



(11)

EP 3 633 917 B1

(12)

EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention
of the grant of the patent:

06.10.2021 Bulletin 2021/40

(21) Application number: **19211911.3**

(22) Date of filing: **10.05.2013**

(51) Int Cl.:

H04W 12/08 ^(2021.01) **H04L 9/32** ^(2006.01)
H04W 12/041 ^(2021.01) **H04W 12/0431** ^(2021.01)
H04W 12/062 ^(2021.01) **H04W 12/069** ^(2021.01)
H04W 36/14 ^(2009.01) **H04W 36/00** ^(2009.01)
H04W 84/12 ^(2009.01)

(54) **EXTENDED SERVICE SET TRANSITIONS IN WIRELESS NETWORKS**

ERWEITERTE SERVICE-SET-ÜBERGÄNGE IN DRAHTLOSEN NETZWERKEN

TRANSITIONS D'UN ENSEMBLE DE SERVICES ÉTENDU DANS DES RÉSEAUX SANS FIL

(84) Designated Contracting States:

**AL AT BE BG CH CY CZ DE DK EE ES FI FR GB
GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO
PL PT RO RS SE SI SK SM TR**

(30) Priority: **11.05.2012 US 201213469618**

(43) Date of publication of application:

08.04.2020 Bulletin 2020/15

(62) Document number(s) of the earlier application(s) in
accordance with Art. 76 EPC:

13788377.3 / 2 850 775

(73) Proprietor: **BlackBerry Limited**

Waterloo, Ontario N2K 0A7 (CA)

(72) Inventors:

- **McCANN, Stephen**
Waterloo, Ontario N2K 0A7 (CA)

- **MONTEMURRO, Michael Peter**
Waterloo, Ontario N2K 0A7 (CA)

(74) Representative: **Hanna Moore + Curley**
Garryard House
25-26 Earlsfort Terrace
Dublin 2, D02 PX51 (IE)

(56) References cited:

EP-A1- 2 445 242 WO-A1-03/092218
US-A1- 2010 271 978 US-A1- 2011 047 382
US-A1- 2012 116 886

- **Konstantinos Georgantas: "Fast Initial
Authentication, a New Mechanism to Enable Fast
WLAN Mobility", , 26 September 2011
(2011-09-26), XP055663146, Retrieved from the
Internet:
URL:<https://www.cs.helsinki.fi/u/gurtov/papers/Georgantas-thesis-for-archive.pdf>
[retrieved on 2020-01-29]**

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 3 633 917 B1

Description**BACKGROUND**

[0001] Wireless network deployments, such as wireless local area networks ("WLANs"), allow mobile devices to access network and Internet services when within proximity of wireless communication signals of those wireless networks. Through network discovery communications with the WLAN, a mobile device or station ("STA") may obtain network information about an access point ("AP") or access network. Access Network Query Protocol ("ANQP") may allow a STA to request additional network information prior to establishing network connectivity. Such network information may include access to particular subscription service provider ("SSP") networks ("SSPN"), roaming agreements to allow connections from wireless clients associated with different SSPs, authentication capabilities to enable secure communications, support for emergency services or support for particular types of multi-media access (e.g., audio and/or video streaming, downloading, etc.). However, there is no expedited process for a mobile device to transition between networks. A mobile device may need to disconnect or disassociate with one network and authenticate/associate with a different network for the transition.

[0002] "Fast Initial Authentication, a new Mechanism to enable Fast WLAN Mobility" discloses an architecture for seamless handovers within a single Extended Service Set, ESS, network.

[0003] EP 2 445 242 A1 discloses an authentication method which includes redirecting a HTTP request message sent by a WLAN terminal to an address of a login webpage of a WLAN network, and returning the redirected HTTP request message to the WLAN terminal.

SUMMARY

[0004] The invention is defined in the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS**[0005]**

Figure 1 illustrates a communication network;
 Figure 2 illustrates a communication layer architecture;
 Figure 3 illustrates an alternative communication network;
 Figure 4 illustrates another alternative communication network;
 Figure 5 illustrates a mobile device ("STA");
 Figure 6 illustrates an access point;
 Figure 7 illustrates key authentication;
 Figure 8 illustrates device authentication;
 Figure 9 illustrates key generation;
 Figure 10 illustrates a process for generating and utilizing a key; and

Figure 11 illustrates another process for generating and utilizing a key for transitioning between ESS networks.

5 DETAILED DESCRIPTION

[0006] The disclosed systems and methods allow mobile devices to transition between networks. The transition may occur seamlessly, such that a consumer never loses the network connection despite transitioning between networks. The communication for enabling a transition may comprise discovery information about a network prior to association with that network. This pre-association communication may be retrieved through a wireless protocol, such as Access Network Query Protocol ("ANQP"), which allows a mobile device to retrieve information about a network prior to associating with that network. Communications prior to network association may be referred to discovery communications (i.e., communications that occur while a mobile device is in a pre-associated state). ANQP may allow a device to retrieve additional network information that can be used for transitioning between networks.

[0007] The seamless transition may be enabled through the creation and utilization of a central key holder authority that works across IEEE 802.11 Extended Service Sets ("ESSs"). The identity of the central key holder (i.e. key holder identity) may be advertised to an IEEE 802.11 mobile device in a pre-associated state. In other words, the key holder identity may be communicated with discovery communications, such as through ANQP messaging. The mobile device can use the key discovery communication along with a key generation method to assist the authentication and/or association with a network and whilst transitioning from one ESS to another.

[0008] There may be a common root key ("K") across ESSs. At each new access point ("AP") that the mobile device encounters, ESS and key holder identities may be discovered through discovery communications, including those available in neighboring APs. This information is available to the mobile device in a pre-associated state. A new IEEE 802.11 network layer key hierarchy that produces the common root key K across ESSs may allow fast authenticated ESS transitions for a mobile device.

[0009] The transitioning between networks and ESSs may be especially needed in an environment where mobile users are frequently entering and leaving the coverage area of an ESS. Every time the mobile device enters an ESS, the mobile device may do an initial link setup to establish wireless local area network ("WLAN") connectivity. With the current IEEE 802.11 specification, initial authentication for a high number of users entering an ESS, may result in signaling overload in an authentication server. This may result in the local hotspot (e.g. an environment that is within communication range of WLAN signals) becoming exhausted of memory. For example, IEEE 802.11r provides a solution to allow a mobile device

to transition between Basic Service Sets ("BSSs"), within the same mobility domain that restricts them to a single network (e.g. ESS). This may be equivalent to a mobile device moving from one WLAN to another, while remaining with the same network. The architecture of this IEEE 802.11 solution does not allow it to be scaled from local network (e.g. BSS) transition to network (e.g. ESS) transition, as the identity of the BSS is delivered in a different manner from that of the ESS. In addition, IEEE 802.11r assumes that security keys have a security association within a single ESS, to enable local network (e.g. BSS) transition.

[0010] A basic service set ("BSS") may be a set of stations ("STAs") that can communicate with each other. Each access point and its wireless devices may be known as a BSS. The BSS may include a STAs that have successfully synchronized using the JOIN service primitives and one STA that has used the START primitive. Membership in a BSS may not imply that wireless communication with all other members of the BSS is possible. According to the IEEE 802.11 standard a STA may be a mobile device, an access point "AP" or a mesh device "MSTA". Although not specified, the messages and protocols described below may be bi-directional and can flow from a mobile device to an AP and vice-versa. In infrastructure mode, a single AP together with all associated STAs is called a BSS. Every BSS has an identification (ID) called the BSSID, which may be the MAC address of the AP servicing the BSS. The simplest BSS may include one AP and one STA. There may be two types of BSS: 1) independent BSS (also referred to as IBSS); and 2) infrastructure BSS. An independent BSS ("IBSS") may be an ad-hoc network of STAs that contains no APs, which means they may not connect to any other basic service set.

[0011] A common distribution system ("DS") and two or more BSSs may create an extended service set ("ESS"). The ESS may be a set of one or more interconnected BSSs and integrated local area networks that appear as a single BSS to the logical link control layer at any STA associated with one of those BSSs. APs in an ESS are connected by a distribution system. The APs communicate amongst themselves to forward traffic from one BSS to another to facilitate movement of STAs between BSSs through the distribution system. The distribution system is the backbone of the wireless LAN and may be constructed of either a wired LAN or wireless network. The distribution system is a thin layer in each AP that determines the destination for traffic received from a BSS. The distribution system determines if traffic should be relayed back to a destination in the same BSS, forwarded on the distribution system to another AP, or sent into the wired network to a destination not in the extended service set. Communications received by an AP from the distribution system are transmitted to the BSS to be received by the destination mobile device.

[0012] Network equipment outside of the extended service set views the ESS and all of its STAs as a single

MAC-layer network where all STAs are physically stationary. Thus, the ESS "hides" the mobility of the mobile devices from everything outside the ESS. In other words, components outside of the ESS need not be aware of or informed about the mobility of the mobile devices within the ESS. This level of indirection provided by the IEEE 802.11 architecture allows existing network protocols that have no concept of mobility to operate correctly with a wireless LAN where there is mobility. With ESS, the entire network may appear as an independent basic service set ("IBSS") to the Logical Link Control layer ("LLC"). Accordingly, STAs within the ESS may communicate or even move between BSSs transparently to the LLC. Each BSS may have an identity ("ID") called a service set identity ("SSID") which is a 32-byte (maximum) character string. As described below, the transition between networks may include a transition between ESSs through the use of a common root key ("K") that is transmitted during discovery communications. Also as described below, there may be an Extended Authentication Server ("EAS") that acts as a key holder for advertising the keys during discovery communications.

[0013] Mobile devices that communicate prior to network association and transition between networks (e.g. ESSs) may include mobile communication devices, mobile computing devices, or any other device capable of communicating wirelessly with a wireless network. Such devices may also be referred to as terminals, wireless terminals, mobile devices, stations ("STA") or user equipment, and may also include mobile smart phones (e.g., a BlackBerry® smart phone or BlackBerry® Playbook), wireless personal digital assistants ("PDA"), machine to machine equipment, equipment within a smart grid ("SmartGrid"), equipment within a mesh network (an ad-hoc or peer network), laptop/notebook/netbook computers with wireless adapters, etc.

[0014] Some mobile devices may transition between ESS networks, which may include a wireless local area network ("WLAN"). Network discovery and connectivity in a WLAN may occur through standards that define access, control and communications in networks, such as the communication standard known as IEEE@ (Institute for Electrical and Electronics Engineers) 802.11, which, among other things, includes features describing "interworking with external networks." The "interworking" standard may be part of the IEEE 802.11-2012 base standard, and was formerly part of the amendment document IEEE 802.11u. Alternatively, the network discovery and connectivity may be subject to other parts of the IEEE 802.11 standard and other wireless communication standards including WLAN standards including any IEEE@ 802.xx standard (e.g. IEEE 802.15, IEEE 802.16, IEEE 802.19, IEEE 802.20, and IEEE 802.22), personal area network standards, wide area network standards, or cellular communication standards.

