server 108. The process of providing the credentials to the authentication server is further discussed in co-pending U.S. patent application Ser. No. 11/899,638, entitled "System and Method for Obtaining Network Credentials," filed Sep. 6, 2007.

**[0058]** The credential request response module 206 or the encryption/decryption module 208 may encrypt the credential request response with an encryption key associated with the DDID or the credential request. In one example, the credential server 116 stores one or more shared encryption keys. Each shared encryption key may be shared by at least one digital device 102. The credential request response module 206 may encrypt the credential request response with the shared encryption key associated with the digital device 102 (e.g., the shared encryption key may be associated with the DDID). The credential request response module 206 or the encryption/decryption module 208 may also encrypt the credential request with an encryption key that is part of a key pair. There may be many ways in which the encryption/decryption module 208 encrypts the credential request.

**[0059]** The encryption/decryption module 208 may decrypt the credential request and encrypt the credential request response. As previously discussed, the encryption/decryption module 208 may decrypt the digital signature of the credential request. In one example, the encryption/decryption module 208 decrypts the digital signature based on an encryption key

that is associated with the DDID contained within the credential request. The encryption/decryption module 208 may also encrypt the credential request response. In one example, the encryption/decryption module 208 encrypts the credential request response based on an encryption key associated with the DDID (e.g., a shared encryption key or an encryption key that is part of a key pair).

**[0060]** In various embodiments, the encryption/decryption module 208 may encrypt the network records contained within the network record storage 210 and manage the encryption key storage 212. The encryption/decryption module 208 may also establish secure communications (e.g., via SSL and HTTPS) with a digital device when storing network credentials. This process is further described in FIG. 7. In accordance with some embodiments, the encryption/decryption module 208 may be optional.

**[0061]** The network record storage 210 and the encryption key storage 212 may store network records and encryption keys, respectively. The network record storage 210 and the encryption key storage 212 may comprise one or more databases. In one example, the network record storage 210 may store network records. A network record may comprise a DDID, SSID, and network credentials. The network record may also comprise a username and password for the user to access, alter, update, or store network records within the credential server 116.

**[0062]** In various embodiments, the network record may also allow multiple digital devices 102 to use the same network credentials. In one example, the user may own multiple digital devices 102. Multiple DDIDs, each DDID associated with a different digital device 102, may be included in the same network record. In some embodiments, multiple devices may be associated with one or more network records, and the one or more network records are associated with a user. As a result, the user may retrieve the network credentials for a hotspot using any number of digital devices 102. Those skilled in the art will appreciate that there are many ways in which the network records and/or the information contained therein may be stored and organized (e.g., different data structures, databases, records, organizing schemes, and/or methodologies).

**[0063]** FIG. 3 is a flow diagram of an exemplary process for providing network access to the digital device 102. When the digital device 102 first enters into a hotspot, the digital device 102 may scan for the local area network 106 in step 300. As a result of the scan, the network device 104 may provide network configuration information in step 302. The network

configuration information may comprise one or more IP addresses for access to the DNS server 110.

**[0064]** In step 304, a credential request is generated by the digital device 102. Subsequently, the credential request may be sent to the DNS server 110 in step 306 using one of the IP addresses previously received from the network device 104.

**[0065]** Based on the credential request, the credential server 116 is identified by the DNS server 110 in step 308. In other embodiments, the DNS server 110 forwards the credential request to the credential server 116. When the DNS server 110 is unable to locally resolve the DNS request, the credential request is forwarded to another DNS server on the communication network 114 (e.g., over port 53) which may then forward the credential request to the credential server 116. The credential request is forwarded, either directly or indirectly through one or more other DNS servers on the communication network 114, to the credential server 116 in step 310.

**[0066]** The credential server 116 identifies the network credential needed based on the credential request in step 312. For example, the credential request may comprise an identifier (i.e., the DDID) for the digital device 102 as well as an identifier for the hotspot SSID (e.g., the service provider such as an operator). The identifiers may be compared against a table (e.g., network record) of such identifiers by the credential request module 204 or the credential request response module 206 to determine the proper network credential. A credential request response is then generated by the credential request response module 206 in step 314 and relayed back to the DNS server 110 in step 316. The DNS server 110 forwards the credential request response back to the digital device in step 318.

**[0067]** The digital device 102 may then retrieve the network credentials from the credential request response in step 320. The network credential may then be provided to the network device 104 in step 322. Upon verifying the network credentials, the network device 104 provides network access to the digital device 102 in step 324.

**[0068]** Referring now to FIG. 4, an exemplary credential request 400 is shown in more detail. According to exemplary embodiments, the credential request module 204 may generate the credential request 400. In one embodiment, the credential request 400 may be a DNS string having a structure that comprises a location identifier 402, a sequence identifier



404, a signature 406, the DDID 408, a service set identifier (SSID) 410, and a version identifier 412.

**[0069]** The optional location identifier 402 may indicate a physical or geographic location of the digital device 102, the network device 104, the authentication server 108, or the access controller 112. In various embodiments, the location identifier 402 may be used by the credential server 116 to track the usage of hotspots, users of the digital device 102, as well as the digital device 102.

**[0070]** The sequence identifier 404 may comprise any number or set of numbers used to correspond to a subsequent request to the credential server 116 to determine if the login is successful. That is, the sequence identifier 404 provides a correlation mechanism by which verification of the login process may be made by the credential server 116.

**[0071]** In exemplary embodiments, the signature 406 comprises a cryptographic signature (i.e., digital signature) that is utilized to prevent spoofing. The signature 406 of the request from digital device 102 is verified by the credential server 116. If the signature 406 is not valid, then the request is rejected by the credential server 116.

**[0072]** The DDID 408 comprises an identifier of the digital device 102. For example, the DDID 408 may comprise a MAC address or any other identifier of the digital device 102.

**[0073]** The SSID 410 comprises an identifier of the network access point or Wi-Fi service provider. For example, the SSID 410 may comprise the name of the service provider or the name of the venue operating the network device 104.

**[0074]** The version identifier 412 may identify the protocol or format of the credential request 400. For example, a digital device 102 may generate the credential request 400 and organize the data in a number of different formats. Each different format may be associated with a different version identifier. In some embodiments, the components of the credential request response module 206 may be updated, reconfigured, or altered over time, which may affect the structure of the credential request 400. As a result, the credential server 116 may receive a plurality of credential requests 400 which are formatted differently. The credential server 116 may access the required information from each credential request based on the respective version identifier.

**[0075]** FIG. 5 is a block diagram of an exemplary credential request response. According to exemplary embodiments, the credential request response module 206 may generate the credential request response 500. In one embodiment, the credential request response 500 may comprise encrypted text 502. The encrypted text may comprise an optional nonce 504 and credential information 506. The credential information may comprise key/value pairs 508 through 510.

**[0076]** As previously discussed, the credential request response may be formatted as a DNS response comprising encrypted text 502. The encrypted text 502 includes the network credentials (e.g., username, password, and login procedure information). Although the credential request response 500 is depicted as including encrypted text 502, the text within the credential request response 500 need not be encrypted.

**[0077]** The encrypted text 502 may comprise the nonce. The nonce, as previously discussed, may be retrieved from the credential request. Once the credential request response 500 is received by the digital device 102, the digital device 102 may compare the nonce within the credential request response 500 to the nonce transmitted within the credential request for authentication. Although the nonce is depicted as within the credential request response 500 in FIG. 5, the nonce is optional.

**[0078]** The credential information 506 may comprise a username, password, login procedure information, or a combination of these. The credential information 506 may comprise key/value pairs 508 through 510. Any number of key/value pairs may be within the credential information 506. The key/value pairs may represent the credential information to be received and translated by the digital device 102. The credential information 506 is depicted as key/value pairs for exemplary purposes only; the credential information may be within any format not necessarily limited to key/value pairs.

**[0079]** FIG. 6 is a flow diagram of the exemplary method for providing network credentials. In step 602, the credential server 116 receives the credential request from the digital device 102.

**[0080]** In various embodiments, the credential server 116 decrypts and authenticates the digital signature with an encryption key. The credential server 116 may then identify a network record based on the DDID and the SSID contained within the network record in step 604. In one example, the credential request response module 206 retrieves one or more

network records associated with the DDID within the credential request. The credential request response module 206 then identifies at least one network credential associated with the SSID within the retrieved network record(s).

**[0081]** In step 606, the credential request response module 206 retrieves the identified network credential(s) from the selected network record. In one example, the credential request response module 206 identifies a username and password that the user of the digital device 102 must provide to the authentication server 108 to obtain network access. The credential request response module 206 generates the credential request response comprising the network credentials (e.g., username, password) to the digital device 102 in step 608.

**[0082]** In some embodiments, the credential request response module 206 may identify login procedural information as part of the network credentials. The credential request response module 206 may retrieve the login procedural information from the network record (e.g., the same network record containing a password associated with the SSID). The login procedural information may contain a form identifier and instructions (e.g., parameters) for the digital device 102 to follow to obtain network access. In one example, the digital device 102 retrieves the form identifier and instructions from the network credential within the credential request response. The digital device 102 may identify forms received from the authentication server 108 and input data based on the form identifier and instructions. In another example, the digital device 102 provides information to the authentication server 108 to obtain network access based on the login procedural information included within the credential request response. The process of providing information to the authentication server 108 is further described in U.S. patent application Ser. No. 11/899,638 entitled "Systems and Methods for Obtaining Network Access", filed Sep. 6, 2007.

**[0083]** FIG. 7 is another flow diagram of the exemplary method for providing network credentials. The digital device 102 may search and find an available wireless network via the network device 104. While connecting to the hotspot, the digital device 102 may receive network configuration information in step 702. Network configuration information may comprise an identifier for the network device 104, or the DNS server 110. In one example, the digital device 102 receives a DNS server IP address (e.g., for the DNS server 110) during the connection process.

**[0084]** In step 704, the digital device 102 generates the credential request. The credential request may comprise a sequence identifier, DDID, and SSID. In step 706, the digital device

102 optionally generates a nonce and digitally signs the credential request with an encryption key. The digital device 102 transmits the credential request as a standard protocol in step 708. The network device 104 may receive and forward the credential request to the communication network 114. In various embodiments, the network device 104 may provide the credential request to the DNS server 110 which may forward the credential request to the credential server 116.

**[0085]** In exemplary embodiments, the credential request module 204 of the credential server 116 receives the credential request. The credential request module 204 may retrieve an encryption key associated with the DDID within the credential server from the encryption key storage 212. The credential request module 204 may then decrypt the digital signature of the credential request for authentication. The credential request module 204 may further retrieve the nonce and a sequence identifier from the credential request.

**[0086]** The credential request response module 206 of the credential server 116 may then retrieve a network record associated with the DDID and the SSID from the network record storage 210. The credential request response module 206 retrieves network credentials from the network record and generates the credential request response. The credential request response may comprise the network credentials and the nonce. The encryption/decryption module 208 may encrypt the credential request response with an encryption key associated with the DDID retrieved from the encryption key storage 212. In some embodiments, the credential request response is formatted as a standard protocol (e.g., DNS).

**[0087]** In step 710, the digital device 102 receives the credential request response. The digital device 102 subsequently authenticates the credential request response in step 712. In one example, the digital device 102 decrypts the credential request response with the same encryption key used to digitally sign the credential request. The digital device 102 may further retrieve the nonce within the credential request response and compare the nonce to the nonce transmitted within the credential request for further authentication. If the credential request response is found to be authentic, the digital device 102 retrieves the network credentials from the credential request response in step 714.

