



- (51) International Patent Classification:
H04L 29/06 (2006.01) *H04W 48/18* (2009.01)
- (21) International Application Number:
PCT/FI2015/050434
- (22) International Filing Date:
15 June 2015 (15.06.2015)
- (25) Filing Language: English
- (26) Publication Language: English
- (71) Applicant: **NOKIA TECHNOLOGIES OY** [FI/FI];
Karaportti 3, FI-02610 Espoo (FI).
- (72) Inventors: **KASSLIN, Mika Ilkka Tapani**; Seljamäki 6
A, FI-02770 Espoo (FI). **MARIN, Janne**; Täysikuu 3 B
37, FI-02210 Espoo (FI). **TERVONEN, Janne Petteri**;
Kilonrinne 7 A 3, FI-02610 Espoo (FI). **MUSTAJÄRVI,**
Jari Pekka; Seitsemäs Järvikuja 6, FI-02730 Espoo (FI).
- (74) Agent: **SEPPO LAINE OY**; Itämerenkatu 3 B, FI-00180
Helsinki (FI).

- (81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,
BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR,
KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG,
MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM,
PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC,
SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ,
TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU,
TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE,
DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU,
LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,
SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, KM, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: ASSISTED NETWORK SELECTION

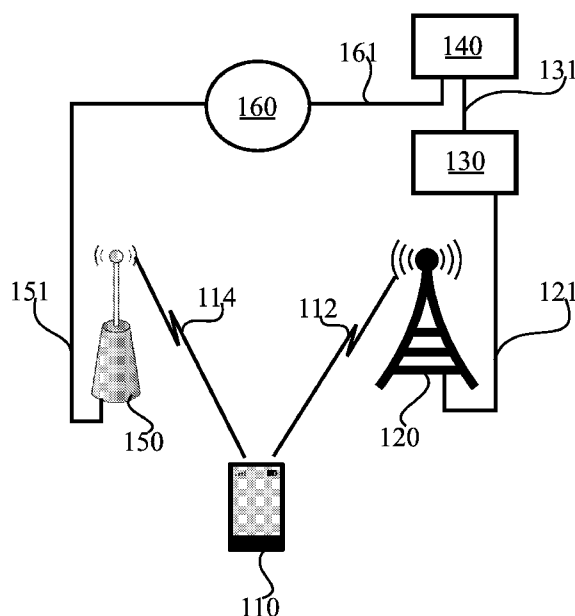


FIGURE 1

(57) Abstract: According to an example aspect of the present invention, there is provided an apparatus comprising a memory configured to store a first nonce, and at least one processing core configured to cause transmission, to a wireless access point, of a first message, the first message comprising the first nonce, to verify a correctness of a first cryptographic signature comprised in a response to the first message, and to use information from the wireless access point in network selection responsive to the cryptographic signature being verified as correct.



Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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

ASSISTED NETWORK SELECTION

FIELD

[0001] The present invention relates to network selection, such as, for example,
5 wireless network selection, using assistance information.

BACKGROUND

[0002] A mobile communication device may be capable of attaching to different types of access points. For example, a cellular device may be configured to interoperate
10 with a 3rd generation partnership project, 3GPP, radio access technology, RAT. Examples of 3GPP RATs include wideband code division multiple access, WCDMA, and long term evolution, LTE. Examples of non-3GPP technologies include Wi-Fi, also known as wireless local area network, WLAN, and wireless interoperability for microwave access, WiMAX.

15 [0003] In 3GPP technologies, the network side is tasked with taking decisions that relate to mobile attachments, for example handovers from one base station or technology to another. For example, a cellular telephone attached to LTE that requires a circuit-switched connection may be caused by the network to handover to WCDMA, where circuit-switched connections are supported. On the other hand, in WLAN technologies, the mobile
20 device is tasked with taking decisions that relate to attaching the mobile device to WLAN access points, APs.

[0004] Mobile devices capable of attaching to, for example, WLAN APs and cellular base stations, may implement network selection policies to facilitate deciding, which type of connectivity to use when communicating, or which access point to select when attaching
25 to WLAN. For example, a mobile device may be configured to request world wide web, WWW, content preferably over a WLAN access, and only use a 3GPP access if a WLAN access is unavailable.

[0005] To enable a mobile device to better decide, whether attaching to a specific WLAN AP is useful, WLAN APs may be configured to provide pre-attachment

information to mobiles. Such pre-attachment information may comprise, for example, information that relates to a backhaul status and service accessibility via the AP. For example, in case a specific AP only has a relatively slow connection to a backhaul connection, a mobile device seeking to transfer a large file may select, based at least in part
5 on the pre-attachment information, another AP for attaching.