[0015] One exemplary network may be a WLAN and is described below. Alternatively, the devices may discover information about other networks through other

protocols and architectures, including a cellular network or a WiMax network. The network may comprise a publicly accessible network, such as the Internet, a private network, such as an intranet, or combinations thereof, and may utilize a variety of networking protocols now available or later developed including, but not limited to TCP/IP based networking protocols. The networks may include any communication method or employ any form of machine-readable media for communicating information from one device to another.

[0016] The transition between networks through discovery communications may be implemented in many environments providing WLAN access for network connectivity or in WLAN access locations or environments in which it may be expected that one or more users carrying respective mobile devices will associate with (i.e., join or connect to) and disassociate from a wireless network, AP, or WLAN as they enter and exit the WLAN access locations or environments.

[0017] In a WLAN environment, network discovery may include, for example, an active scan procedure or passive scan procedure performed by the mobile device. Typically, scanning procedures within a WLAN environment involve scanning for (i.e., determining) candidate STAs (e.g., mobile device, APs or mesh stations "MSTAs") with which the mobile device may associate with during an association procedure or re-associate with during a re-association procedure. In a passive scan procedure, a mobile device may "listen for" (i.e., receive or detect) beacon frames periodically transmitted from another STA (e.g., a mobile device, an AP or MSTAs). In an active scan procedure, the mobile device generates one or more probe request frames. A STA (e.g., a mobile device, an AP or MSTAs) that receives a probe request frame, in response, transmits a probe response frame. The mobile device then processes any received probe response frames.

[0018] In some WLAN environments, network discovery may further include an IEEE 802.11 authentication procedure. In other words, network discovery may include a successful authentication, an unsuccessful authentication, or a deauthentication of a mobile device with one of the STAs that were identified during the scanning procedure discussed above. Stated another way, network discovery may include: a transition of the mobile device from "State 1" to "State 2" based on a successful authentication of the mobile device; an unchanged state (i.e., remaining in "State 1") of the mobile device if authentication of the mobile device was unsuccessful; or a transition of the mobile device from "State 2" to "State 1" based on a deauthentication of the mobile device.

[0019] Some WLAN locations or environments may be known as "hotspots" in reference to a location or environment that is within communication range of WLAN signals. WLAN locations or environments may include coffee shops, retail stores, home locations (e.g. homes and apartments), educational facilities, office environments, airports, public transportation stations and vehi-

cles, hotels, etc. Such WLANs are often implemented as access networks that provide access to publicly accessible networks and may be associated with, or support access to, external networks (or WLAN-supported networks) owned and/or operated by subscription-based service providers. For example, an external network can be owned and/or operated by an Internet-access service provider or a telecommunications carrier/service provider that provides subscription-based Internet access for a fee (e.g., a monthly fee). In some systems, a subscriber/user may subscribe to such a service can use wireless network access and/or Internet-access services based on such a subscription when the subscriber is in communication proximity of the WLAN with an appropriate mobile device. In some instances, different WLANs may provide access to different types of network information. For example, some WLANs may provide access to particular subscription service provider networks, and some WLANs may support roaming agreements to allow connections from mobile devices associated with different SSPs.

[0020] During some network discovery processes a mobile device may transmit a query for certain network information from the wireless local area network ("WLAN"). The terminal may obtain network information made available by WLANs to determine, based on the network information, whether to continue with a connection process to associate with that network.

[0021] In accordance with the embodiments described herein, mobile devices may request network information from WLANs using an Access Network Query Protocol ("ANQP"). ANQP supports information retrieval from an Advertisement Server that supports a Generic Advertisement Service ("GAS"). ANQP and GAS are defined in IEEE® 802.11u™ and also IEEE® 802.11-2012™.

[0022] Generic Advertisement Service ("GAS") may serve as a transport mechanism, at layer-2 (see e.g. Figure 2), for an advertisement protocol such as ANQP. The advertisement protocol may connect the mobile device to one of several interworked servers. The advertisement protocol allows the transmission of frames between a mobile device and a server in the network prior to network connectivity. For example, GAS provides support for network selection by a mobile device as well as for communication between the mobile device and other information resources in the network before the mobile device associates with a WLAN. The mobile device may be connected to a layer-2 radio service, without exchanging any authentication parameters or without having a recognized session (because no session keys are established and no internet protocol "IP" address is assigned). When in compliance with the IEEE 802.11 standard, no data traffic is allowed in this state.

[0023] Other layer-2 transport mechanisms or even authentication mechanisms may be used. For example, the Extensible Authentication Protocol ("EAP") may be used to carry the advertisement protocol. The advertisement protocol information would be encapsulated within

a suitable EAP-TLV (type length value) method frame (or alternative EAP method frame) and transported by the EAP. Use of secure credentials exchanged during the EAP transactions would also provide a level of security for any information carried within the advertisement protocol. For example, if EAP-SIM (or EAP-AKA) were to be the authentication protocol, any advertisement protocol information encapsulated (i.e. securely carried) within a suitable EAP-TLV frame during the same EAP transaction may also be protected by the SIM credentials.

[0024] Access Network Query Protocol ("ANQP") is an advertisement protocol and operates as a query and response protocol used by a mobile device to discover a range of information from a server including accessible roaming partners internet protocol address type availability, and other metadata useful in the mobile device's network selection process. ANQP is capable of discovering information about hotspots or wireless networks, prior to the mobile device establishing network connectivity and associating with that network. In addition to being defined in IEEE® 802.11u, additional ANQP messages may alternatively or additionally be defined in the Wi-Fi Alliance ("WFA") Hotspot 2.0 (also referred to as Passpoint) specifications. These ANQP extensions within the WFA Hotspot 2.0 specifications may be referred to as Hotspot ("HS") 2.0 ANQP elements. Alternatively, other advertisement protocols (e.g., Registered Location Query Protocol "RLQP" as defined in IEEE® 802.11af and Hotspot Registration Protocol "HRP" as defined in Wi-Fi Alliance Hotspot 2.0) may also be used. ANQP provides one embodiment for communication with a WLAN at the network discovery stage without requiring an association with the WLAN. Network information that is communicated prior to network association (or at the network discovery stage) is discussed below. In alternative embodiments, other layer-2 transport mechanisms or even authentication mechanisms such as the Extensible Authentication Protocol (EAP) could be used to carry the ANQP messages. The ANQP message would be encapsulated within a suitable EAP-TLV method frame (or alternative EAP method frame) and transported by the EAP.

[0025] A network discovery exchange may involve a requesting STA querying another STA (e.g., a mobile device, an AP or MSTA) for network information. A WLAN AP (also referred to simply as an AP) is an entity that contains one STA and provides access to distribution services via a wireless medium for associated STAs. The queried or receiving STA (e.g., a mobile device, an AP or an MSTA) may respond to the received query with the requested information in a response. The queried or receiving terminal can provide the response information with or without proxying the query to a server in an external network (e.g., a subscription service provider ("SSP") network). For example, an external network connected to a queried WLAN may have certain network information accessible via the WLAN and of which a querying mobile device may be made aware. The network

discovery exchange or communications prior to network association may use ANQP or other query protocols too, just as information exchange services may be used alternatively.

[0026] Figure 1 illustrates a communication network 100. Network information may be communicated during network discovery using ANQP over the communications network 100. The communication network 100 includes a plurality of WLAN access locations 102a-c having respective access points ("APs") 104a-c that provide access to respective access networks 106a-c. The APs 104a-c are further described with respect to Figure 6. The access network A 106a provides access to an external network A 108a and the access network B 106b provides access to an external network B 108b. Unlike the access networks A 106a and B 106b that do not connect directly to the Internet 112, the access network C 110 may connect directly to a publicly accessible network like the Internet. Thus, the access network C 106c may be a public network, while the access networks A 106a and B 106b may be private networks. Any of the described networks may form part of an ESS.

[0027] In one embodiment, each of the external networks A 108a and B 108b may be a subscription service provider network ("SSPN") owned or operated by data subscription service providers, Internet subscription service providers, media (e.g., audio/video) subscription service providers, wireless communications subscription service providers, or any combination thereof. The external networks A 108a and B 108b are connected to the Internet 112 and may, for example, provide subscription-based Internet access to mobile device devices. In some implementations, roaming agreements between different subscription service providers may enable the external networks A 108a and B 108b to support roaming connections for mobile devices associated with other subscription service providers. In one embodiment, the external networks 108a-b are ESS networks. Alternatively, networks 106a-c may be ESS networks.

[0028] The WLAN access location 102a illustrates a mobile device 114 in wireless range of the access point ("AP") 104a. The mobile device 114 is further described with respect to Figure 5. The AP 104a connects with the access network A 106a, which may provide a direct or indirect connection to other networks, including publicly accessible network like the Internet 112. Prior to the mobile device 114 associating with the access network A 106a, mobile device 114 sends a discovery request 116 to the AP 104a. The AP 104a may respond with a discovery response 118. In alternative embodiments, the discovery request 116 may originate from the AP 104a and the discovery response 118 may be from the mobile device 114, such as with mesh, peer to peer, ad-hoc or Wi-Fi direct networks. The discovery request 116 or the discovery response 118 may include discovery communications 120. The discovery communications 120, also known as network information, discovery information, or network discovery information, may include information

about the network and/or device that is communicated between the device and the network prior to the device associating with the network. Accordingly, the discovery communications 120 may be referred to as pre-association communications or pre-association information. In one embodiment, the discovery communications 120 may be communicated using the ANQP protocol.

[0029] The discovery communications (request 116 and response 120) may be exchanged at a media access control ("MAC") sub-layer of a data link layer of the Open Systems Interconnection ("OSI") Reference Model without needing to use operations at or above an internet protocol ("IP") layer (i.e., a network layer) and without needing to otherwise provide access to the IP layer while discovering discovery communications 120. Discovering network information using messages exchanged at or above the network layer may require more processing power for a mobile device than implementing processes at the MAC sub-layer. The layers in which the discovery communication occurs are further illustrated in Figure 2.

[0030] Each of the APs 104a-c and the mobile device 114 may include a network adapter or network interface card that facilitates connections to a wireless medium. The network interface component may be referred to as a station ("STA"). Each of the access networks 106a-c and the external networks 108a-b may be associated with one or more ESSs and a key holder identifier may be provided to mobile devices 114 prior to the association with a network.

[0031] The mobile device 114 may associate with different APs (e.g., the APs 104a-c) based at least partially on the discovery communications 120 received regarding the available external networks. The mobile device 114 may receive information from the APs when moved in range of one of the WLAN access locations 102a-c, respectively. The information received may be discovery communications prior to association that include information about the particular BSS or ESS for the networks. The information received may be utilized when transitioning between networks.