**[0088]** In step 716, the digital device 102 identifies the authentication requirements associated with network access. In various embodiments, the digital device 102 determines the correct information and network credentials to provide to the authentication server 108. In one example, the digital device 102 retrieves one or more network access pages from the

authentication server 108. The digital device 102 may access the correct network access page from the authentication server and automatically make selections. In one example, the digital device 102 may automatically activate selections (e.g., activate buttons within the network access page, check boxes, and select radio buttons).

**[0089]** For example, the credential request response module 206 may provide instructions to the digital device 102 for the automatic selections within a network access page. As discussed herein, a network access page may comprise one or more web pages, one or more tags, or a combination of both retrieved from the authentication server 108. In one example, software within the digital device 102 may automatically check all selection boxes within a network access page. The digital device 102 may then uncheck select boxes based on the login procedure information. Those skilled in the art will appreciate that there may be many methods with which selections may automatically be made. In other embodiments, the digital device 102 receives XML tags from the authentication server 108. The digital device 102 may provide information based on the XML tags and instructions within the login procedural information to the authentication server 108 to obtain network access.

**[0090]** In step 718, the digital device 102 provides the network credential to the network device 104 to obtain network access to the communication network 114. In one example, the credential request response module 206 retrieves one or more forms from the authentication server 108, populates the forms with one or more network credentials, and provides the completed forms to the authentication server 108. In another example, the credential request response module 206 provides the network credentials as needed to the authentication server 108. Once the network credentials are received by the authentication server 108, the authentication server 108 may allow communication between the digital device 102 and the communication network 114. In one example, the authentication server 108 commands the access controller 112 to allow the digital device 102 access to the communication network 114.

**[0091]** The digital device 102 may subsequently test network connectivity to confirm network access. In one example, the digital device 102 transmits a request to the credential server 116 to determine if the communication network 114 is available. In some embodiments, the query or command contains the sequence identifier previously submitted within the credential request. If network access is successful, the credential server 116 may

receive the request and retrieve the sequence identifier. The credential server 116 may then confirm that network access was successful.

**[0092]** FIG. 8 is a flow diagram of an exemplary method for receiving and storing network credentials. In various embodiments, users may create and store network records within the credential server 116. For example, the credential server 116 may comprise a credential storage module (not depicted) that provides a graphical user interface (GUI) that allows users to create, store, update, remove, and modify network records.

**[0093]** In step 802, the credential server 116 provides the user with a network credential request form. In one example, the credential server 116 provides the network credential request form to a user as one or more web pages over the Internet. The network credential request form is configured to receive the service provider's name (e.g., operator's name) and/or SSID and network credentials.

**[0094]** The service provider's name may comprise the name of the entity that operates the hotspot, one or more components related to the hotspot (e.g., the network device 104), or the infrastructure of the local area network 106. In some embodiments, the service provider's name comprises the name of an organization that manages one or more hotspots for another service provider. In one example, a coffee shop and bookstore may both use a third-party manager to manage the hotspots, even if the hotspots have different service providers. In some embodiments, the network credential request form may be configured to receive the third-party manager's name. In some embodiments, the service provider's name comprises the name of an organization that resells access to a hotspot network (e.g., an aggregator).

**[0095]** The network credential request form may also receive the SSID as a network service selection. In one example, the network credential request form comprises a pull down menu of different service providers and/or hotspots that the user may select. For example, a user may select "Starbucks" or "San Francisco International Airport" as a hotspot. The user may be given further options to such as geographic locations of the hotspot. The user may also select the service provider. For example, the user may select "T-Mobile" as a service provider. The network credential request form may then allow the user to select among one or more various hotspots associated with T-mobile. The selection(s) may then be stored as a network record. Alternately, a network service identifier associated with the selection(s) is generated as the SSID.

**[0096]** Further, the network credential request form may receive the network credential from the user. For example, the user may enter a username, password, passcode as network credentials within the network credential request form. In some embodiments, after the network credential request form receives the SSID, the network credential request form determines the type of network credentials required. For example, the network credential request form identifies the information required to access a network at a hotspot at the San Francisco International Airport previously selected by the user. The network credential request form then generates fields or selections to allow the user to enter only the information necessary (e.g., username, password) to obtain network access at the hotspot.

**[0097]** The credential server 116 may also require the user to register prior to receiving the network credential request form. During registration, the user may be required to agree to terms of service and enter customer information. Customer information comprises a username and a password to access the credential server 116 to store network credentials. Optionally, the customer information may comprise the user's address, contact information, and payment options for the user to use services offered by the credential server 116.

**[0098]** In step 804, the credential server 116 receives the customer information and network service selections over the network credential request form. In step 806, the credential server may retrieve the network credential. In step 808 the credential server 116 receives the customer information. The credential server 116 associates the network credential with the customer information, network service selection and network credential(s) in step 810 to create a network record. The network record is then stored in step 812.

**[0099]** In some embodiments, the user may manually access the credential server 116 via the Internet. In other embodiments, the user may download and install network credential software on the digital device 102. The network credential software may identify and send the DDID of the digital device 102 to the credential server 116. In other embodiments, the network credential software may be pre-installed on the digital device 102. When the digital device 102 first activates the network credential software, the network credential software may identify and send the DDID of the digital device 102 to the credential server.

**[00100]** The user may input the SSID (e.g., identify the service provider or hotspots) into the network credential software. The user may also input the network credentials within the network credential software. After the network credential software has obtained the DDID, SSID, and network credentials, the network credential software may upload the information

to the credential server 116 which stores the information within a network record. In various embodiments, the network credential software may be downloaded from the credential server 116.

**[00101]** FIG. 9 is a block diagram of an exemplary digital device. The credential server 116 comprises a processor 900, a memory system 902, a storage system 904, an I/O interface 906, a communication network interface 908, and a display interface 910. The processor 900 is configured to execute executable instructions (e.g., programs). In some embodiments, the processor 900 comprises circuitry or any processor capable of processing the executable instructions.

**[00102]** The memory system 902 is any memory configured to store data. Some examples of the memory system 902 are storage devices, such as RAM or ROM. The memory system 902 can comprise the ram cache. In various embodiments, data is stored within the memory system 902. The data within the memory system 902 may be cleared or ultimately transferred to the storage system 904.

**[00103]** The storage system 904 is any storage configured to retrieve and store data. Some examples of the storage system 904 are flash drives, hard drives, optical drives, and/or magnetic tape. In some embodiments, the credential server 116 includes a memory system 902 in the form of RAM and a storage system 904 in the form of flash data. Both the memory system 902 and the storage system 904 comprise computer readable media which may store instructions or programs that are executable by a computer processor including the processor 900.

**[00104]** The optional input/output (I/O) interface 906 is any device that receives input from the user and output data. The optional display interface 910 is any device that is configured to output graphics and data to a display. In one example, the display interface 910 is a graphics adapter. It will be appreciated that not all digital devices 102 comprise either the I/O interface 906 or the display interface 910.

**[00105]** The communication network interface (com. network interface) 908 can be coupled to a network (e.g., the local area network 106 and communication network 114) via the link 912. The communication network interface 908 may support communication over an Ethernet connection, a serial connection, a parallel connection, or an ATA connection, for example. The communication network interface 908 may also support wireless



communication (e.g., 802.11 a/b/g/n, WiMax). It will be apparent to those skilled in the art that the communication network interface 908 can support many wired and wireless standards.

**[00106]** In various embodiments, systems and methods are described that enable a digital device to automatically select and access an available wireless network from a plurality of available wireless networks based on rules to achieve a satisfactory quality of service. Such rules could be implemented in the digital device itself, on a server in communication with the digital device, or a combination of both. In various embodiments, a wireless network is a network that allows wireless access between a digital device and a communication network such as the Internet.

**[00107]** In accordance with some embodiments, a user of a wireless digital device (e.g., digital device capable of Wi-Fi communication) creates an account on a web server and registers one or more digital devices (e.g., computers, laptops, personal digital assistants, and cell phones) with that account. The registered digital devices can be managed and a network record provisioned by a central server (e.g., a profile server or a credential server) via a network communication mechanism, such as HTTP.

**[00108]** FIG. 10 is a diagram of another environment in which embodiments of the present invention may be practiced. In various embodiments, a user with a digital device 1002 enters an area located near the network devices 1004 and 1006. In one example, the network devices 1004 and 1006 are separate access points which may each be used to establish communication between the digital device 1002 and the communication network 1008.

**[00109]** The digital device 1002 may scan the area surrounding the digital device 1002, detect the two network devices 1004 and 1006, and generate a list of available wireless networks with which the digital device 1002 may establish communication. In some embodiments, the list of available wireless networks comprises DDID, SSID, and/or BSID identifiers of the network devices 1004 and 1006.

**[00110]** Subsequently, the digital device 1002 provides the list of available wireless networks to a rules server 1010. In one example, the digital device 1002 provides the list of available wireless networks as a standard protocol over an open port of either the network device 1004 or the network device 1006 to the communication network 1008 and, ultimately,

to the rules server 1010. In another example, the digital device 1002 provides the list of available wireless networks over another network such as a cellular communication network (e.g., via CDMA, GSM, 3G, or EVDO) or other wireless network (e.g., Wi-Fi, Wimax, or LTE network) not depicted.

**[00111]** The rules server 1010 receives the list of available wireless networks and may retrieve a network profile for each wireless network identified within the list. A network profile is a record that is associated with a wireless network and comprises attributes concerning performance and/or quality of service provided by the associated network. In one example, the rules server 1010 identifies each network within the list and provides the SSID and/or BSID for each network to the profile server 1014. The profile server 1014 may then provide a network profile (based on the SSID and/or BSID) for each network to the rules server 1010. In some embodiments, the profile server 1014 retrieves the network profile from a database or other server (e.g., network database server 1012).

**[00112]** The rules server 1010 may select a preferred wireless network from the list of available wireless networks based on attributes within the network profiles and/or any attributes received from the digital device 1002. An attribute is a characteristic of a wireless network. In various embodiments, an attribute includes a performance metric, a shared indicator, or a service identifier. A performance metric of a wireless network is any measure of network performance. In some examples, a performance metric may comprise a latency metric, a bandwidth metric, or a quality of service (QOS) metric. Those skilled in the art will appreciate that a performance metric may include any type of metric that represents performance of a wireless network.

**[00113]** A latency metric is a measurement that represents time to send a packet of data from the digital device to a server on a network. In some embodiments, the digital device 1002 may send an ICMP “echo request” packet to a server and listen for an ICMP “echo response” reply. The latency metric may comprise an estimate of the round-trip time (generally in milliseconds) and/or include any packet loss. In another example, the latency metric is half of the estimated round-trip time.

**[00114]** A bandwidth metric is a measurement of the available bandwidth of a wireless network. In one example, the digital device may test available bandwidth by sending a block of data over the wireless network to a server and timing the response.

**[00115]** A QOS metric is any metric that measures the quality of service of the wireless network, the access device 1004, the access device 1006, and/or the communication network 1008. In one example, the QOS metric represents a reliability of the DHCP which is determined by timing the length of time required to get an IP address. The reliability of the DHCP may comprise a statistical measurement, a probability of receiving an IP address at all, and/or a distribution of time.