SUMMARY OF THE INVENTION

10 [0006] The invention is defined by the features of the independent claims. Some specific embodiments are defined in the dependent claims.

[0007] According to a first aspect of the present invention, there is provided an apparatus comprising a memory configured to store a first nonce, and at least one processing core configured to cause transmission, to a wireless access point, of a first
15 message, the first message comprising the first nonce, to verify a correctness of a first cryptographic signature comprised in a response to the first message, and to use information from the wireless access point in network selection responsive to the first cryptographic signature being verified as correct.

[0008] Various embodiments of the first aspect may comprise at least one feature
20 from the following bulleted list:

- the at least one processing core is configured to discard without using in network selection the information from the wireless access point responsive to the first cryptographic signature being verified as incorrect or not present
- the at least one processing core is further configured to obtain a second nonce, to
25 calculate a second cryptographic signature based at least in part on the second nonce, and to include the second cryptographic signature in the first message
- the at least one processing core is configured to obtain the second nonce from a broadcast transmission originating in the wireless access point
- the at least one processing core is configured to obtain the second nonce by
30 requesting for it from the wireless access point

- the at least one processing core is configured to obtain the second nonce from a preselected public variable
- the at least one processing core is further configured calculate a second cryptographic signature based at least in part on the first nonce, and to include the second cryptographic signature in the first message
- the at least one processing core is configured to verify the correctness of the first cryptographic signature based, at least in part, on the first nonce and a security key
- the at least one processing core is further configured to cause the apparatus to participate in an authentication procedure between the apparatus and an authentication server, and to store the security key in connection with the authentication procedure
- the first message and the response to the first message are pre-association messages.

[0009] According to a second aspect of the present invention, there is provided an apparatus comprising at least one processing core, at least one memory including computer program code, the at least one memory and the computer program code being configured to, with the at least one processing core, cause the apparatus at least to receive, from a user equipment, a first message, the first message comprising a first nonce, obtain a first cryptographic signature based at least in part on the first nonce, and cause provision, to the user equipment, of the first cryptographic signature comprised in a response to the first message, and to cause provision, to the user equipment, of network selection information.

[0010] Various embodiments of the second aspect may comprise at least one feature from the following bulleted list:

- the at least one memory and the computer program code are configured to, with the at least one processing core, cause the apparatus to obtain the first cryptographic signature based at least in part on the network selection information
- the at least one memory and the computer program code are configured to, with the at least one processing core, cause the apparatus to obtain the first cryptographic signature, at least in part, by transmitting a request to an authentication server
- the at least one memory and the computer program code are configured to, with the at least one processing core, cause the apparatus to establish a second nonce, and to verify, at least in part based on the second nonce, a second cryptographic signature,

the second cryptographic signature being received in the apparatus from the user equipment

- the first message comprises the second cryptographic signature
- the first message and the response to the first message are pre-association messages
- 5 • the at least one memory and the computer program code are configured to, with the at least one processing core, cause the apparatus to verify the correctness of the second cryptographic signature based, at least in part, on a security key
- the at least one memory and the computer program code are configured to, with the at least one processing core, cause the apparatus to obtain the security key from a
- 10 node that has participated in an authentication procedure with the user equipment.

[0011] According to a third aspect of the present invention, there is provided a method comprising storing a first nonce, causing transmission, to a wireless access point, of a first message, the first message comprising the a first nonce verifying a correctness of a first cryptographic signature comprised in a response to the first message, and using

15 information from the wireless access point in network selection responsive to the first cryptographic signature being verified as correct.

[0012] Various embodiments of the third aspect may comprise at least one feature corresponding to a feature from the preceding bulleted list laid out in connection with the first aspect.

20 [0013] According to a fourth aspect of the present invention, there is provided a method comprising receiving, in an apparatus, from a user equipment, a first message, the first message comprising first nonce obtaining a first cryptographic signature based at least in part on the first nonce causing provision, to the user equipment, of the first cryptographic signature comprised in a response to the first message, and causing

25 provision, to the user equipment, of network selection information.

[0014] Various embodiments of the fourth aspect may comprise at least one feature corresponding to a feature from the preceding bulleted list laid out in connection with the second aspect.