[0032] Figure 2 illustrates a communication layer architecture 200. The communication layer architecture 200 includes seven layers which may be implemented in accordance with the Open Systems Interconnection ("OSI") Reference Model. The communication layer architecture 200 includes a data link layer 202, which includes a media access control ("MAC") sub-layer 204. Mobile devices (e.g., the mobile device 114 of Figure 1) may provide network information or discovery communications 120 (e.g. the discovery request 116 and the discovery response 118) with wireless access points (e.g., the APs 102a-c of Figure 1) at the MAC sub-layer 204. A mobile device may access information from a memory or other hardware of the mobile device at the MAC sub-layer 204 without needing to perform operations at or above an internet protocol layer (e.g., a network layer 208) and without needing to provide access to the internet protocol layer. Mobile devices (e.g., the mobile device

114 of Figure 1) that include mobile smart phones, PDA's, processor based devices, etc. may have relatively limited processor cycles and less available electrical power than fixed-location computing devices powered using wired (e.g. alternating current) electricity sources. Low-level resource operations at the MAC sub-layer require relatively fewer system resources than user-interface-intensive and operating system intensive operations (e.g., web-browser operations) at an application layer.

[0033] Some communications or authentication techniques that use hypertext transfer protocol ("HTTP") or other internet protocol processes may require establishing a connection between a mobile device and a wireless access point at one or more of the layers between and including the network layer 208 and an application layer 210 of the communication layer architecture 200. In these applications, discovery communications 120 may not require a connection or access to the network layer 208 or any layers within a protocol suite. An inclusion of a discovery communication 120 on the MAC sub-layer 204 may allow for a mobile device to communicate with a network without associating with the network.

[0034] Discovering network information available via access points using the MAC sub-layer may be used for identifying the BSS and/or ESS associated with a particular AP. As described below in Figures 3-4, the ESS information may be used by a mobile device to transition seamlessly between different networks associated with different ESSs. The discovery communications 120 may indicate whether a particular network (e.g., a SSPN) has the extended capability for improved transitions between ESS networks. An indication of that capability may be a particular bit added to the Extended Capability information element ("IE") that indicates the ability to utilize a key K for faster transitions between ESS networks. As described below, the particular bit may be referred to as a Fast Initial Link Setup ("FILS") bit and may be a part of discovery communications prior to association. The FILS bit may indicate whether the extended capability for expedited transitions is possible. Further, the discovery communications may include a key holder identifier that is advertised to mobile devices to allow those terminals to determine when ESS networks have access to the same key. The key may be derived at the mobile device through an algorithm which eliminates the need to transmit the key.

[0035] Figure 3 illustrates an alternative communication network 300. In particular, the network 300 illustrates the communication between the mobile device 114, the AP 104, and an ESS network 305. An Extended Authentication Server ("EAS") 302 may be the key holder that provides the key identification to be used, by the AP 104, during pre-association communications. The EAS 302 may be implemented as hardware and/or software. In one embodiment, the EAS 302 may be an additional hardware device that communicates with the ESS network 305. Alternatively, the EAS 302 may be software that runs on existing hardware in communication with the

ESS network 305. Exemplary existing hardware that may operate as the EAS 302 may include a maintenance server and/or a billing server that are configured (through software) to act as the EAS 302. The EAS 302 may be an authentication mechanism that covers multiple networks over a large area. For example, an EAS 302 may cover a small city or county. The ESS network 305 may advertise, via the AP 104, the EAS 302 to the mobile devices 114 that the ESS network 305 is associated with. In particular, as the EAS 302 may be the key holder, its identity, referred to as " K_{ID} ", may be advertised or broadcast.

[0036] Upon initial entry into the network 305, the mobile device 114 discovers the identity of a key holder " K_{ID} " from AP 104 (as advertised by the AP 104 in pre-association communications) together with identity of the ESS itself. The K_{ID} may be implemented to identify the K key holder, which is the EAS 302 in the example shown in Figure 3. AP 104 may advertise or broadcast (to mobile devices, such as the mobile device 114) the identity of the K key holder K_{ID} . A new ANQP-message or field may be utilized to allow advertisement of the K_{ID} . Once the mobile device 114 detects the Fast Initial Link Setup ("FILS") bit within the broadcasted Extended Capabilities IE from the AP, the mobile device 114 may then retrieve the K_{ID} using this new ANQP-message or field.

[0037] The K_{ID} may be the address of the EAS and may also be referred to as the Fast Initial Link Setup ("FILS") identity. FILS may refer to mechanisms for improving the initialization and association of devices with wireless networks. In this case, the transition between networks is fast and seamless because of the key identification. In particular, if the ESS 305 is the network that the mobile device 114 wishes to connect to, a "K" key security association is established between the mobile device 114 and the EAS 305 by an authentication sequence (examples of which are described with respect to Figures 7-8).

[0038] At each new AP 104 that the mobile device 114 encounters, ESS 305 and key holder identities may be discovered through discovery communications (e.g. using a new ANQP-message or field). A new ESS level key ("K") is created at the ESS (network) level and may then be used as a symmetric key between the mobile device 114 and the EAS 302 that the mobile device 114 connects to. The K key may be derived from the IEEE 802.11u HESSID identifier used to identify homogeneous ESSs (e.g. ESSs that share some sort of relationship). The K key may also be derived by an authentication sequence between the mobile device 114 and the EAS 302, with the IEEE 802.11u HESSID being used to identify the EAS 302 in one example. An existing IEEE 802.11 parameter such as the HESSID (or FQDN or other new network identifier) may be used to carry the K_{ID} parameter. Once the mobile device 114 detects the FILS bit within the broadcast Extended Capabilities IE from the AP, the mobile device 114 may directly use the HESSID parameter. The HESSID parameter and FILS bit may also broadcast

from the AP. If the HESSID is not being used as the K_{ID} , then another ANQP-message may be used to retrieve it.

[0039] The EAS 305 maintains the K key and the K_{ID} (the address of the EAS) becomes the identity of the K key holder. As described, the AP 104 advertises (through discovery communications) the K_{ID} before association with the network. Mobile devices may then utilize the K_{ID} information that is transmitted before network association to transition between networks with the same K_{ID} .

[0040] Extended authentication request and response messages may be generated to allow the K key to be transported from the device to an AP, to allow a more efficient authentication mechanism when transitioning from one ESS to another. The extended messages may include an extra bit that is added to the advertised Extended Capability information element ("IE"). The extra bit may indicate that ESS transitioning using the K key is enabled. The Extended Capability IE may be returned to a mobile device by an AP in a probe response with a single bit set within this IE to indicate ESS transitioning support.

[0041] Figure 4 illustrates another alternative communication network. In particular, Figure 4 shows that the mobile device 114 can use the K key to perform an expedited authentication (e.g. a Fast Initial Link Setup "FILS") with another access point AP2 that is connected to a different ESS network (ESS2), advertising the same K_{ID} (i.e. the address of the same EAS 302 as shown in Figure 3). The expedited authentication may be beneficial as it is faster than conventional authentication, due to the fact that the presence of the K key and K_{ID} implies an existing security association between the mobile device 114 and the access network AP2. In other words, assuming that the mobile device 114 has previously connected with the first access network AP1, the mobile device 114 will know the K_{ID} and have already established a security association with the EAS with the K key. Then, if the mobile device 114 has discovery communications (pre-association) with the second access point AP2, the K_{ID} will be transmitted to the mobile device 114 during the discovery communications. Since the EAS 302 and K key cover both the ESS 1 and ESS2 networks, the mobile device 114 can quickly transition to the second access point AP2 network because of the prior security association. The EAS 302 providing the K_{ID} and the K key association with the mobile device 114 allows for fast transitions between any ESS networks associated with that EAS 302.

[0042] Figure 5 illustrates a mobile device 114 as shown in Figures 1, 3, and 4. The mobile device 114 includes a processor 502 that may be used to control the overall operation of the mobile device 114. The processor 502 may be implemented using a controller, a general purpose processor, a digital signal processor, dedicated hardware, or any combination thereof. The processor 502 may include a central processing unit, a graphics processing unit, a digital signal processor or other type of processing device. The processor 502 may be a com-

ponent in any one of a variety of systems. For example, the processor 502 may be part of a standard personal computer or a workstation. The processor 502 may be one or more general processors, digital signal processors, application specific integrated circuits, field programmable gate arrays, servers, networks, digital circuits, analog circuits, combinations thereof, or other now known or later developed devices for analyzing and processing data. The processor 502 may operate in conjunction with a software program, such as code generated manually (i.e., programmed).

[0043] The mobile device 114 also includes a terminal message generator 504 and a terminal data parser 506. The terminal message generator 504 may generate network information discovery messages such as the discovery request 116 and discover response 118 for communicating the network information 120 from Figure 1. The terminal data parser 506 may be used to retrieve network information from memory (e.g., random access memory 510, etc.). For example, the terminal data parser 506 may retrieve network information 120 that is cached in the mobile device 114 after receipt from a WLAN (e.g., the access networks 106a-c of Figure 1).

[0044] In the illustrated embodiment, the terminal message generator 504 and the terminal data parser 506 are shown as separate from and connected to the processor 502. In alternative embodiments, the terminal message generator 504 and the terminal data parser 506 may be implemented in the processor 502 and/or in a wireless communication subsystem (e.g., a wireless communication subsystem 518). The terminal message generator 504 and the terminal data parser 506 may be implemented using any combination of hardware, firmware, and/or software. For example, one or more integrated circuits, discrete semiconductor components, and/or passive electronic components may be used. For example, the terminal message generator 504 and the terminal data parser 506, or parts thereof, may be implemented using one or more circuits, programmable processors, application specific integrated circuits, programmable logic devices, field programmable logic devices, etc.

[0045] The terminal message generator 504 and the terminal data parser 506, or parts thereof, may be implemented using instructions, code, and/or other software and/or firmware, etc. stored on a machine accessible medium and executable by, for example, a processor (e.g., the processor 502). The terminal message generator 504 or the terminal data parser 506 may be stored on or include a tangible storage medium or memory. For example, the terminal message generator 504 or the terminal data parser 506 may be implemented in software stored on a memory that is executable by the processor 502. Alternatively, the terminal message generator 504 and/or the terminal data parser 506 may be implemented in hardware with software functions. The memory for storing software associated with the terminal message generator 504 and/or the terminal data parser 506 may include, but is not limited to, computer readable storage

media such as various types of volatile and non-volatile storage media, including random access memory, read-only memory, programmable read-only memory, electrically programmable read-only memory, electrically erasable read-only memory, flash memory, magnetic tape or disk, optical media and the like. In one embodiment, the memory may include the random access memory 510 for the processor 502, or may be an external storage device or database for storing recorded ad or user data. Examples include a hard drive, compact disc ("CD"), digital video disc ("DVD"), memory card, memory stick, floppy disc, universal serial bus ("USB") memory device, or any other device operative to store user data. The memory is operable to store instructions executable by the processor 502.