**[00116]** A shared indicator indicates if a wireless network is shared. In some embodiments, the shared indicator may be one of three states including “shared,” “not shared,” and “unknown”. Although the shared indicator may only include a single state (e.g., “not shared”), those skilled in the art will appreciate that the shared indicator can have any number of states. A wireless network with a shared indicator that indicates that the network is “shared” may indicate that the owner of the wireless network intends for others to use the network. One example of a “shared” network may include a wireless network which is intentionally “open” (e.g., unencrypted) for others to use.

**[00117]** A wireless network with a shared indicator that indicates that the network is “not shared” may indicate that the owner of the wireless network does not desire anyone who does not have express permission to access the network. In one example, wireless networks that are not shared are often intentionally encrypted (e.g., through WEP or WPA) so as to limit access to unauthorized users. Not all networks that are “not shared,” however, are encrypted. For example, the owner of the network may misconfigure the network device or, through error, allows a network to be open (i.e., unencrypted) even though the network is not intended to be shared.

**[00118]** A wireless network with a shared indicator that indicates that the network is “unknown” may indicate that the wireless network may either be “shared” or “not shared.” For example, the intent of the owner of an open network may not be known.

**[00119]** A service identifier may identify one or more services supported by the wireless network. In one example, one or more service identifiers indicate that a wireless network supports VOIP, teleconferencing, and/or video conferencing. The service identifier may identify any kind of service supported by the wireless network. In some embodiments, the service identifier may identify services that are not supported by the wireless network.

**[00120]** Those skilled in the art will appreciate that the network profile may comprise any number of attributes. Further, those skilled in the art will appreciate that the network profile may comprise only one or more performance metrics, only one shared indicator, or only one or more service identifiers.

**[00121]** In various embodiments, the rules server 1010 selects one or more wireless networks from the list of available wireless networks based on the attribute analysis. In one example, the rules server 1010 applies rules to the attributes. The rules may comprise minimum requirements, personalized settings, and attribute comparisons. In one example, the rules applied by the rules server 1010 may compare the attributes of one or more wireless networks to one or more minimum requirements. If the attributes for a wireless network are below the minimum requirements, then the wireless network may not be selected or removed from the list of available wireless networks.

**[00122]** In some embodiments, the rules applied by the rules server 1010 may be based on personalized settings by the user. For example, the user of the digital device 1002 may indicate personalized settings that indicate that the digital device 1002 is only to connect over wireless networks that have been designated as "shared." In this example, the rules server 1010 may select only those wireless networks with an attribute that comprises a shared indicator that identifies the wireless network as "shared."

**[00123]** In various embodiments, the rules applied by the rules server 1010 may be based on a comparison of the attributes of one wireless network to another. In one example, the attributes may indicate that one wireless network has a greater bandwidth and shorter latency than another. In this example, the rules server 1010 may select one wireless network that has better performance or valuable services in comparison to another. Those skilled in the art will appreciate that there may be any kind of rule used to select or to assist in the selection of a wireless network from the list of available wireless networks.

**[00124]** More than one rule may be applied by the rules server 1010 in making the wireless network selection. In one example, the rules server 1010 may apply personalized settings of the user before comparing attributes from different wireless networks and making a selection. In another example, the rules server 1010 may apply minimum requirements to the attributes before comparing the attributes.

**[00125]** Once the rules server 1010 selects the wireless network based on the comparison of attributes from the network profiles, the rules server 1010 may provide the wireless network selection to the digital device 1002. A wireless network selection includes one or more identifiers (e.g., network identifiers) that identify at least one wireless network. The wireless network selection may identify a single wireless network or comprise a sorted list of wireless networks which is sorted in order of preference.

**[00126]** In some embodiments, the rules server 1010 provides credentials (e.g., a credential request response) for the selected wireless network in addition to the wireless network selection to the digital device 1002. In one example, the rules server 1010 provides the selected wireless network to the credential server 1016 which then provides a credential request response (even though no credential request has been made) for the selected wireless network to the digital device 1002. In other embodiments, the digital device 1002 receives the wireless network selection and then proceeds to transmit a credential request to the credential server 1016 to receive the credentials as discussed herein.

**[00127]** Further, in various embodiments, the digital device 1002 attempts to establish a connection based on the selected wireless network. If the connection fails, the digital device 1002 may transmit a credential request to the credential server 1016 to retrieve credentials for network access as described herein. The digital device 1002 may provide the credential request to the credential server 1016 over an open port of the network device 1004. In another example, the digital device 1002 may provide a credential request over any other network including a connection with a different network device or over a cellular connection.

**[00128]** Although the rules server 1010, network database server 1012, profile server 1014, the credential server 1016, and the web server 1018 are depicted as separate servers in Fig. 1, the servers may all be combined as one or more servers. Similarly, the functions of any of the servers may be performed by one of the other servers depicted or any other server.

**[00129]** Although FIG. 10 depicts multiple servers (e.g., rules server, network database server, profile server, credential server, and web server) for performing the selection of a wireless network from the plurality of available wireless networks, it will be appreciated by those skilled in the art that the selection of the wireless networks may occur within the digital device 1002. In one example, the digital device 1002 retrieves the scan results listing available wireless networks and selects a wireless network based on configuration preferences. The configuration preferences may be based on one or more locally executed

rules, preferred signal strength, or any other attribute or attributes. In another example, the digital device 1002 selects a wireless network that supports a desired service (e.g., VOIP), meets a minimum latency standard, and meets a minimum QOS standard. In another example, the profile server 1014 provides the desired network profiles to the digital device 1002 which performs the analysis to determine the preferred wireless network.

**[00130]** FIG. 11 is a flow diagram of an exemplary process for providing a selection of a wireless network. In step 1102, a server (e.g., rules server 1010, network database server 1012, profile server 1014, credential server 1016, or web server 1018) receives a list of available wireless networks from the digital device 1002. In some examples, the list comprises the SSIDs or BSIDs of one or more network devices (e.g., network device 1004 and network device 1006). The list can comprise any information that identifies a network and/or network device.

**[00131]** In some embodiments, the server also receives one or more attributes associated with a network and/or network device. In various embodiments, the digital device 1002 measures signal strength, determines available services, or takes a performance metric for one or more networks and/or network devices that are identified on the list of available wireless networks.

**[00132]** In step 1104, the server retrieves a network profile from a plurality of network profiles stored in a network database for each available wireless network on the list of available wireless networks. Each network profile may comprise at least one attribute. In some embodiments, not all wireless networks on the list have a network profile. When a network profile for a wireless network on this list is not found, a network profile associated with the wireless network may be then created. If attributes are received from the digital device 1002, the server may determine which attribute received from the digital device 1002 is associated with which network, network device, and/or network profile.

**[00133]** In step 1106, the server compares attributes from each network profile against minimum requirements. In one example, the server compares latency metrics from all network profiles in the list (if available) against a minimum latency metric. The server may also compare attributes received from the digital device 1002 against the minimum requirements. In step 1108, the server removes one or more wireless networks from the list of available wireless networks and/or wireless network profiles based on the comparison(s). For example, any wireless network with a latency metric that falls below the minimum

latency metric may not be selected. In other embodiments, a wireless network with a latency metric that falls below the minimum latency metric may receive a weighted value that will be compared to other wireless networks to assist in the selection process.

**[00134]** In some embodiments, the user of the digital device 1010 determines the minimum requirements. In other embodiments, the minimum requirements may be selected for the user (e.g., by an administrator).

**[00135]** In step 1110, the server retrieves personalized settings for a user. The personalized settings may be sent by the user to the server. In some embodiments, the user has an account with the web server 1018 which contains the personalized settings. In one example, the server receives a user identifier along with the list of available wireless networks. The server then accesses the user's account and receives the personalized settings which are then applied to the attributes of the network profiles associated with a wireless network on the list. In various embodiments, users may configure personalized settings (e.g., the "aggressiveness") at which a digital device 1002 may connect to a wireless network. Such configurations could include:

- (a) Connect to anything open regardless of shared indicator;
- (b) connect to anything open except those with default manufacturer SSIDs (e.g., "linksys") that likely indicate the owner simply left the access point open out of the box and is unaware how to configure security functions;
- (c) connect to anything open that the profile server 108 has seen (or stored information regarding the Wi-Fi network); or
- (d) connect to anything open with a shared indicator of "shared," or has been marked as shared by some other means.

Those skilled in the art will appreciate that there may be many personalized settings.

**[00136]** In step 1112, the server removes one or more wireless networks from the list or network profiles based on the personalized settings. For example, the personalized settings may indicate that the user only wishes to connect to wireless networks that support videoconferencing and maintain a user defined QOS requirement. The server may then remove any wireless networks from the list of available wireless networks based on the

attributes either from the network profiles or recently received from the digital device 1002 that do not meet the user's personalized settings.

[00137] In some embodiments, the personalized settings may then be taken into account either before or after comparison of attributes from the network profiles. In one example, personalized settings indicate that the user does not wish to connect to a wireless network that is not designated as "shared" or providing certain services. In one example, the rules server 1010 either does not retrieve the network profiles associated with networks that do not provide the necessary service and/or does not compare attributes associated with those networks. In other embodiments, the digital device 1002 applies personalized settings to results (e.g., the wireless network selection) received from the rules server 1010 before accessing a preferred wireless network.

[00138] In step 1114, the server compares the attributes of the remaining wireless networks on the list. In various embodiments, the server will apply a weight and normalize one or more of the attributes (e.g., metrics) from within the network profiles. In some embodiments, older attributes may be removed or weighed less than other attributes that are newer. In one example, any metric that is over one week old may receive less weight than a similar newer metric. In another example, a metric that is over one month old may be removed from the network profiles or not considered in the comparison. Those skilled in the art will appreciate that not all attributes or information from within the network profiles may be taken into account in the comparison.

[00139] Each network profile may comprise any number of attributes. In one example, the rules server 1010 makes a wireless network selection based on comparing a metric from two different network profiles. In some embodiments, the rules server 1010 selects a wireless network based on a comparison between two similar metrics (i.e., the latency metric from the first network profile is compared to the latency metric from the second network profile). Those skilled in the art will appreciate that the rules server 1010 may select a wireless network based on comparisons between two similar recently received metrics or a recently received metric and another within a network profile.

[00140] In other embodiments, the rules server 1010 selects a wireless network based on a comparison of two dissimilar metrics (i.e., the latency metric from the first network profile is compared to a bandwidth metric from the second network profile). The rules server 1010 may execute an algorithm to weigh and normalize similar and/or dissimilar metrics or



attributes in order to make a comparison for selecting the appropriate wireless network. In one example, the rules server 1010 compares a latency metric in the first network profile to a bandwidth metric in the second network profile. The rules server 1010 may execute an algorithm to weigh and normalize the metrics. The algorithm may weigh the latency metric more than the bandwidth metric since latency may have a greater impact on network performance.

**[00141]** An attribute or metric may receive different weights depending on any number of factors. For example, a latency metric may receive a given weight when the metric falls within an acceptable range, otherwise the latency metric may be significantly less weight. A metric recently received from the digital device 1002 may receive greater weight than a metric of a similar type within a network profile. Those skilled in the art will appreciate that there are many ways to compare similar and/or dissimilar performance and/or qualitative metrics.

**[00142]** In step 1116, the server selects a wireless network based on the comparison of attributes. The wireless network selection may comprise a single preferred wireless network or a list of wireless networks sorted in order of preference. In one example, the rules server 1010 identifies the most preferred network, the second most preferred network, and so on. The rules server 1010 then provides the wireless network selection to the digital device 1002 in step 1118.