[0015] According to a fifth aspect of the present invention, there is provided an

30 apparatus comprising means for storing a first nonce, means for causing transmission, to a wireless access point, of a first message, the first message comprising the first nonce,

means for verifying a correctness of a first cryptographic signature comprised in a response to the first message, and means for using information from the wireless access point in network selection responsive to the first cryptographic signature being verified as correct.

[0016] According to a sixth aspect of the present invention, there is provided an apparatus comprising means for receiving, in an apparatus, from a user equipment, a first message, the first message comprising a first nonce, means for obtaining a first cryptographic signature based at least in part on the first nonce, means for causing provision, to the user equipment, of the first cryptographic signature comprised in a response to the first message, and means for causing provision, to the user equipment, of network selection information.

[0017] According to a seventh aspect of the present invention, there is provided a non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least store a first nonce, cause transmission, to a wireless access point, of a first message, the first message comprising the first nonce, verify a correctness of a first cryptographic signature comprised in a response to the first message, and use information from the wireless access point in network selection responsive to the first cryptographic signature being verified as correct.

[0018] According to an eighth aspect of the present invention, there is provided a non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least receive, in an apparatus, from a user equipment, a first message, the first message comprising a first nonce, obtain a first cryptographic signature based at least in part on the first nonce, cause provision, to the user equipment, of the first cryptographic signature comprised in a response to the first message, and cause provision, to the user equipment, of network selection information.

[0019] According to a ninth aspect of the present invention, there is provided a computer program configured to cause a method in accordance with at least one of the third and fourth aspects to be performed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] FIGURE 1 illustrates an example system in accordance with at least some embodiments of the present invention;

[0021] FIGURE 2 illustrates pre-association messaging in accordance with at least
5 some embodiments of the present invention;

[0022] FIGURE 3 illustrates an example apparatus capable of supporting at least some embodiments of the present invention;

[0023] FIGURE 4 illustrates messaging in accordance with at least some embodiments of the present invention;

10 [0024] FIGURE 5 is a first flow graph illustrating a first method in accordance with at least some embodiments of the present invention, and

[0025] FIGURE 6 is a second flow graph illustrating a second method in accordance with at least some embodiments of the present invention.

15

EMBODIMENTS

[0026] To enable a mobile device to better trust pre-association information provided by a network, or access point, the pre-association information may comprise a cryptographic signature. The cryptographic signature may be produced using a key that the
20 mobile device is aware of, for example due to a prior authentication process. The cryptographic signature may be calculated, at least in part, over a nonce provided by the mobile device. The cryptographic signature may be used not only to prove an identity of the sender but it can also protect a message from tampering, if the signature is calculated also over content to be protected, for example both the nonce and network selection
25 information. Both scenarios are included here, respectively in applicable embodiments. Where the cryptographic signature is calculated over the network selection information, that is, the signature is obtained based at least in part on the network selection information, an attempt to modify the network selection information afterward would be detected in connection with verifying the cryptographic signature.

[0027] The mobile device may provide a cryptographic signature to the network to prove its identity, wherein this mobile-provided cryptographic signature may be calculated, at least in part, over a nonce provided by the network, for example by broadcasting or responsive to a request from the mobile device. A mobile-provided cryptographic signature
5 may be produced using the same key as the network-provided cryptographic signature, wherein the key is known to the mobile device from a prior authentication, and the key is known to the network from an authentication server that the mobile device performed the prior authentication with.

[0028] FIGURE 1 illustrates an example system in accordance with at least some
10 embodiments of the present invention. The system of FIGURE 1 comprises device 110, which may comprise, for example, a smartphone, tablet computer, laptop computer, cellular phone or other suitable electronic device with wireless connectivity. In FIGURE 1, a multi-access device 110 is illustrated, but in other embodiments of the invention device 110 may support a single wireless connectivity technology. Device 110 of FIGURE 1 has
15 wireless link 112 with base station 120. Base station 120 may comprise, for example, a WCDMA or LTE base station, which may be known as a node-B or eNB, respectively. Wireless link 112 is configured to operate in accordance with a same RAT as base station 120, for example, where base station 120 comprises a WCDMA node-B, wireless link 112 comprises a WCDMA wireless link. Wireless link 112 may comprise an uplink for
20 conveying information from device 110 to base station 120. Wireless link 112 may comprise a downlink for conveying information from base station 120 to device 110.