[0046] The mobile device 114 may include a FLASH memory 508, a random access memory 510, and/or an expandable memory interface 512 coupled with the processor 502. The FLASH memory 508 may store computer readable instructions and/or data. In some embodiments, the FLASH memory 508 and/or the RAM 510 may store the network information 120 from Figure 1 and instructions for communicating that network information 120. The processor 502 may be coupled with the memory (e.g. the FLASH memory 508, or the RAM 510) for storing software instructions executable by the processor 502. The memory may include, but is not limited to, computer readable storage media such as various types of volatile and non-volatile storage media, including random access memory, read-only memory, programmable read-only memory, electrically programmable read-only memory, electrically erasable read-only memory, flash memory, magnetic tape or disk, optical media and the like. The functions, acts or tasks illustrated in the figures or described herein may be performed by the programmed processor 502 executing the instructions stored in the memory. The functions, acts or tasks are independent of the particular type of instruction set, storage media, processor or processing strategy and may be performed by software, hardware, integrated circuits, firm-ware, micro-code and the like, operating alone or in combination. Likewise, processing strategies may include multiprocessing, multitasking, parallel processing and the like.

[0047] The mobile device 114 may include a security hardware interface 514 to receive a SIM card from a wireless service provider. A SIM card may be used for network discovery communications including authentication of the mobile device 114 for establishing a connection with a WLAN-supported network. The mobile device 114 may be provided with an external data I/O interface 516. The external data I/O interface 516 may be used by a user to transfer information to the mobile device 114 through a wired medium.

[0048] The mobile device 114 may include wireless communication subsystem 518 to enable wireless communications with access points (e.g., the APs 104a-c of Figure 1). Although not shown, the mobile device 114 may also have a long-range communication subsystem

to receive messages from, and send messages to, a cellular wireless network. In the illustrated examples described herein, the wireless communication subsystem 518 can be configured in accordance with the IEEE@ 802.11 standard. In other example implementations, the wireless communication subsystem 518 may be implemented using a BLUETOOTH® radio, a ZIGBEE® device, a wireless USB device, an ultra-wideband radio, a Near Field Communications ("NFC") device, or a Radio Frequency Identifier ("RFID") device.

[0049] The mobile device 114 may include a user interface for communicating with the mobile device. The user interface may be separate component or it may include a speaker 520, a microphone 522, a display 524, and a user input interface 526. The display 524 may be a liquid crystal display, an organic light emitting diode, a flat panel display, a solid state display, a cathode ray tube, a projector, a printer or other now known or later developed display device for outputting determined information. The user input interface 526 may include alphanumeric keyboard and/or telephone-type keypad, a multi-direction actuator or roller wheel with dynamic button pressing capability, a touch panel, etc. The network discovery information that is communicated with a network prior to connection may be communicated with or without each of the user interfaces described herein. The speaker, 520, the microphone 522, the display 524, the user input interface 526, and/or any combination thereof may be omitted in alternative embodiments. In one embodiment, the mobile device 114 is a battery-powered device and includes a battery 528 and a battery interface 530.

[0050] Figure 6 illustrates an access point ("AP") 104a. The access point shown in Figure 6 is AP 104a, but may also be illustrative of other access points (e.g. APs 104b, 104c). AP 104a includes a processor 602 to perform operations of the AP 104a. The processor 602 may be similar to the processor 502 described above.

[0051] The AP 104a includes an access point message generator 604 to generate network information communications and an access point data parser 606 for retrieving network information communications from the mobile device 114 and/or the external network A 108a as illustrated in Figure 1. The access point message generator 604 may be similar to the terminal message generator 504 of Figure 5, and the access point data parser 606 may be similar to the terminal data parser 506 of Figure 5. As with the terminal message generator 504 and the terminal data parser 506 of Figure 5, the access point message generator 604 and the access point data parser 606 may be implemented in software stored on a memory that is executable by the processor 602 or may be implemented in hardware with software functions executed by the processor 602. Alternatively, the access point message generator 604 and the access point data parser 606 may be implemented in a wireless communication subsystem (e.g., a wireless communication subsystem 612) using any combination of hardware, firmware,

and/or software including instructions stored on a tangible computer readable medium and/or a non-transitory computer readable medium.

[0052] The AP 104a may also include a FLASH memory 608 and a RAM 610, both of which are coupled to the processor 602. The FLASH memory 608 and/or the random access memory ("RAM") 610 may be configured to store network information (e.g., network information 120 including discovery communications from Figure 1). The RAM 610 may also be used to generate messages for communication with the mobile device 114 and/or to the external network A 108a. The RAM 610 may also store received messages communicated by the mobile device 114 and/or the external network A 108a.

[0053] To communicate with mobile devices such as the mobile device 114, the AP 104a may include a wireless communication subsystem 612, which may be similar to the wireless communication subsystem 518 of the mobile device 114 illustrated in Figure 5. To communicate with a WLAN-supported network or external network (e.g., the networks 106a-c, 108a, and 108b of Figure 1), the AP 104a may include a network uplink communication interface 614.

[0054] Figure 7 illustrates key authentication. In particular, Figure 7 shows an example initial authentication sequence where the ESS (network) level K key is derived between a mobile device and an EAS. In one embodiment, the K_{ID} may have no relationship to the K key itself. The K key may be derived using a pseudo-random function (e.g. the IEEE 802.11r KDF) based on a hash of elements that may include the mobile identity (MAC address), the EAS Identity, a mutually derived key based on the result of mutual authentication during the initial association process, supplicant Nonce "SNonce" (e.g. from the mobile device), authenticator Nonce "ANonce" (e.g. from the EAS), and the SSID of the ESS where the mobile initially connected. A Nonce may be a random number that is not repeated, such as the date and time.

[0055] In message 702, the advertisement of the ESS identity and the EAS identity (K_{ID}) provides the mobile device 114 with parameters that are related to the network to which the AP is connected. The advertisement may be performed during discovery communications while the mobile device 114 is in a pre-associated state. In block 704, an authentication request is sent from the mobile device 114 to the EAS 302. The authentication request may include the K_{ID} along with an SNonce variable. In message 706, the authentication response is sent to the mobile device 114 from the EAS 302. The authentication response may include the K_{ID} along with an ANonce variable. In message 708, an association message exchange may occur. The association message exchange may occur between the mobile device 114 and the EAS 302 resulting in the generation of the key K value. In one embodiment, the key K is not transmitted for security reasons, rather the key K is generated (e.g. derived or calculated) mutually by the mobile device 114 and the EAS 302. In another embodiment, the key

K is not transmitted for security reasons, rather the key K is generated asymmetrically by the EAS 302 using an identity of the mobile device 114. In another embodiment, the K key has a lifetime. When the lifetime of K expires, the mobile device may re-run the initial authentication sequence (with the same EAS 302 or a new EAS) to generate a new K key. This new K key will be different from the old one, as SNonce and ANonce have different values.

[0056] Figure 8 illustrates device authentication. As illustrated in Figure 8, the messages may be related to the expedited transition and authentication of the mobile device 114 with a second access point 104 and a second ESS network after previously authenticating with a first access point 104 and a first ESS network associated with the same EAS 302. In other words, Figure 8 illustrates the communications between the EAS 302, ESS Network 2, AP2, and the mobile device 114 as illustrated in Figure 4.

[0057] The messages in Figure 8 include an initialization message 802 between the access point 104 and the EAS 302. The initialization message 802 may allow the AP to have both the K key and K_{ID} , before the mobile device 114 comes into radio range of the ESS network. It is also possible to split this message into two parts so that the K_{ID} can be delivered to AP 104 at system initiation, and then the K key may be delivered once it has been derived as the mobile device enters the ESS network range. Accordingly, the K_{ID} can be advertised to the mobile devices 114 from the AP 104 through the advertisement message 804. The advertisement message 804 may be performed using a probe request or a probe response between the mobile device 114 and the AP 104. Alternatively, ANQP messages may be sent from the mobile device 114 to the AP 104. In this message the identity of the ESS to which the AP 104 is connected (ESS) and the identity of the K Key holder (K_{ID}) may be transmitted to the mobile device 114. The mobile device 114 receives the ESS and/or K_{ID} and knows whether an expedited authentication is possible. In particular, if the mobile device 114 has already authentication with the same K_{ID} , then expedited authentication is possible for the other ESSs associated with that key holder (i.e. the EAS is the same). The expedited authentication sequence 806 may then occur. The authentication sequence may take place between the mobile device 114 and the access point 104. The EAS may need to pass the key K to the access point 104, prior to the initial authentication sequence.

[0058] Figure 9 illustrates key generation 901. In particular, the key generation 901 may occur at the individual devices (e.g. the mobile device 114 and the EAS 302) so that the key K does not need to be communicated. The local key generation 901 may be performed through an algorithm that utilizes certain information, such as the K_{ID} and appropriate Nonces, to generate the key K. The generation of the K key may result from a symmetrical algorithm operating between individual devices (mu-

tual) or an asymmetric algorithm operating in one device only. The key generation 901 may include network level K key 902, certificate based K key 904, and/or Kerberos ticket K key 906.

[0059] The certificate based K key 904 may be derived from a certificate delivered by a Root Certificate Authority that has a trust relationship with the mobile device and the EAS. The type of certificate may be insignificant. In this case, the mobile device 114 may have to perform an initial out of band ("OOB") enrolment protocol with the EAS (potentially using GAS or some other protocol) to initialize its certificate. Each access point may also have a certificate derived from the same Root Certificate Authority. An alternative is that a manufacturer's certificate may be used, although this may be difficult to revoke if the security of the mobile device is compromised. Once the mobile device 114 has a certificate, either an asymmetric or symmetric algorithm (e.g. Diffie-Hellman) exchange may be used between it and the EAS to derive a public/private K key pair, which is used for authentication as the mobile device 114 moves between ESSs. The lifetime of the derived private key may be difficult to manage when using a certificate based K key 904.

[0060] The Kerberos ticket K Key 906 may be derived when the mobile device 114 authenticates with an initial ESS for the first time. The K key itself may not be passed over the air. Rather mathematical parameters which allow the K key to be derived may be passed. Although, this initial transaction may be rather slow, subsequent transactions may be much faster. An exemplary process for a mobile device 114 may include: 1) an initial login using IEEE 802.1X (authenticate); 2) obtaining a Kerberos ticket (enrollment process); 3) re-authenticate (when necessary) to a new hotspot using the Kerberos ticket; and 4) perform an online signup to establish more permanent credentials. Kerberos tickets may be time limited, for example, to only multiple hours. If the Kerberos Server is located on the same realm (advertised by K_{ID}) as the EAS (see Figure 4), then the mobile device 114 may perform expedited authentication and association as it transitions between each ESS.

[0061] Figure 10 illustrates a process for generating and utilizing a key for transitioning between ESS networks. In block 1002, a mobile device may receive an advertisement of a key holder identity K_{ID} from a particular network. The key holder may be an EAS that provides the key holder identity to a number of ESS networks. The advertisement may be a discovery communication prior to network association and may be an ANQP communication. In block 1004, the mobile device may connect with or associate with a first ESS network associated with the EAS. The association may include an authentication process in which the mobile device is authenticated to access the network. When within range of a second ESS network, the device may receive an advertisement from the second ESS network that includes the same key holder identity K_{ID} that was advertised from the first ESS network as in block 1006. The receipt of the

advertisement from the second ESS network may occur after the mobile device has left the first ESS network, or it may occur while the mobile device is still associated with the first ESS network. The advertisements of the key holder identity K_{ID} may include an identifier of the particular ESS network (e.g. ESS1 or ESS2).