**[00143]** In various embodiments, the rules server 1010 only compares metrics that are recently received from the digital device 1002. In one example, two latency metrics are received from the digital device 1002. Each latency metric is associated with a separate wireless network identified on a list of available networks. In this example, the rules server 1010 may select a wireless network based on a comparison of the two attributes.

**[00144]** FIG. 12 is a flow diagram of an exemplary process for selecting a wireless network. In step 1002, the digital device 1002 enters into an area with two wireless networks and the digital device 1202 scans for networks to access. In step 1204, the digital device 1002 receives a first and a second network identifier of available wireless networks. As discussed herein, the first and second network identifiers may comprise BSIDs, SSIDs, or any other network identifiers. For example, the first network identifier may comprise a BSID and the second network identifier may comprise an SSID identifier. In another example, the first network may provide multiple identifiers including a BSID and an SSID while the second

network provides only an SSID. In this example, the first network identifier may comprise both the BSID and the SSID of the first network device while the second network identifier is only an SSID of the second network device.

**[00145]** In step 1206, the digital device 1002 generates a list of available wireless networks. For example, the digital device 1002 may generate a list comprising the first network identifier and the second network identifier. The list is then provided to a server in step 1208.

**[00146]** In step 1210, the digital device 1002 receives a wireless network selection from the server. The wireless network selection may comprise an identifier that identifies the selected wireless network or identifies the network device associated with the selected wireless network (e.g., a BSID and/or SSID of the network device). In various embodiments, the wireless network selection may comprise a list of wireless networks sorted by preference. The list may comprise two or more identifiers that identifies a selected wireless network or network device.

**[00147]** In step 1212, the digital device 1002 receives credentials for the wireless network selection from the server. In some embodiments, the credentials are received from the same server that received the list of available wireless networks from the digital device 1002.

**[00148]** In various embodiments, the digital device 1002 receives the wireless network selection from the server and then provides a credential request to receive the credentials for the desired network. In one example, the digital device 1002 provides the credential request in the same manner that the digital device 1002 provided the list of available wireless networks (e.g., over an open port of a network). In some embodiments, the preferred network does not require credentials or the credentials are stored locally on the digital device 1002.

**[00149]** In step 1214, the digital device 1002 accesses the selected wireless network with the credentials. The process of applying the credentials to a login page or the like is discussed herein.

**[00150]** In various embodiments, the digital device 1002 may provide the list of available wireless networks to the server over an open port of a network device in a manner similar to providing a credential request discussed herein. In other embodiments, the digital device 1002 may provide the list to the server over another network. In one example, the digital device 1002 generates a list of available Wi-Fi networks and provides the list over a cellular

network (e.g., EV-DO or HSDPA network). In this example, the wireless network selection may be returned to the digital device over the cellular network and then the digital device 1002 may attempt to access the preferred Wi-Fi network.

**[00151]** In another example, the digital device 1002 accesses one wireless network. The digital device 1002 can then provide a list of the available wireless networks to the server. The server may return the wireless network selection to the digital device 1002. If the preferred wireless network is not the network that the digital device 1002 has originally accessed, then the digital device 1002 may drop the connection and access the preferred wireless network.

**[00152]** Although Figs. 10-12 contemplate a server receiving a list of available wireless networks, determining a wireless network selection, and providing the selection to the digital device 1002, those skilled in the art will appreciate that a server is not necessary. In one example, the digital device 1002 generates a list of available wireless networks and then retrieves any available information regarding the networks on the list (e.g., from locally stored network profiles, from one or more network devices, from a local or remote database, and/or retrieving information from another network such as the Internet). The digital device 1002 may then make comparisons based on what attributes associated with the networks are available to make a selection or generate a prioritized list. The digital device 1002 may then access the selected wireless network.

**[00153]** In various embodiments, the digital device 1002 may generate and provide attributes regarding one or more networks to update the network profiles. In one example, the digital device 1002 determines the quality of the signal, bandwidth, or any other metrics and provides those metrics along with the list of available wireless networks to a server. In another example, as the digital device 1002 accesses a selected wireless network, measures attributes, and provides the attributes update metrics within a network profile. Attributes (e.g., latency metrics, bandwidth metrics, and QOS metrics) may be taken by the digital device 1002 at any time and used to update the network profiles.

**[00154]** FIG. 13 is a diagram for selecting a wireless network and accessing the selected wireless network. In various embodiments, the network device 1004 and network device 1006 provide a first and second network identifiers to the digital device 1002 in steps 1302 and 1304. In step 1306, the digital device 1002 generates metrics (i.e., attributes) by taking measurements regarding wireless networks associated with the network device 1004 and

network device 1006. In some examples, the metrics may include latency, strength of signal, or QOS metric.

**[00155]** In step 1308, the digital device 1002 generates a list of available wireless networks which may include the network identifier from the network device 1004 as well as the network identifier from the network device 1006. In some embodiments, the digital device 1002 may also comprise personalized settings which may indicate a preference between the two network identifiers or eliminate one or both of the network identifiers. In one example, the personalized settings indicate that only open networks that do not have a default manufacturer SSID (e.g., "linksys") may be accessed. In this example, if the network identifier from the network device 1004 indicates a default manufacturer SSID, the digital device 1002 may not include that network identifier for the network device 1004 in the list of available wireless networks. .

**[00156]** In some embodiments, if the digital device 1002 cannot generate a list identifying at least two or more networks, the digital device 1002 does not send the list. In one example, if the digital device 1002 can only identify one available wireless network that meets the user's requirements, then the digital device 1002 may attempt to access the wireless network directly or send a credential request for to a server to retrieve any necessary credentials for access.

**[00157]** In step 1310, the digital device 1002 provides the attributes and the list of available wireless networks over an open port (e.g., port 53) of the network device 1006 which acts like a proxy in providing the attributes and list of available networks to the rules server 1010. In other embodiments, the digital device 1002 provides the attributes and the list over an open port of the network device 1004. Alternately, the digital device 1002 may provide the attributes and the list over separate networks (e.g., the attributes over an open port of one of the network devices and the list over a cellular network). In step 1312, the network device 1006 acts as a proxy by providing the attributes and list via DNS to the rules server 1010.

**[00158]** In step 1314, the rules server 1010 retrieves network profiles. In one example, the rules server 1010 retrieves the network identifiers from the list and retrieves network profiles associated with the network identifiers.

**[00159]** In step 1316, the rules server 1010 (or profile server 1014) updates attributes within the network profiles with the attributes received from the digital device 1002. In one example, a new latency metric from the digital device 1002 is used to update the network profile associated with the network identifier from the network device 1004. A time-to-live value associated with the attribute may also be updated to indicate that the new latency metric is recent.

**[00160]** In step 1318, the rules server 1010 selects a network device based on comparing the attributes from within the network profiles. In some embodiments, the rules server 1010 also applies personalized settings from the digital device 1002 or from an account associated with the digital device 1002 (e.g., via the web server 1018) before making a selection. The rules server 1010 may prepare a prioritized list of the two network devices from the list provided by the digital device 1002. The list is prioritized based on which of the two network devices provides the most desirable service based on the metrics from the network profiles.

**[00161]** In step 1320, the rules server 1010 provides the wireless network selection and credentials via DNS back to the network device 1006 to function as a proxy to send the information to the digital device 1002. In one example, the rules server 1010 selects the network device 1004. The rules server 1010 may retrieve credentials for the network device 1004 based on the network identifier of the network device 1004. For example, the rules server 1010 may provide a credential request to the credential server 1016. The credential server 1016 may provide a credential request response containing necessary credentials to the rules server 1010 which then sends both the credentials received from the credential server 1016 as well as the wireless network selection to the digital device 1002.

**[00162]** In step 1322, then network device 1006 provides the network selection and the credentials over the open port to the digital device 1002. In step 1324, the digital device 1002 provides the credentials to access the network device 1004 and generates additional attributes regarding the network (i.e., take additional measurements). Once a connection is established, the new attributes are provided to the rules server 1010 or profile server 1014 to update the network profile associated with the network device 1004 in step 1326. In one example, the digital device 1002 may measure the time required to establish the connection with the network device 1004. The time required to establish the connection may then be used to update attributes in a network profile. If a connection is not established or fails, that information may also be provided to update the associated network profile.

**[00163]** In some embodiments, if the network connection with the selected network fails, the digital device 1002 may re-attempt to make the connection. If multiple attempts to make the connection fail, information regarding the failure is sent to update the associated network profile. The digital device 1002 may then attempt to make a connection with another network device (e.g., the network device 1006). In some embodiments, the digital device 1002 re-scans the area, generates a new list of available networks which may not include the network that the digital device 1002 failed to connect. The new list may be sent to the rules server 1010 to receive a new wireless network selection and the process may repeat.

**[00164]** In some embodiments, the rules server 1010 provides a prioritized list of available wireless networks sorted by preference. In one example, the rules server 1010 provides a prioritized list of three networks to the digital device 1002. The digital device 1002 may then attempt to access the first wireless network on the prioritized list. If the digital device 1002 is unable to connect to the first wireless network, then the digital device 1002 may proceed to attempt to connect to the next network on the list. Those skilled in the art will appreciate that the prioritized list may contain all, one, or some of the wireless networks identified in the list of available wireless networks. For example, the rules server 1010 may not identify wireless networks which are known to provide poor performance, do not provide desired service (e.g., VOIP service), and/or are otherwise blacklisted.

**[00165]** In various embodiments, the user of the digital device 1002 may override the wireless network selection to access any wireless network. In one example, the user chooses the priority of available wireless networks. In some embodiments, the user may configure the digital device 1002 or configure an account with the web server 1018 to include personal preferences that may reorder or otherwise alter a prioritized list of wireless networks from the rules server 1010. For example, the list of available wireless networks may be altered based on user preferences by the digital device 1002 or the web server 1018 prior to being provided to the rules server 1010.

**[00166]** In some embodiments, in addition to one or more open Wi-Fi networks, there may also be one or more encrypted Wi-Fi networks in a given location. A digital device 1002 may connect to an open Wi-Fi network and transmit the SSID of other Wi-Fi networks, including encrypted Wi-Fi networks, to the rules server 1010 via a network communication protocol such as HTTP.

**[00167]** The rules server 1010 may then determine, based on personalized settings or other rules, that an available encrypted Wi-Fi network is the preferred choice for a network connection. The rules server 1010 may transmit the necessary encryption keys to the digital device 1002 over the current open Wi-Fi network connection and send instructions to the digital device 1002 to switch to the encrypted Wi-Fi network.

**[00168]** The above-described functions and components can be comprised of instructions that are stored on a storage medium such as a computer readable medium. The instructions can be retrieved and executed by a processor. Some examples of instructions are software, program code, and firmware. Some examples of storage medium are memory devices, tape, disks, integrated circuits, and servers. The instructions are operational when executed by the processor to direct the processor to operate in accord with embodiments of the present invention. Those skilled in the art are familiar with instructions, processor(s), and storage medium.

**[00169]** The present invention is described above with reference to exemplary embodiments. It will be apparent to those skilled in the art that various modifications may be made and other embodiments can be used without departing from the broader scope of the present invention. Therefore, these and other variations upon the exemplary embodiments are intended to be covered by the present invention.