[0062] Since the mobile device has already authenticated with a related ESS network (ESS1, which is related because of the common security association with EAS), there may be an abbreviated or expedited authentication. This expedited authentication process may also be referred to as a seamless or expedited transition between ESS networks. In block 1008, the key K may be derived on the mobile device as described with respect to Figure 9. Once the K key is derived, the mobile device may transition from the first ESS network to the second ESS network.

[0063] Figure 11 illustrates another process for generating and utilizing a key for transitioning between ESS networks. In block 1102, the key may be generated. As described above, the key may be generated at the mobile device and/or the EAS without passing the key over a network. In block 1104, a key holder identifier K_{ID} that is used to identify the key holder may be generated. As described, the K_{ID} may identify the EAS for one or more ESS networks. In block 1106, discovery communications from the access points are advertised that include the K_{ID} . In addition to identifying the key holder identity (EAS, K_{ID}), the discovery communications may also identify the ESS for the particular access point. In block 1108, authentication messages may be derived based on the generation of the key K at the mobile device and at the EAS. The authentication may include a verification at the mobile device and/or the EAS that the key was properly generated. In one embodiment, this verification may occur without any authentication messages being transmitted. In block 1110, the mobile device may transition between ESS networks. When those networks are connected with the same EAS the transition may be expedited in part because the K key is already known. The expedited transition may be utilized when the mobile device recognizes the K_{ID} that is advertised.

[0064] The system and process described may be encoded in a signal bearing medium, a computer readable medium such as a memory, programmed within a device such as one or more integrated circuits, and one or more processors or processed by a controller or a computer. If the methods are performed by software, the software may reside in a memory resident to or interfaced to a storage device, synchronizer, a communication interface, or non-volatile or volatile memory in communication with a transmitter. A circuit or electronic device designed to send data to another location. The memory may include an ordered listing of executable instructions for implementing logical functions. A logical function or any system element described may be implemented through optic circuitry, digital circuitry, through source code, through analog circuitry, through an analog source such

as an analog electrical, audio, or video signal or a combination. The software may be embodied in any computer-readable or signal-bearing medium, for use by, or in connection with an instruction executable system, apparatus, or device. Such a system may include a computer-based system, a processor-containing system, or another system that may selectively fetch instructions from an instruction executable system, apparatus, or device that may also execute instructions.

[0065] A "computer-readable medium," "machine readable medium," "propagated-signal" medium, and/or "signal-bearing medium" may comprise any device that includes, stores, communicates, propagates, or transports software for use by or in connection with an instruction executable system, apparatus, or device. The machine-readable medium may selectively be, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, device, or propagation medium. A non-exhaustive list of examples of a machine-readable medium would include: an electrical connection "electronic" having one or more wires, a portable magnetic or optical disk, a volatile memory such as a Random Access Memory "RAM", a Read-Only Memory "ROM", an Erasable Programmable Read-Only Memory (EPROM or Flash memory), or an optical fiber. A machine-readable medium may also include a tangible medium upon which software is printed, as the software may be electronically stored as an image or in another format (e.g., through an optical scan), then compiled, and/or interpreted or otherwise processed. The processed medium may then be stored in a computer and/or machine memory.

[0066] In an alternative embodiment, dedicated hardware implementations, such as application specific integrated circuits, programmable logic arrays and other hardware devices, can be constructed to implement one or more of the methods described herein. Applications that may include the apparatus and systems of various embodiments can broadly include a variety of electronic and computer systems. One or more embodiments described herein may implement functions using two or more specific interconnected hardware modules or devices with related control and data signals that can be communicated between and through the modules, or as portions of an application-specific integrated circuit. Accordingly, the present system encompasses software, firmware, and hardware implementations.

[0067] The illustrations of the embodiments described herein are intended to provide a general understanding of the structure of the various embodiments. The illustrations are not intended to serve as a complete description of all of the elements and features of apparatus and systems that utilize the structures or methods described herein. Many other embodiments may be apparent to those of skill in the art upon reviewing the disclosure. Other embodiments may be utilized and derived from the disclosure, such that structural and logical substitutions and changes may be made without departing from the

scope of the disclosure. Additionally, the illustrations are merely representational and may not be drawn to scale. Certain proportions within the illustrations may be exaggerated, while other proportions may be minimized. Accordingly, the disclosure and the figures are to be regarded as illustrative rather than restrictive.

Claims

1. A method for generating and utilizing, by a mobile device (114), a key for transitioning between extended service set, ESS, networks, the method comprising:

receiving (702) an identifier of a key holder (302) and an identifier of a first ESS network from a first access point (104), the first access point (104) being connected to the first ESS network, and the first ESS network being associated with the key holder (302);

constructing an authentication request (704), the authentication request including a first nonce, where the first nonce includes first randomly generated data;

transmitting the authentication request (704) to the key holder (302);

receiving an authentication response (706) including a second nonce, where the second nonce includes second randomly generated data;

generating a mutually derived key with the key holder (302) based on a symmetrical algorithm using the authentication request (704) and the authentication response (706);

using the mutually derived key to allow the mobile device (114) to perform an authentication with the first access point (104);

receiving the identifier of the key holder (302) and an identifier of a second ESS network from a second access point, the second access point being connected to the second ESS network, and the second ESS network being associated with said key holder (302); and

using said mutually derived key to perform an authentication with the second access point, allowing the mobile device to perform a transition from the first ESS network to the second ESS network.

2. The method of claim 1, wherein each of said identifiers of the first and second ESS networks is a homogenous extended service set identifier, HESSID.
3. The method of claim 1, wherein the identifier of the key holder (302) is received prior to the mobile device (114) associating with the first ESS network connected to the first access point (104).

4. The method of claim 1, wherein the identifier of the key holder (302) is received at a media access control, MAC, sub-layer (204).

5. A mobile device (114) comprising a processor (502) configured to carry out the method of any of claims 1 to 4.

6. A computer readable medium comprising instructions which, when executed by a processor (502) of a mobile device (114), causes the mobile device (104) to carry out the method of any of claims 1 to 4.

15 Patentansprüche

1. Verfahren zum Erzeugen und Benutzen, durch ein Mobilgerät (114), eines Schlüssels zum Übergehen zwischen Extended-Service-Set(ESS)-Netzwerken, wobei das Verfahren Folgendes umfasst:

Empfangen (702) eines Identifiers eines Schlüsselinhabers (302) und eines Identifiers eines ersten ESS-Netzwerks von einem ersten Zugangspunkt (104), wobei der erste Zugangspunkt (104) mit dem ersten ESS-Netzwerk verbunden ist und das erste ESS-Netzwerk mit dem Schlüsselinhaber (302) verknüpft ist;

Konstruieren einer Authentifizierungsanforderung (704), wobei die Authentifizierungsanforderung einen ersten Zeitstempel beinhaltet, wobei der erste Zeitstempel erste zufällig erzeugte Daten beinhaltet;

Übertragen der Authentifizierungsanforderung (704) an den Schlüsselinhaber (302);

Empfangen einer Authentifizierungsantwort (706), die einen zweiten Zeitstempel beinhaltet, wobei der zweite Zeitstempel zweite zufällig erzeugte Daten beinhaltet;

Erzeugen eines gegenseitig abgeleiteten Schlüssels mit dem Schlüsselhalter (302) basierend auf einem symmetrischen Algorithmus unter Verwendung der Authentifizierungsanforderung (704) und der Authentifizierungsantwort (706);

Verwenden des gegenseitig abgeleiteten Schlüssels, um es dem Mobilgerät (114) zu ermöglichen, eine Authentifizierung mit dem ersten Zugangspunkt (104) durchzuführen;

Empfangen des Identifiers des Schlüsselinhabers (302) und eines Identifiers eines zweiten ESS-Netzwerks von einem zweiten Zugangspunkt, wobei der zweite Zugangspunkt mit dem zweiten ESS-Netzwerk verbunden ist und das zweite ESS-Netzwerk mit dem Schlüsselinhaber (302) verknüpft ist; und

Verwenden des gegenseitig abgeleiteten Schlüssels, um eine Authentifizierung mit dem

zweiten Zugangspunkt durchzuführen, Ermöglichen, dass das Mobilgerät einen Übergang von dem ersten ESS-Netzwerk zu dem zweiten ESS-Netzwerk durchführt.

2. Verfahren nach Anspruch 1, wobei jeder der Identifier des ersten und des zweiten ESS-Netzwerks ein Homogenous Extended Service Set Identifier (HES-SID) ist.
3. Verfahren nach Anspruch 1, wobei der Identifier des Schlüsselinhabers (302) empfangen wird, bevor sich das Mobilgerät (114) mit dem ersten ESS-Netzwerk verknüpft, das mit dem ersten Zugangspunkt (104) verbunden ist.
4. Verfahren nach Anspruch 1, wobei der Identifier des Schlüsselinhabers (302) an einer Media-Access-Control(MAC)-Unterschicht (204) empfangen wird.
5. Mobilgerät (114), das einen Prozessor (502) umfasst, der konfiguriert ist, um das Verfahren nach einem der Ansprüche 1 bis 4 zu vollziehen.
6. Computerlesbares Medium, das Anweisungen umfasst, die, wenn sie durch einen Prozessor (502) eines Mobilgeräts (114) ausgeführt werden, das Mobilgerät (104) veranlassen, ein Verfahren nach einem der Ansprüche 1 bis 4 zu vollziehen.

Revendications

1. Procédé pour générer et utiliser, par un dispositif mobile (114), une clé pour la transition entre des réseaux d'ensemble de services étendu, ESS, le procédé comprenant :

la réception (702) d'un identifiant d'un détenteur de clé (302) et d'un identifiant d'un premier réseau ESS provenant d'un premier point d'accès (104), le premier point d'accès (104) étant connecté au premier réseau ESS, et le premier réseau ESS étant associé au détenteur de clé (302) ;

la construction d'une demande d'authentification (704), la demande d'authentification comportant un premier nombre aléatoire, le premier nombre aléatoire comportant des premières données générées de manière aléatoire ;

la transmission de la demande d'authentification (704) au détenteur de clé (302) ;

la réception d'une réponse d'authentification (706) comportant un second nombre aléatoire, le second nombre aléatoire comportant des secondes données générées de manière aléatoire ;

la génération d'une clé dérivée mutuellement

avec le détenteur de clé (302) sur la base d'un algorithme symétrique à l'aide de la demande d'authentification (704) et de la réponse d'authentification (706) ;

l'utilisation de la clé dérivée mutuellement pour permettre au dispositif mobile (114) d'effectuer une authentification avec le premier point d'accès (104) ;

la réception de l'identifiant du détenteur de clé (302) et d'un identifiant d'un second réseau ESS en provenance d'un second point d'accès, le second point d'accès étant connecté au second réseau ESS, et le second réseau ESS étant associé audit détenteur de clé (302) ; et

l'utilisation de ladite clé dérivée mutuellement pour effectuer une authentification avec le second point d'accès, permettant au dispositif mobile d'effectuer une transition du premier réseau ESS au second réseau ESS.