### **Claims**

1. A method comprising:  
receiving a first network device identifier for a first network device and a second network device identifier for a second network device;  
obtaining a first network profile comprising a first attribute, the first network profile based on the first network device identifier;  
obtaining a second network profile comprising a second attribute, the second network profile based on the second network device identifier; and  
selecting either the first network device identifier or the second network device identifier based on an attribute analysis of the first attribute and the second attribute.
2. The method of claim 1, wherein the first network device identifier and the second network device identifier are received from a digital device by a server.
3. The method of claim 1, further comprising providing a wireless network selection identifier based on the selection.
4. The method of claim 1, further comprising providing a credential request response based on the selection.
5. The method of claim 1, wherein the network selection identifier comprises the first network device identifier.
6. The method of claim 1, wherein the network selection identifier comprises a list including the first network device identifier and the second network device identifier sorted based on the attribute analysis of the first attribute and the second attribute.
7. The method of claim 1, further comprising comparing the first attribute and the second attribute to minimum requirements wherein selecting either the first network identifier or the second network device identifier is also based at least in part on the comparison of the attributes to the minimum requirements.
8. The method of claim 1, further comprising comparing the first attribute and the second attribute to personalized settings wherein selecting either the first network identifier or the second network device identifier is also based at least in part on the comparison of the attributes to personalized settings.



9. The method of claim 1, further comprising receiving a user identifier and retrieving the personalized settings from a user account based on the user identifier.

10. The method of claim 1, wherein the attributes comprise a performance metric, a shared indicator, and a service identifier.

11. A system comprising:

a digital device coupled to a communication network and configured to transmit a first network device identifier for a first network device and a second network device identifier for a second network device over the communication network; and

a server coupled to the communication network and configured to receive the first network device identifier for a first network device and a second network device identifier for a second network device from the digital device, to obtain a first network profile comprising a first attribute, the first network profile based on the first network device identifier, to obtain a second network profile comprising a second attribute, the second network profile based on the second network device identifier, and to select either the first network device identifier or the second network device identifier based on an attribute analysis of the first attribute and the second attribute.

12. The system of claim 11, wherein the first profile and the second profile are obtained from a network database.

13. The system of claim 11, wherein the server is further configured to provide a wireless network selection identifier based on the selection to the digital device.

14. The system of claim 11, wherein the server is further configured to provide a credential request response based on the selection.

15. The system of claim 11, wherein the network selection identifier comprises the first network device identifier.

16. The system of claim 11, wherein the network selection identifier comprises a list including the first network device identifier and the second network device identifier sorted based on the attribute analysis of the first attribute and the second attribute.

17. The system of claim 11, wherein the server is further configured to compare the first attribute and the second attribute to minimum requirements wherein selecting either the first

network identifier or the second network device identifier is also based at least in part on the comparison of the attributes to the minimum requirements.

18. The system of claim 11, wherein the server is further configured to compare the first attribute and the second attribute to personalized settings wherein selecting either the first network identifier or the second network device identifier is also based at least in part on the comparison of the attributes to personalized settings.

19. The system of claim 18, wherein the server is further configured to compare receiving a user identifier and retrieving personalized settings from a user account based on the user identifier.

20. The system of claim 18, wherein the attributes comprise a performance metric, a shared indicator, and a service identifier.

21. A computer readable storage medium configured to store instructions, the instructions comprising a method, the method comprising the steps of:

receiving a first network device identifier for a first network device and a second network device identifier for a second network device;

obtaining a first network profile comprising a first attribute, the first network profile based on the first network device identifier;

obtaining a second network profile comprising a second attribute, the second network profile based on the second network device identifier; and

selecting either the first network device identifier or the second network device identifier based on an attribute analysis of the first attribute and the second attribute.

1/13

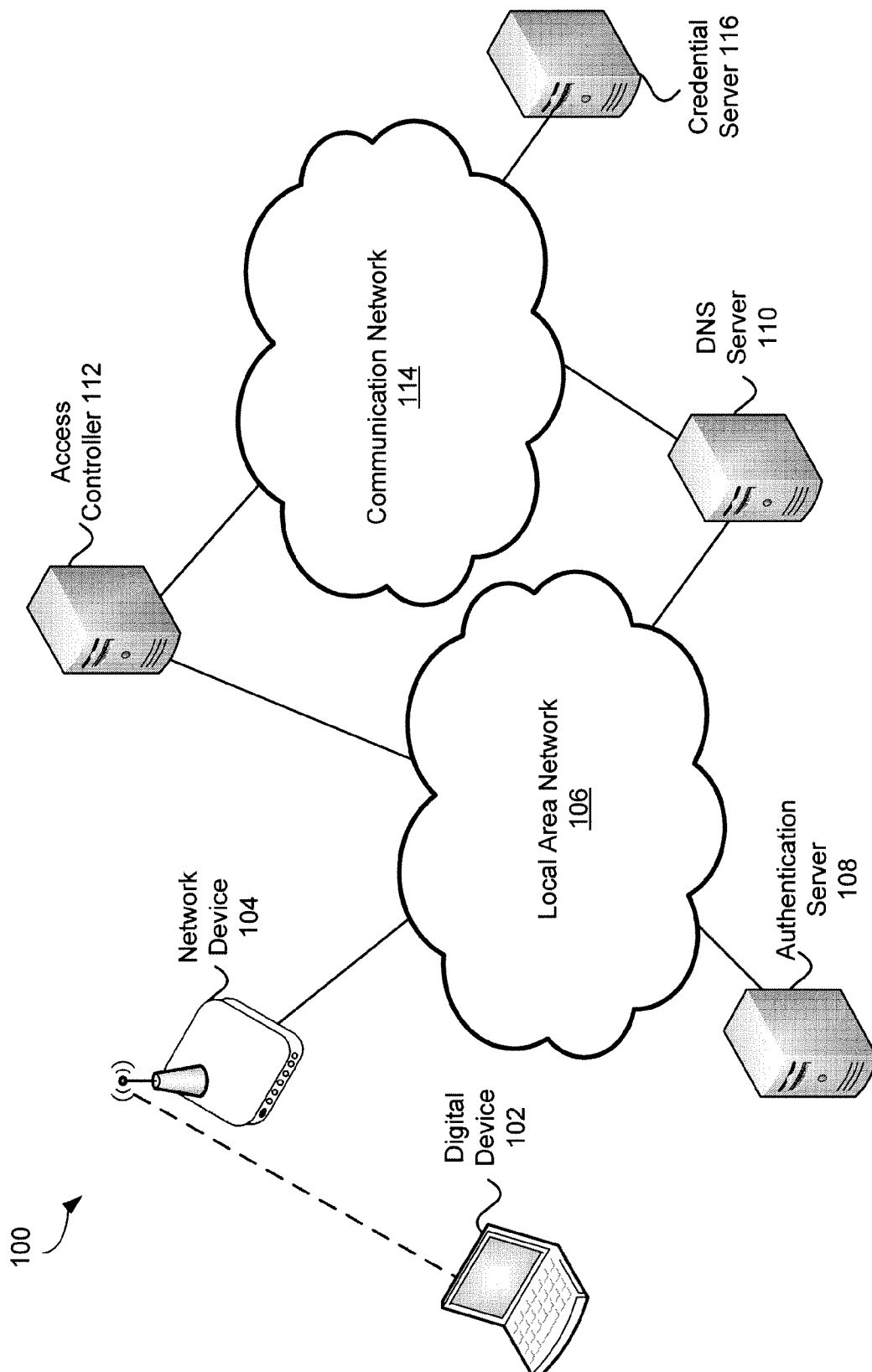


FIG. 1

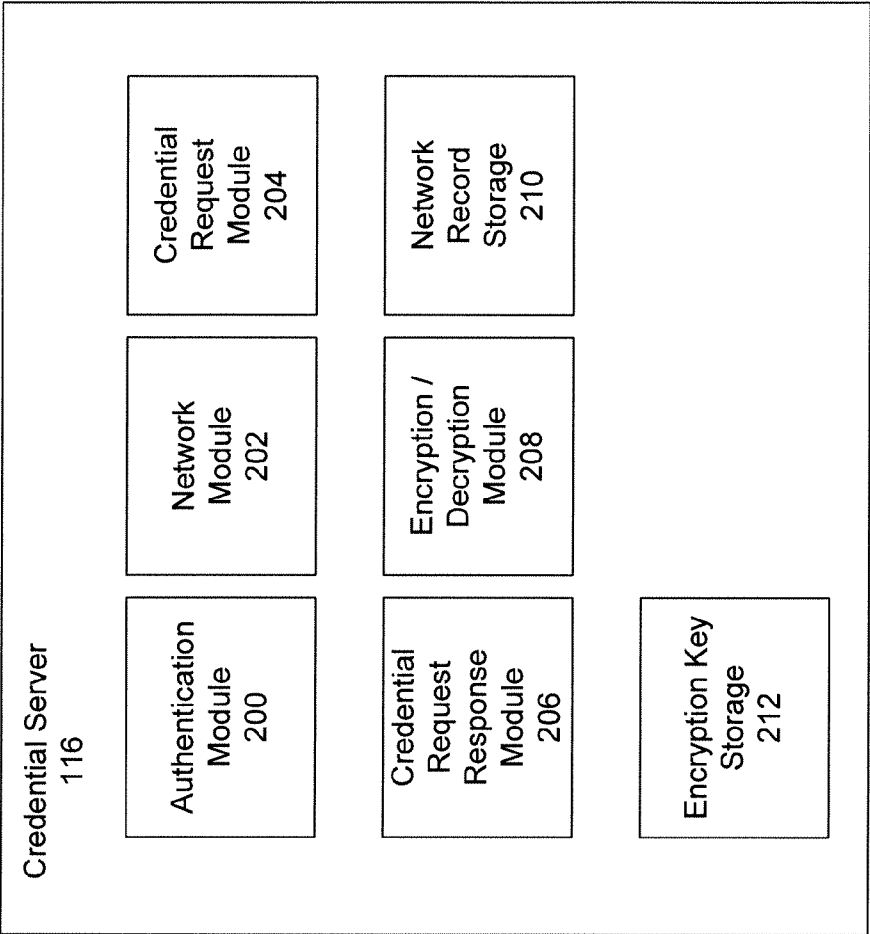


FIG. 2

3/13

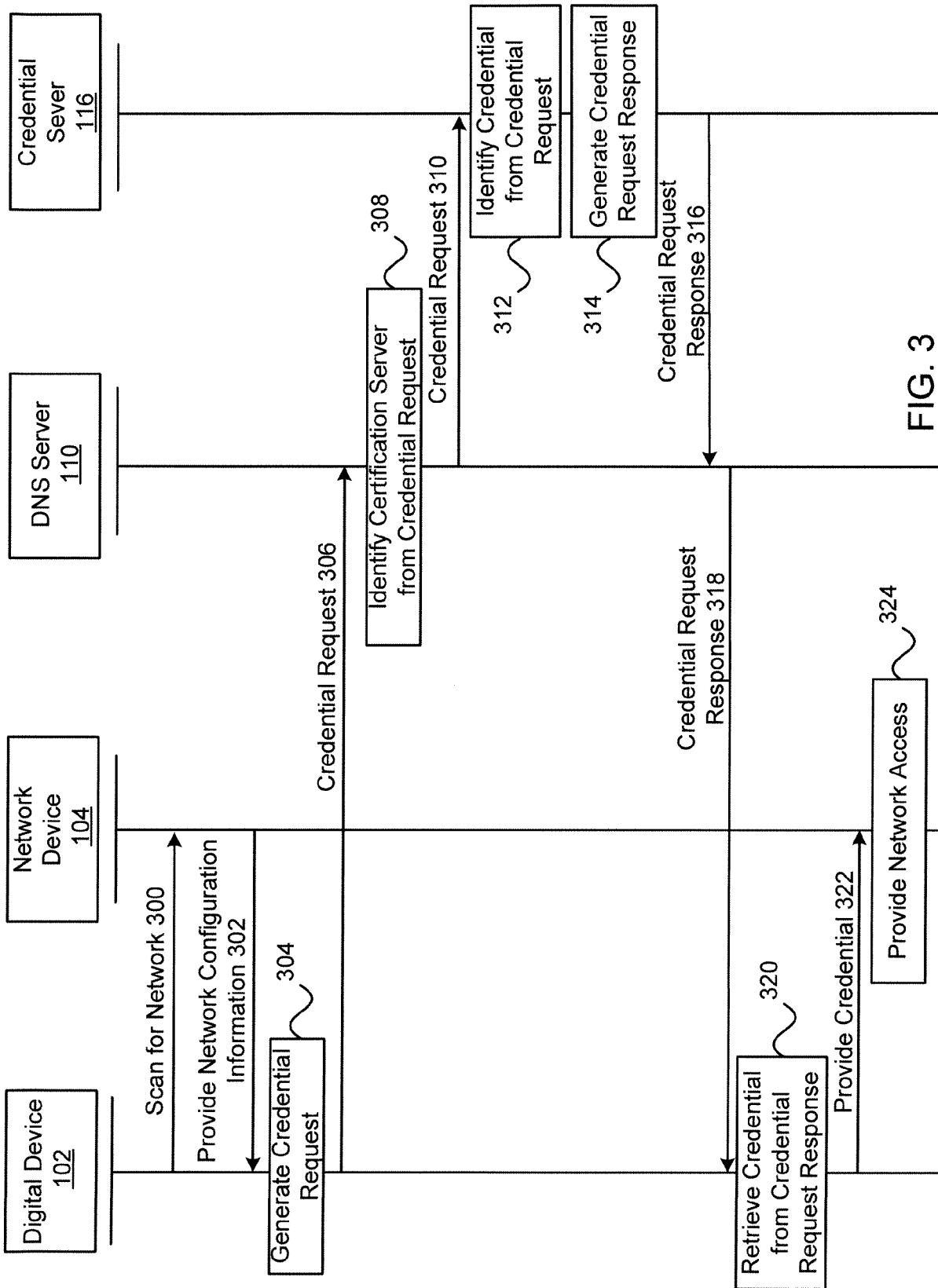


FIG. 3

Credential  
Request 400

Location Identifier 402	Sequence Identifier 404	Signature 406	DDID 408	SSID 410	Version Identifier 412
----------------------------	----------------------------	------------------	-------------	-------------	---------------------------

FIG. 4

5/13

Credential  
Request  
Response 500

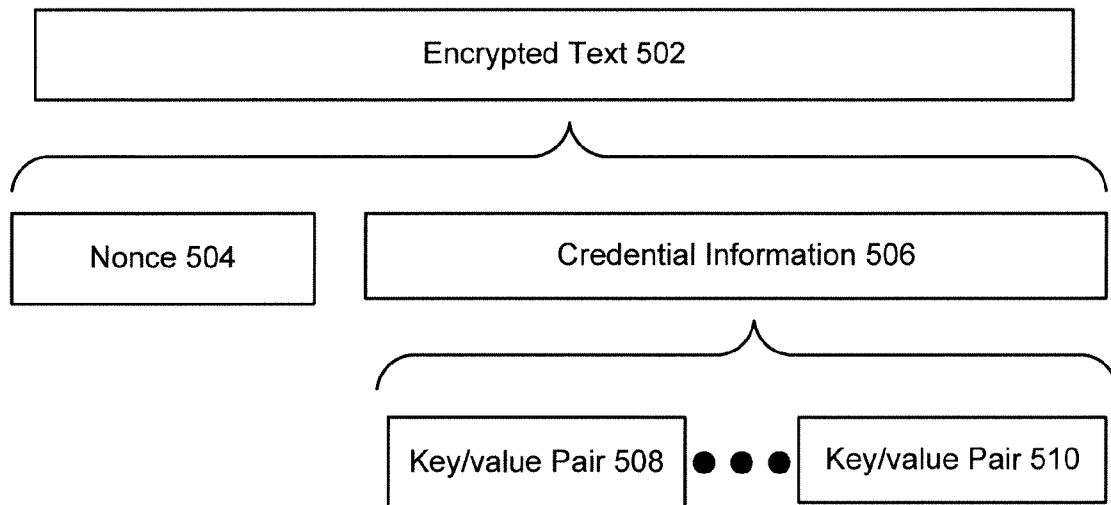


FIG. 5

6/13

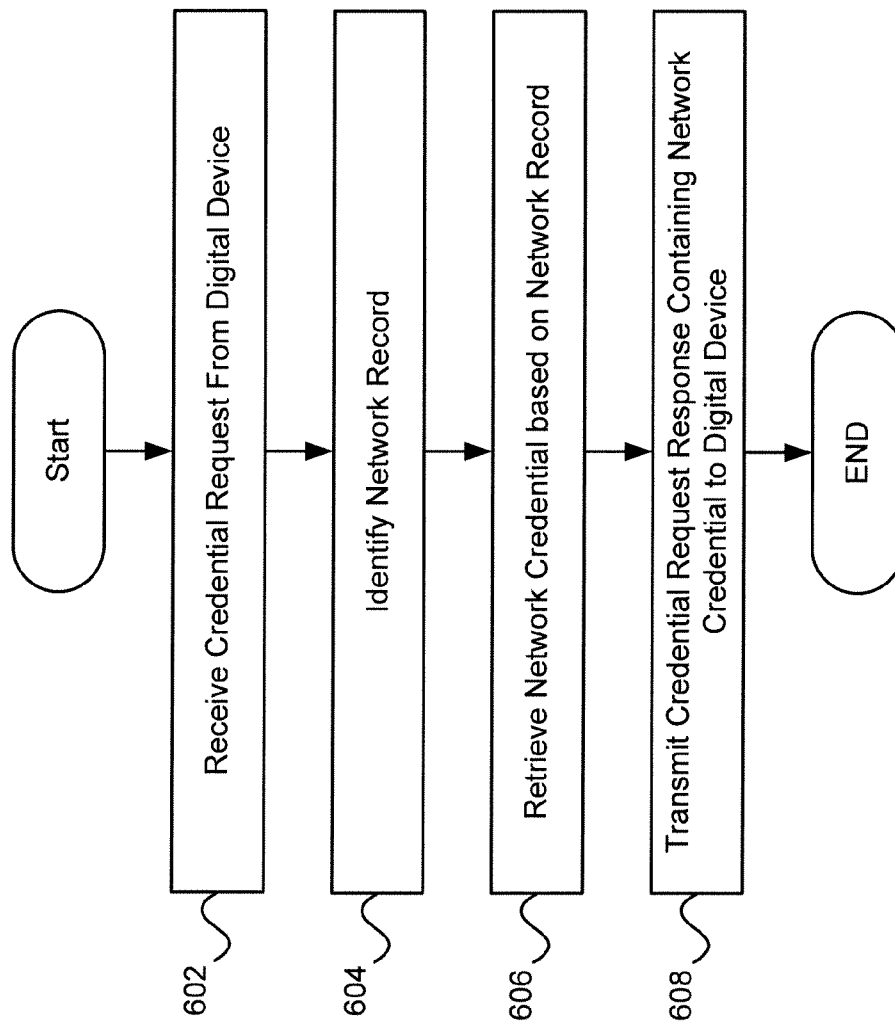
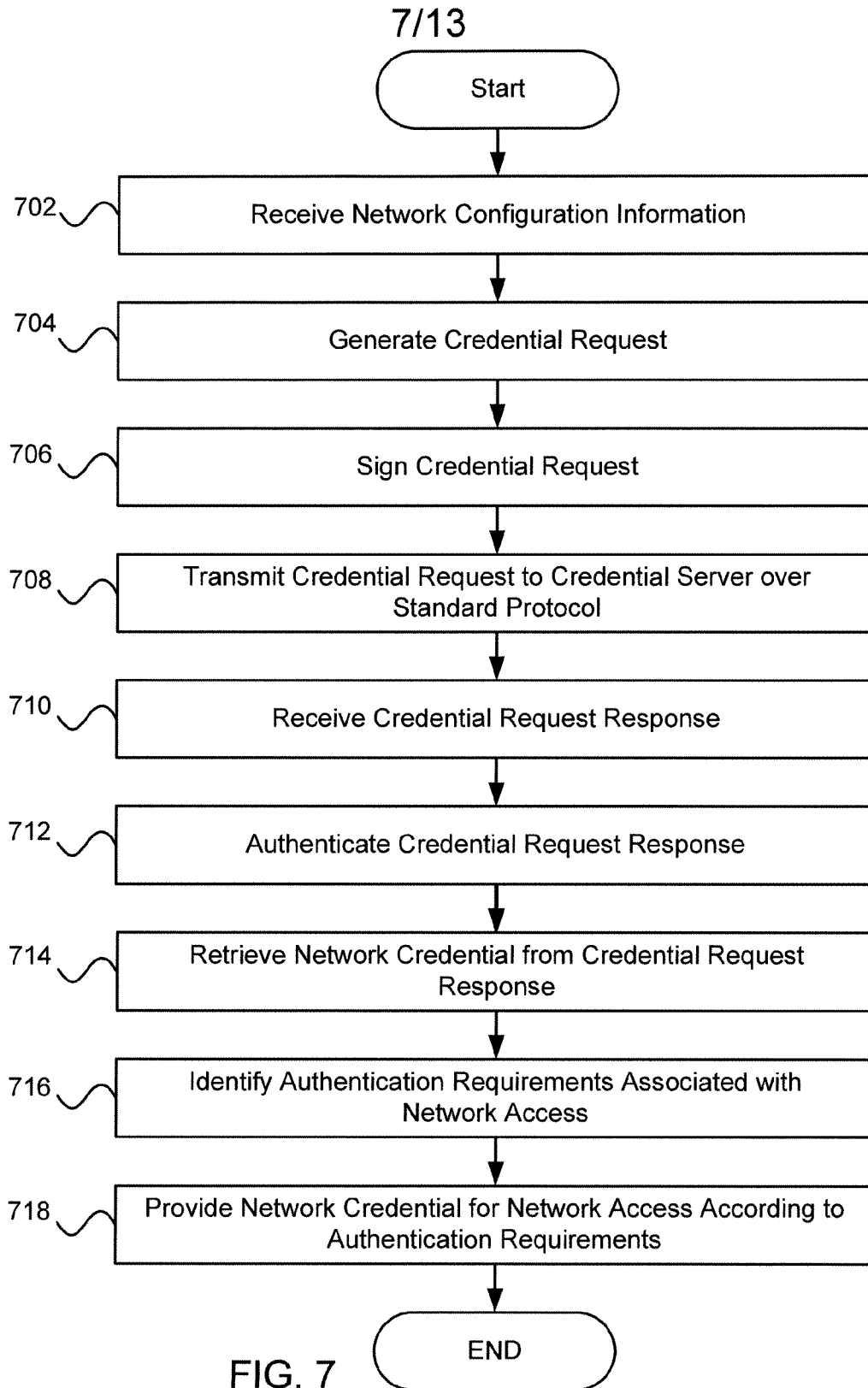