2. Procédé selon la revendication 1, chacun desdits identifiants des premier et second réseaux ESS étant un identifiant d'ensemble de services étendu homogène, HESSID.

3. Procédé selon la revendication 1, l'identifiant du détenteur de clé (302) étant reçu avant que le dispositif mobile (114) ne s'associe au premier réseau ESS connecté au premier point d'accès (104).

4. Procédé selon la revendication 1, l'identifiant du détenteur de clé (302) étant reçu au niveau d'une sous-couche de commande d'accès au support, MAC, (204).

5. Dispositif mobile (114) comprenant un processeur (502) configuré pour mettre en œuvre le procédé selon l'une quelconque des revendications 1 à 4.

6. Support lisible par ordinateur comprenant des instructions qui, lorsqu'elles sont exécutées par un processeur (502) d'un dispositif mobile (114), amènent le dispositif mobile (104) à mettre en œuvre un procédé selon l'une quelconque des revendications 1 à 4.

Figure 1

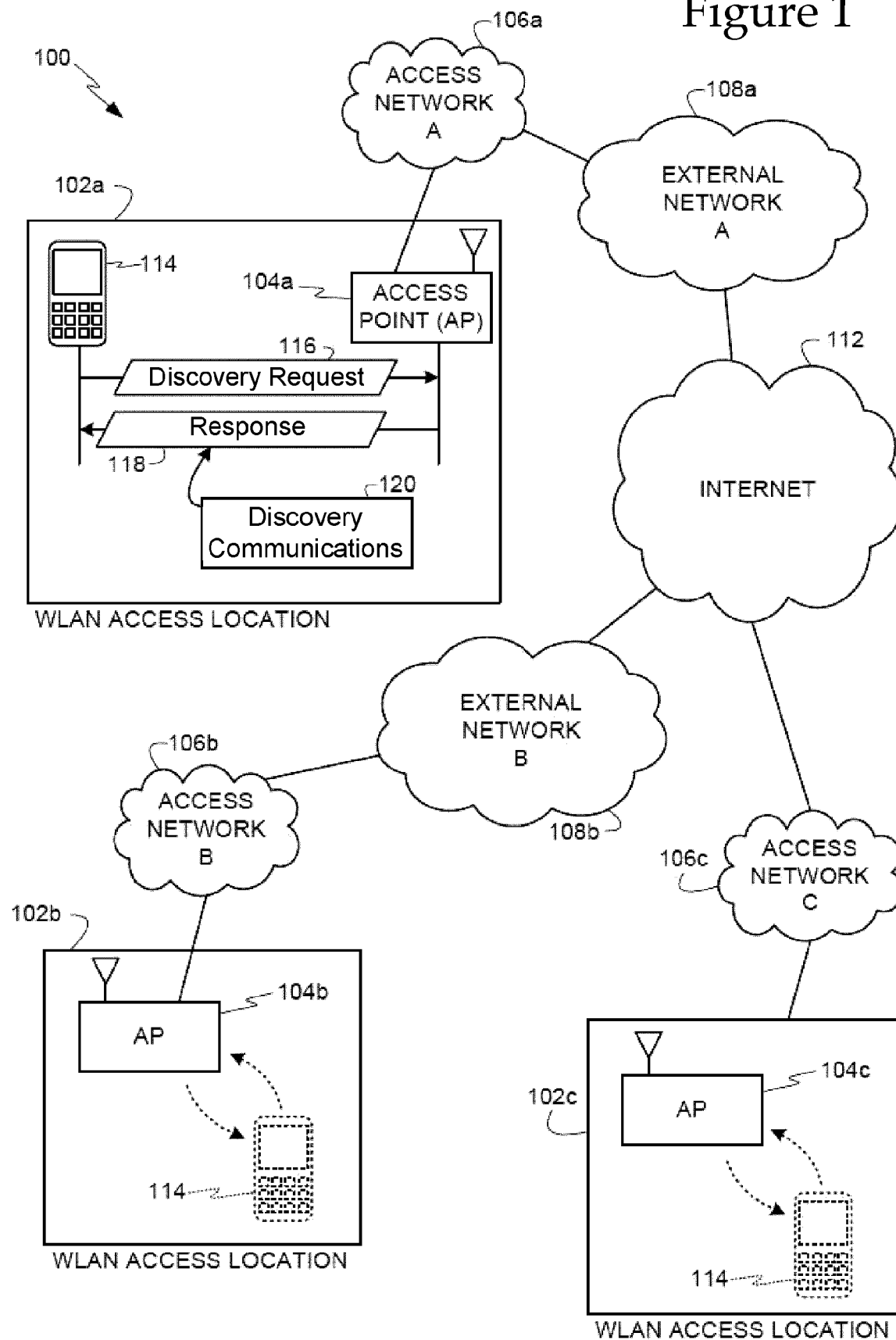
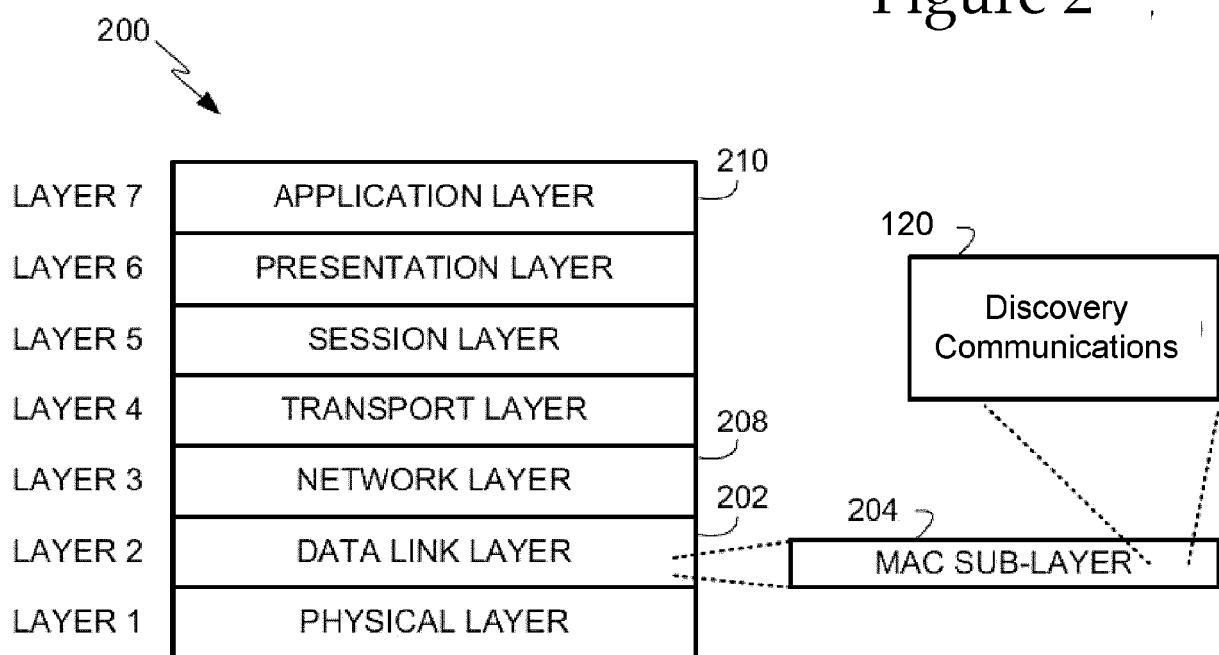


Figure 2



COMMUNICATION LAYER ARCHITECTURE

Figure 3

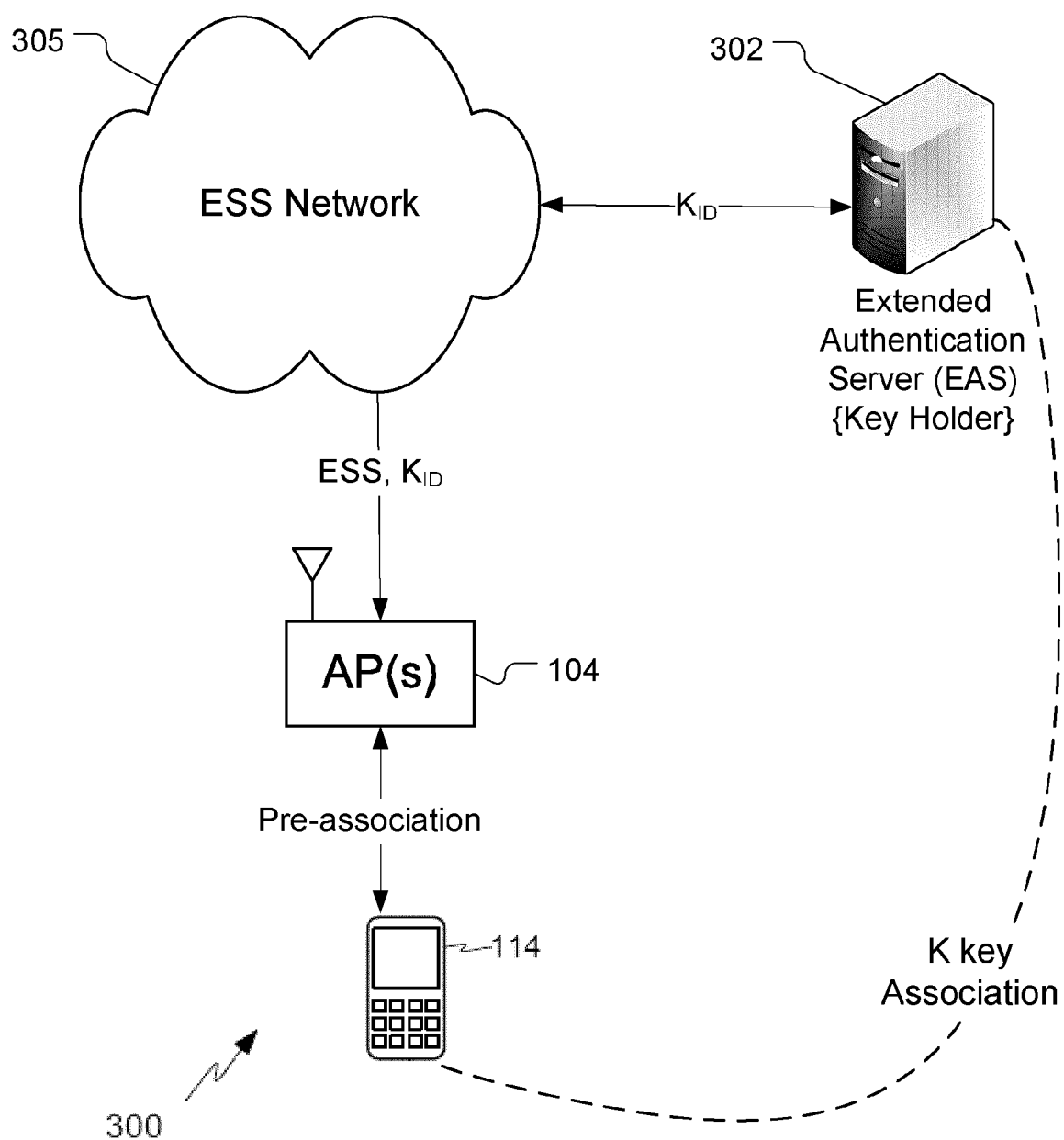


Figure 4

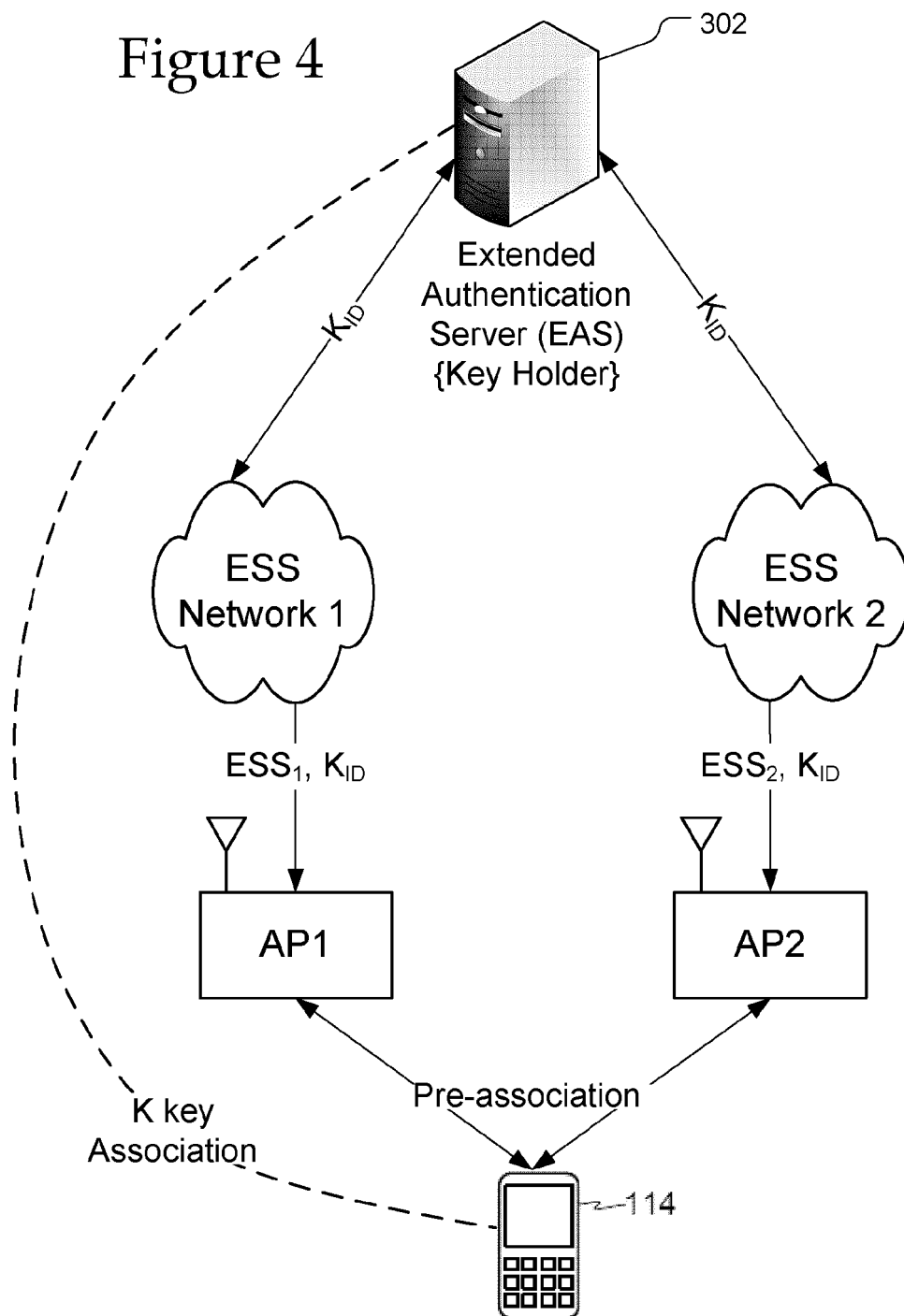


Figure 5

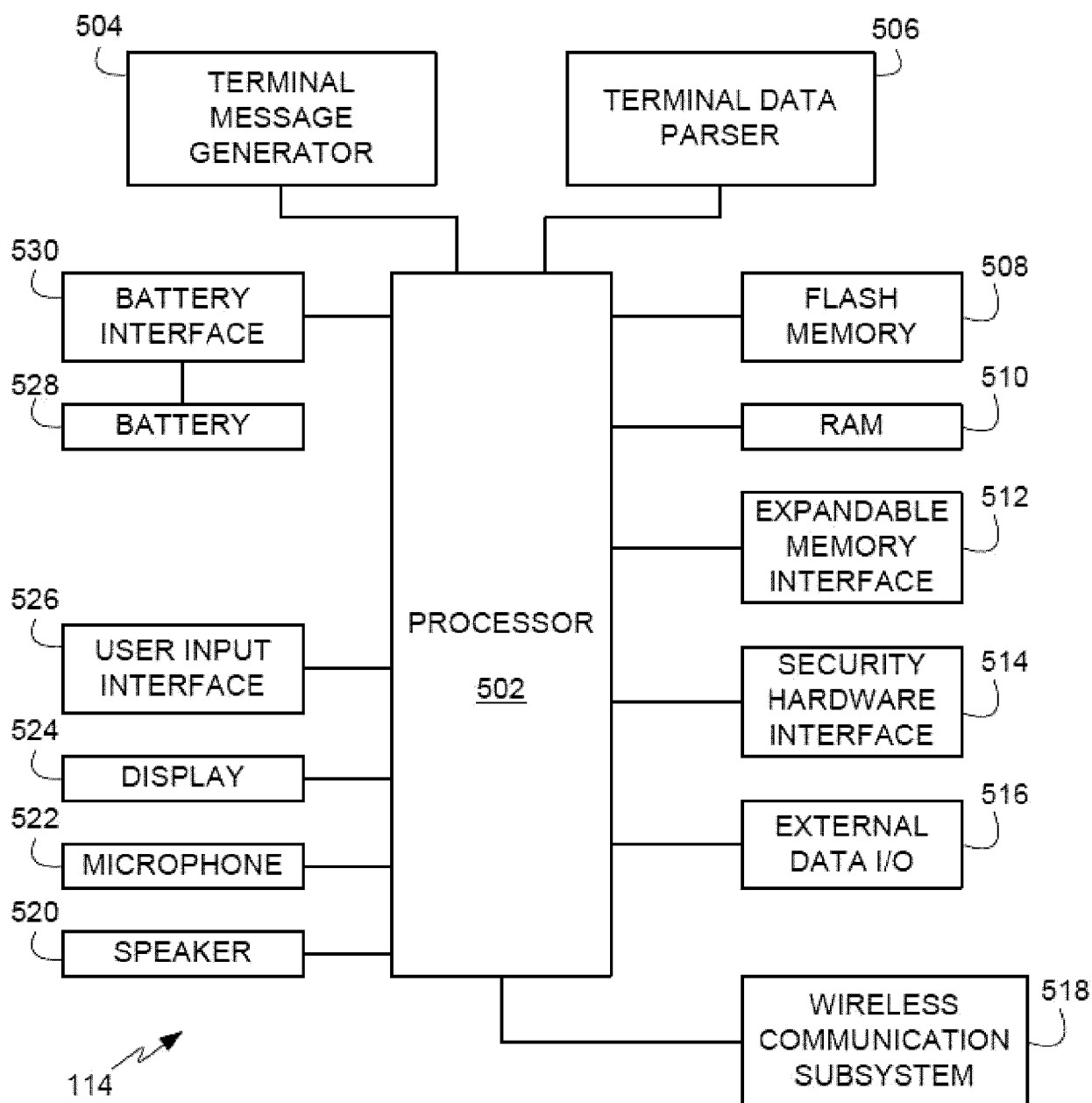


Figure 6

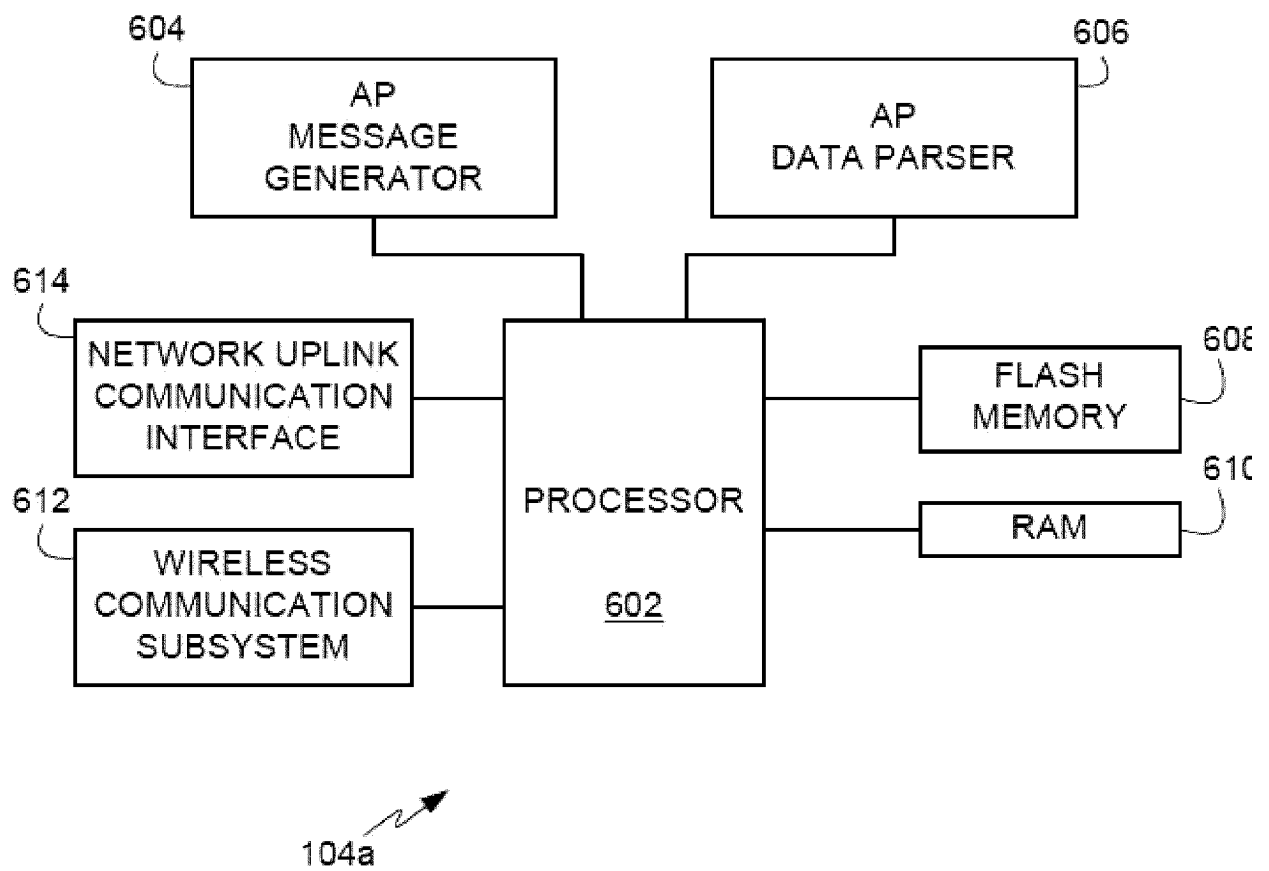


Figure 7

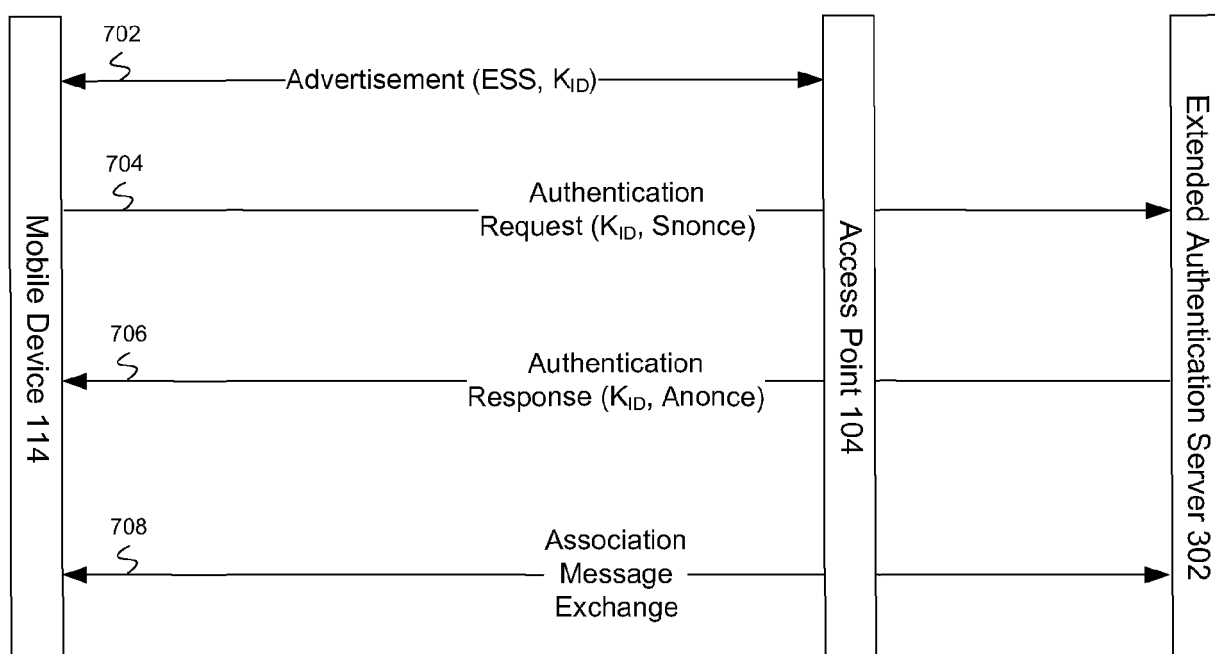