FIG. 6





8/13

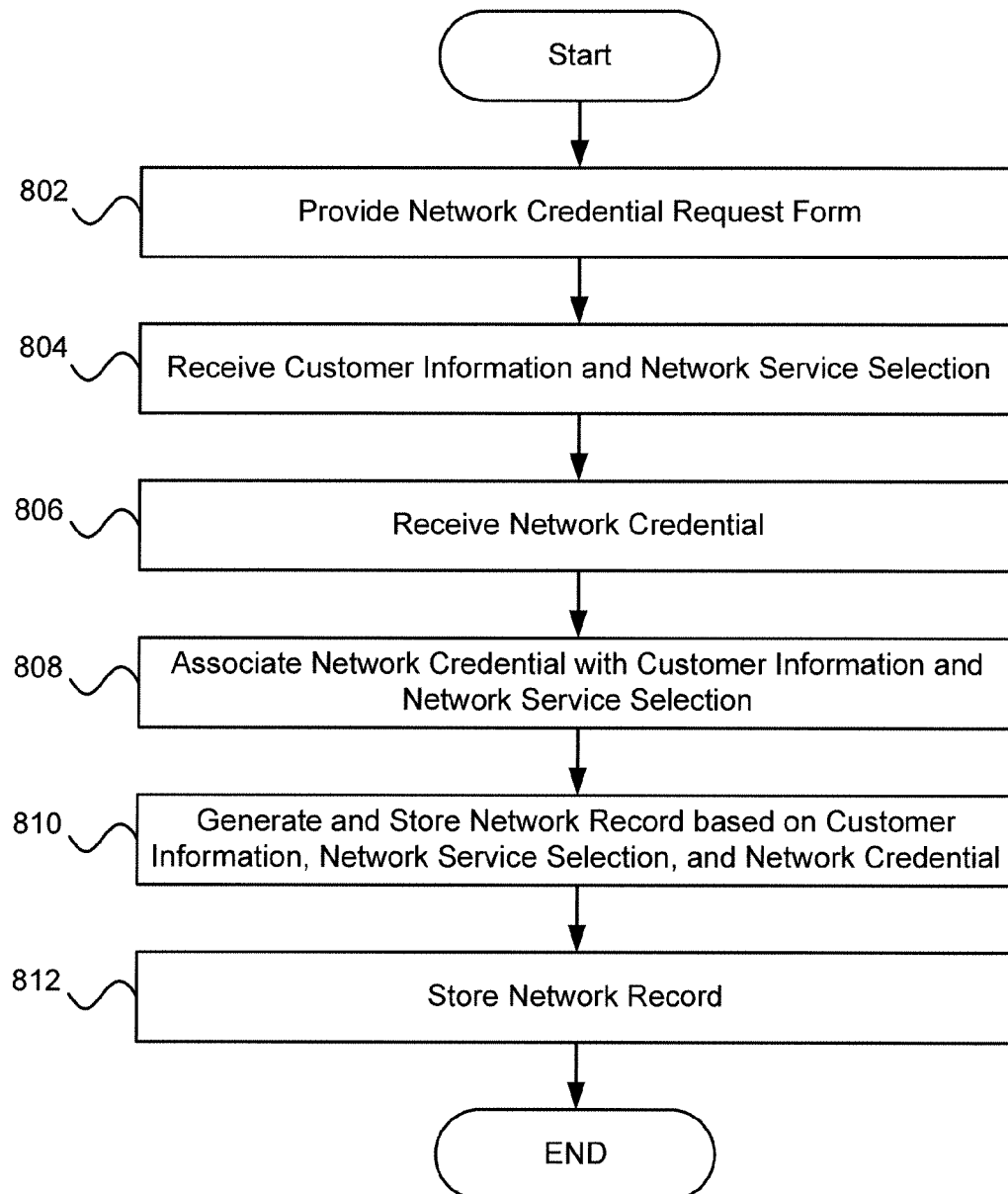


FIG. 8

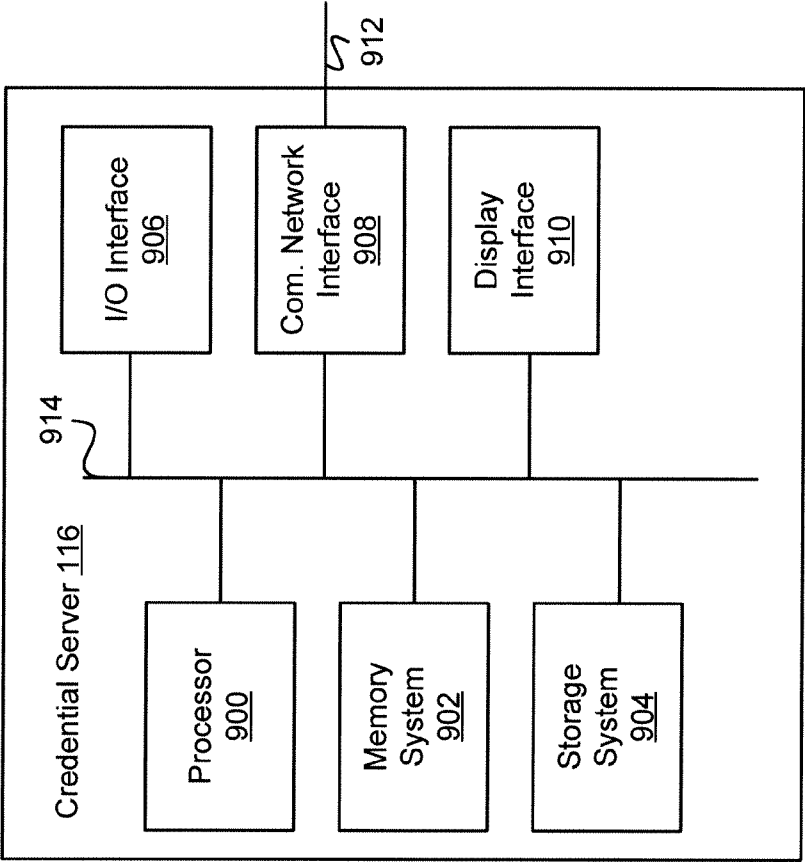


FIG. 9

10/13

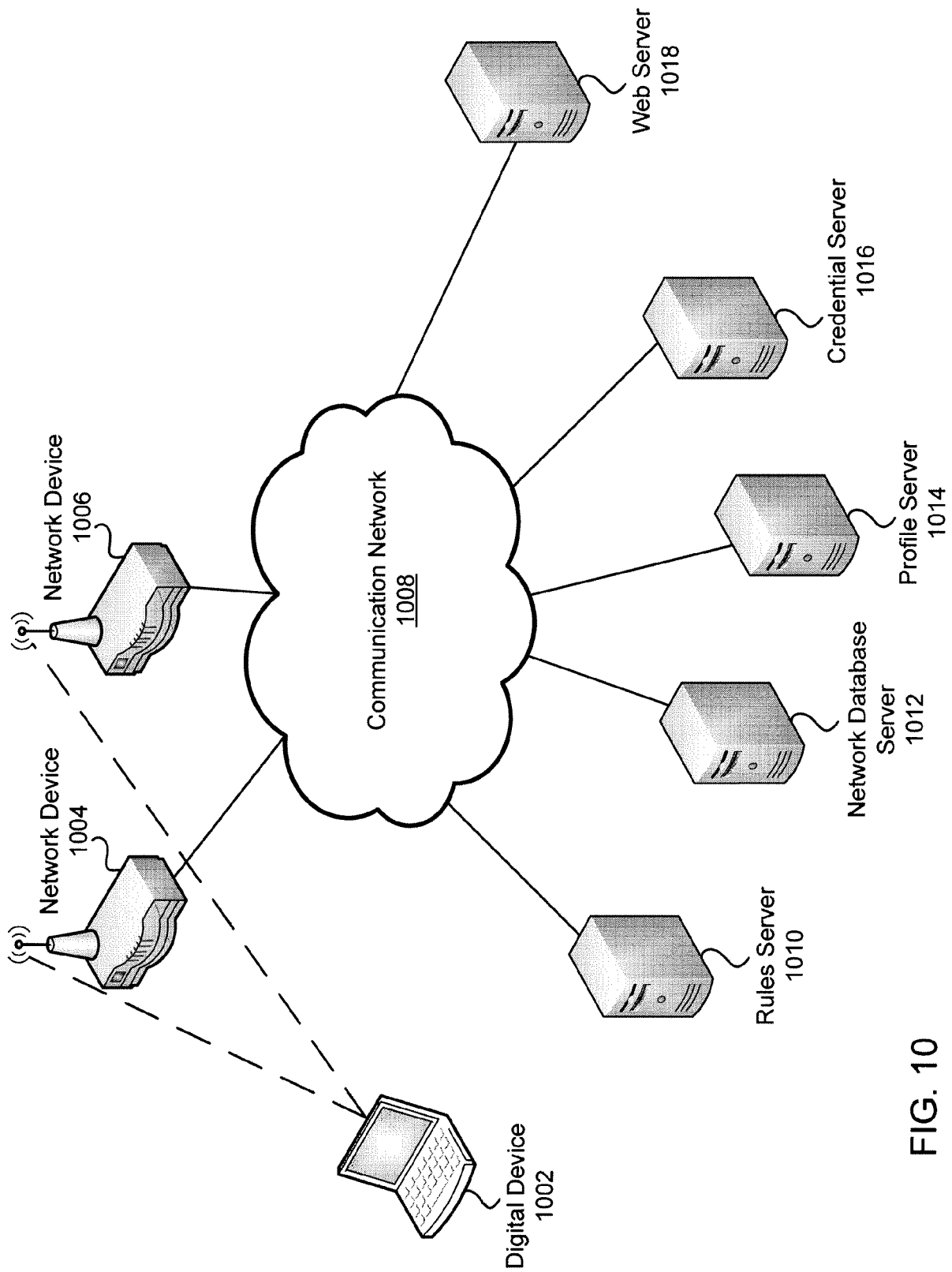


FIG. 10

11/13

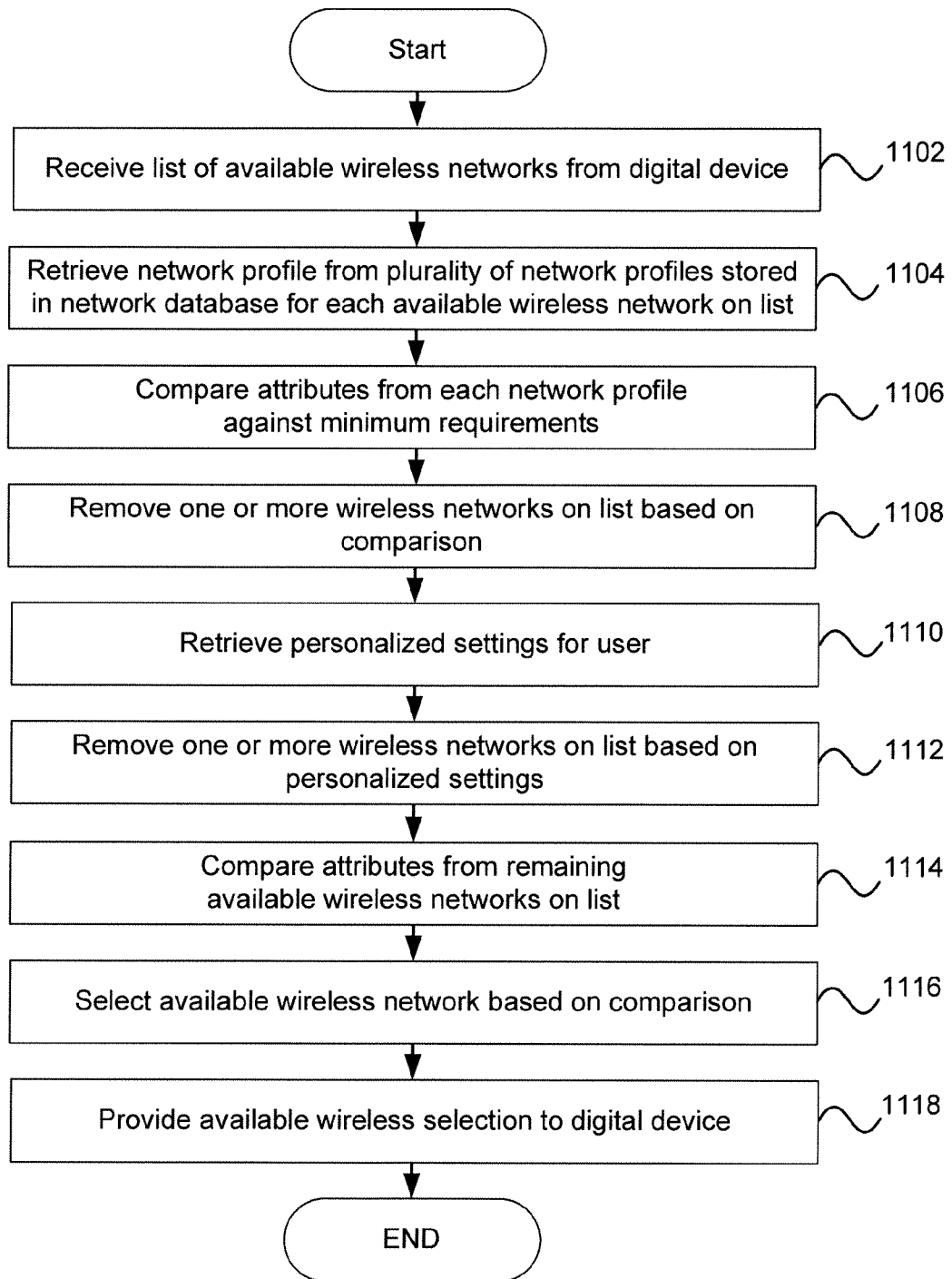


FIG. 11

12/13

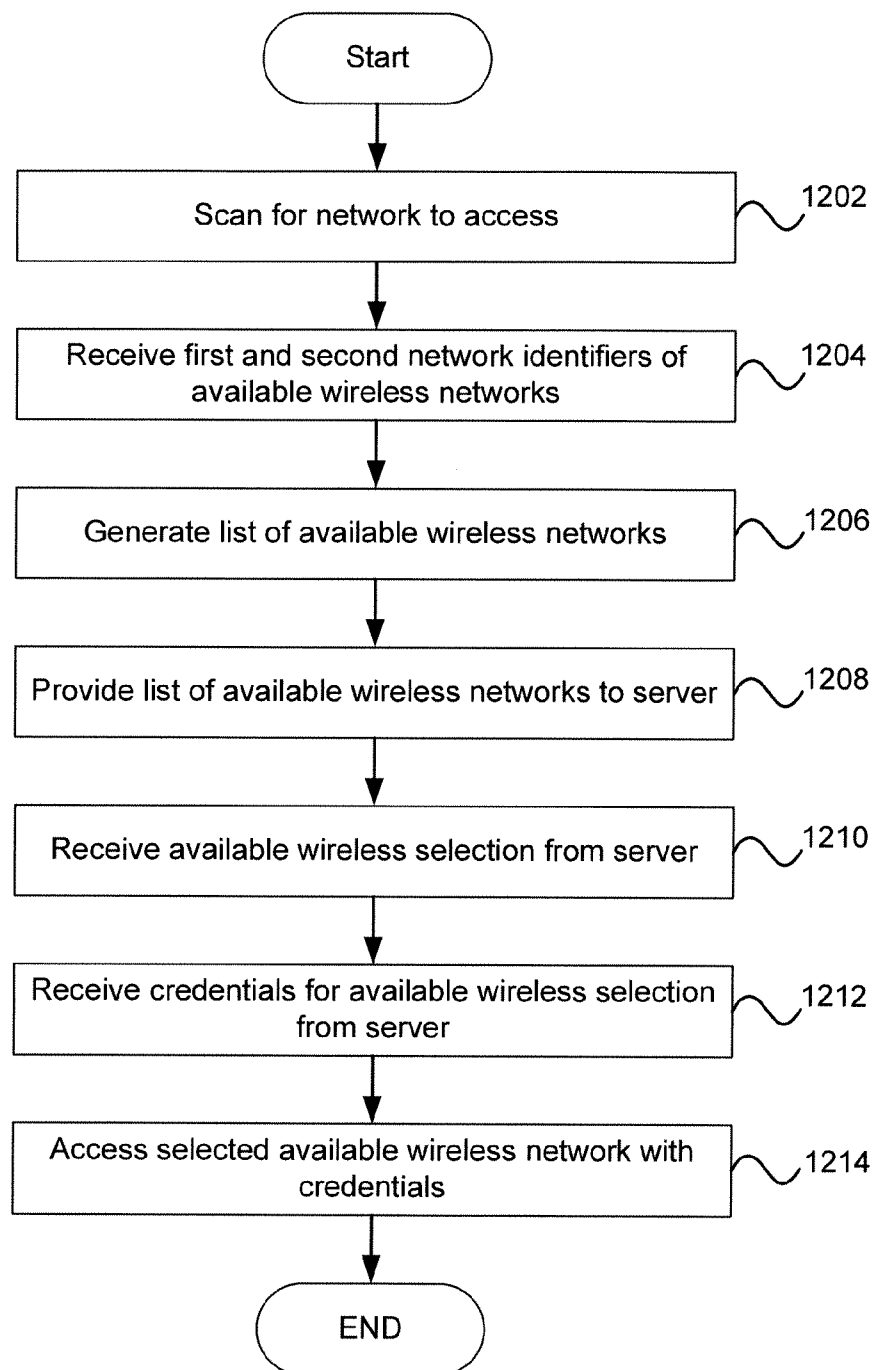


FIG. 12

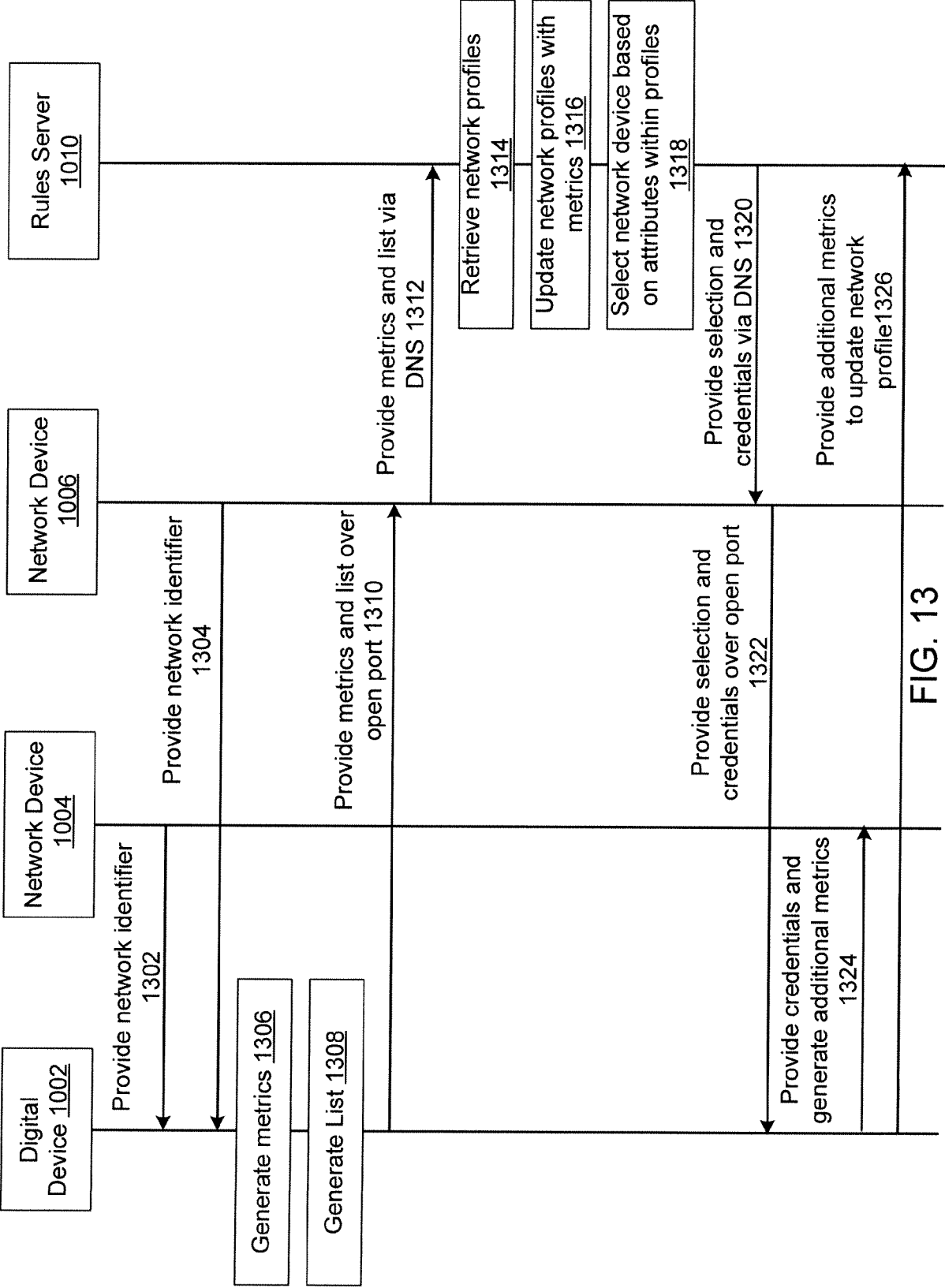


FIG. 13

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 08/78191

## A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - H04Q 7/20 (2008.04)

USPC - 455/432.3

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)

USPC - 455/432.3

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
USPC - 455/432.1-432.3, 434, 435.1, 435.2 -- see search terms below

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

DialogWEB; Google

Search Terms Used: wireless, network, identif, device, profile, select, digital, attribute, factor, preference, strength, cellular, compar, database, signal, credential, personaliz, setting

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2006/0221919 A1 (MCRAE et al.) 05 October 2006 (05.10.2006), Para [0005] - [0008], [0014], [0023], [0026], [0045]	1-5, 8-11, 13-15, 18-21 ----- 6, 7, 12, 16, 17
Y	US 6,799,038 B2 (GOPIKANTH) 28 September 2004 (28.09.2004), abstract, Col 7 Ins 16-19 and Ins 35-36, Col 8 Ins 56-59	6, 7, 12, 16, 17

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

\* 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

"&amp;" document member of the same patent family

Date of the actual completion of the international search

18 November 2008 (18.11.2008)

Date of mailing of the international search report

03 DEC 2008

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents  
P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-3201

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300  
PCT OSP: 571-272-7774