Figure 8

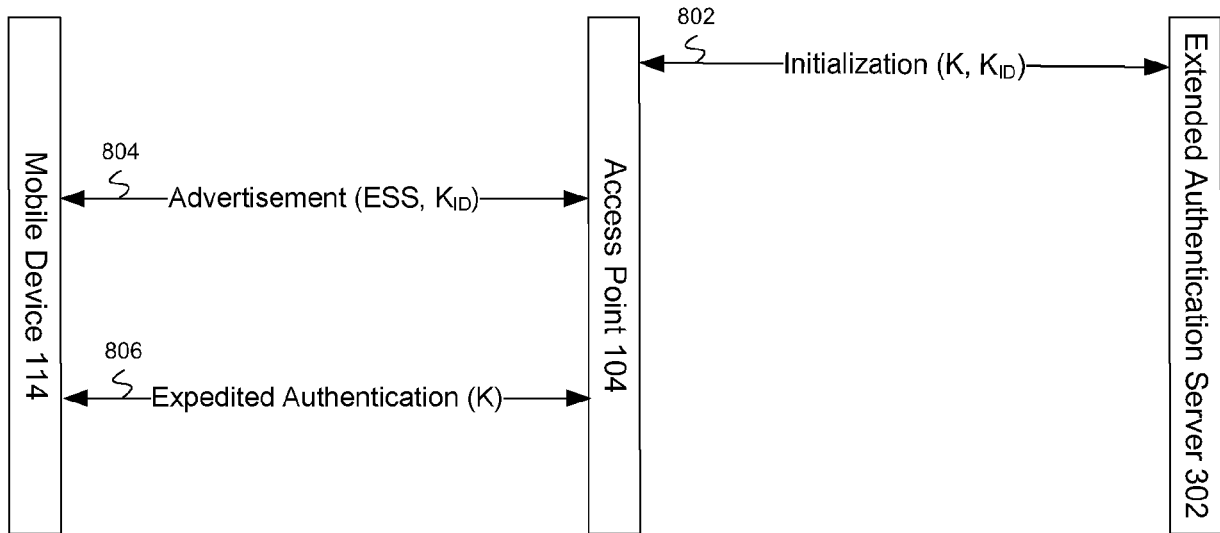


Figure 9

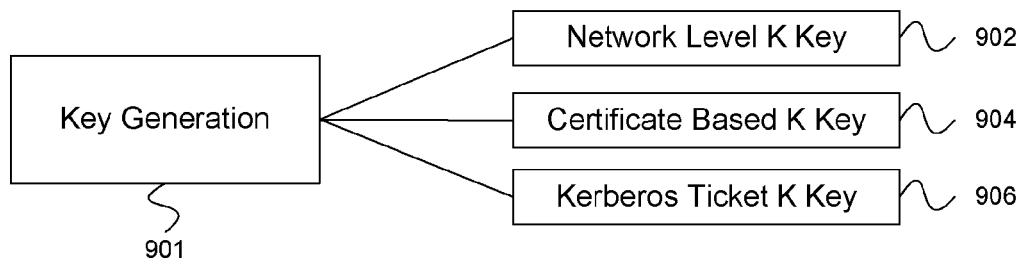


Figure 10

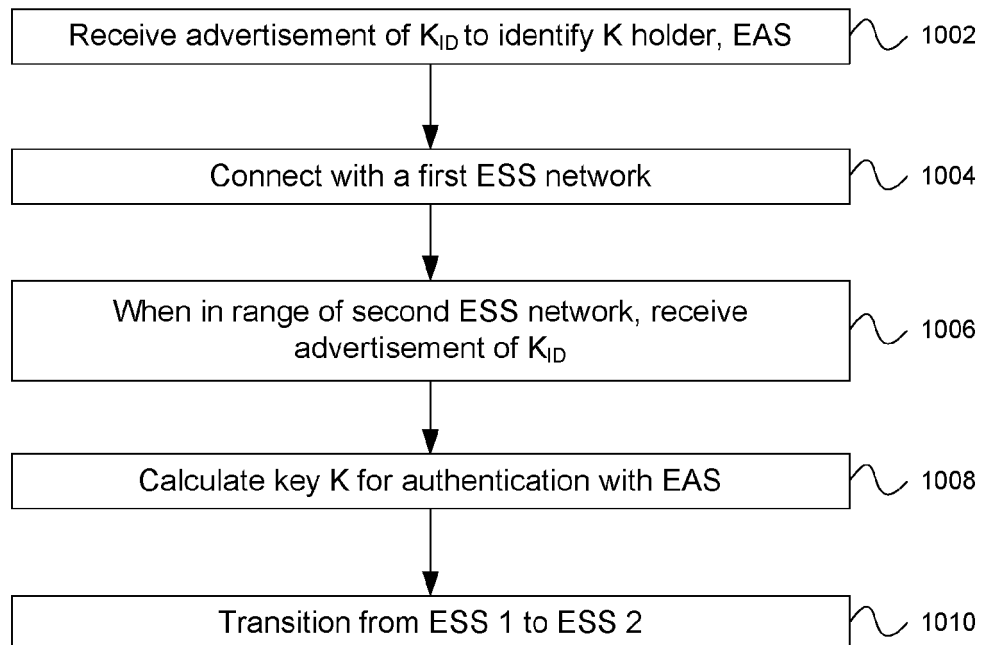
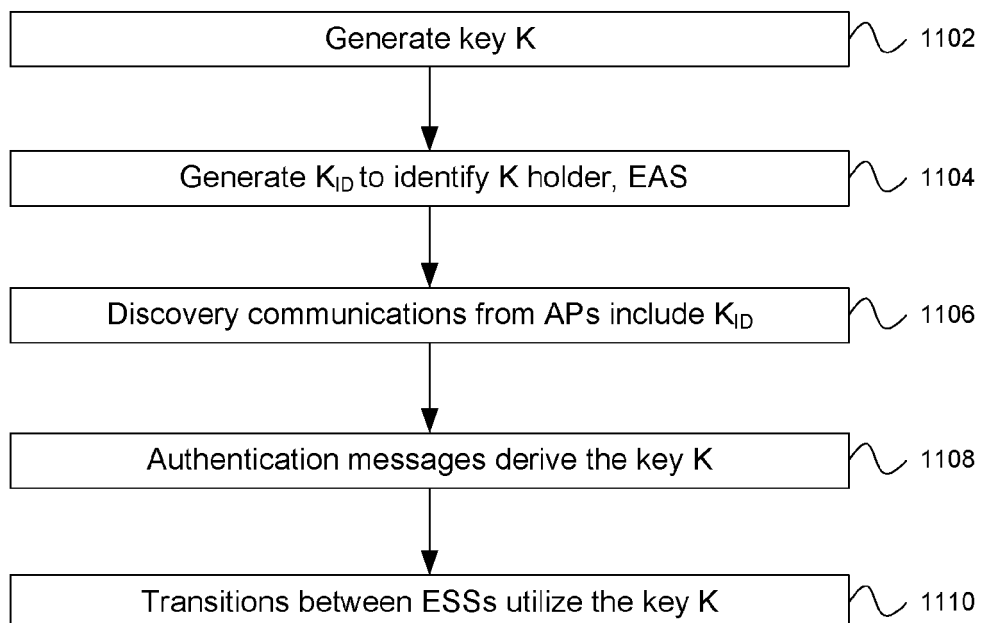


Figure 11



REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- EP 2445242 A1 [0003]