[0029] Base station 120 may be coupled, via connection 121, with network node 130. Network node 130 may comprise a radio network controller, RNC, or a core network node, for example, depending on the technology used. In some embodiments, network
25 node 130 may be absent. Where network node 130 is absent, base station 120 may communicate directly with authentication server 140. Where network node 130 is present, network node 130 may be communicatively coupled with authentication server 140, via connection 131. Base station 120 may exchange messages with authentication server 140 via network node 130, for example.

30 [0030] Device 110 may be configured to perform an authentication procedure with authentication server 140, such that messages comprised in the authentication procedure are exchanged between device 110 and authentication server 140 via wireless link 112,

base station 120, and, where present, network node 130. Alternatively, the authentication process may be performed between device 110 and authentication server 140 via AP 150. An example of an authentication procedure is an extensible authentication protocol, EAP, authentication, such as, for example, an EAP-SIM, EAP-AKA or EAP-AKA' authentication. A further example is a password-based authentication followed by a Diffie-Hellman exchange. In connection with the authentication procedure, a master session key (MSK) and extended master session key (EMSK) may be generated between device 110 and authentication server 140 from the established keying material. These master keys may be used to generate temporary session keys between device 110 and AP 150 acting as authenticator, potentially via different key hierarchies, for example. Nevertheless, both device 110 and authentication server 140 may know the key hierarchy and be able to derive same key hierarchy and keys from the MSK or EMSK, depending on the use case. EAP-RP is variation of this; device 110 and authentication server 140 derive a new root key for EAP-RP usage from the EMSK. The authenticator assumes ERP server role or provides the EAP-RP root key rRK to ERP server. Later we don't separate these roles and authentication server may mean either of them. The authentication procedure is now carried out between device 110 and authentication server 140 using the keys derived from MSK or EMSK or rRK. Copies of the generated master keys may be stored in device 110 and in authentication server 140. Copies of the generated keys may be stored in device 110 and in base station 120 or AP 150 acting as authenticator. The device 110 may have means to indicate to the authenticator which keys are in use and the authenticator or authentication server may have means to recognize this so the same keys are used in both endpoints.

[0031] In general, whereas AP 150 is herein referred to as participating in processes with device 110 or other nodes, it is to be understood that in various embodiments, a wireless local area network, WLAN, controller, WLC, or access network query protocol, ANQP, server may perform, at least in part, the role described herein as that of AP 150. In general, AP 150, a WLC or an ANQP server may be considered to act as an authenticator when performing this role.

[0032] Device 110 may be arranged to communicate wirelessly with AP 150. AP 150 may be configured to operate in accordance with a non-cellular technology, such as, for example, WLAN or WiMAX. Wireless link 114 may comprise an exchange of information in messages, such that device 110 is not attached to AP 150. In this regard,

such messages exchanged over wireless link 114 may be considered pre-association messages. As an association process leading to association between device 110 and AP 150 may comprise an association request frame and an association response frame, pre-association messages may comprise messages exchanged between device 110 and AP 150
5 such that there is no current association and no association request frame has been exchanged between device 110 and AP 150 since an end of any prior association. In general, messages exchanged between device 110 and AP 150 before an active association is setup may be considered pre-association messages. One example of pre-association messaging is General Advertisement Service that has been described in standard IEEE
10 802.11-2012. An active association enables for device 110 access to network services via AP 150.

[0033] AP 150 may provide to device 110 network selection information in the pre-association messaging. Network selection information may comprise at least one of information characterizing AP 150, its connectivity and/or services accessible via AP 150,
15 information about its neighbourhood and instruction to move to cellular networks instead. For example, network selection information may comprise information of a data bandwidth AP 150 has to a backbone network, characterizing a communication speed obtainable when communicating with the Internet via AP 150, for example. In principle, device 110 may choose to use the network selection information received from AP 150 when selecting
20 which AP or base station to attach to. However, a maliciously behaving AP 150 may provide inaccurate network selection information intending to cause a device 110 to associate with this AP, in order, for example, to eavesdrop on communications of device 110. Even worse, the AP may instruct the device to move to cellular connection when there is no need for this. Therefore, device 110 advantageously could establish some trust with
25 AP 150 before using the pre-association network selection information received from AP 150.

[0034] Establishing trust may comprise verifying AP 150 has the identity it claims to have, and/or that AP 150 has a secure association with an authentication server device 110 is willing to trust. Device 110 may assume that only reliable access points have access to
30 authentication servers device 110 itself uses, since device 110 is associated securely with an access provider that manages these authentication servers. For example, in terms of FIGURE 1, authentication server 140 may be managed by an access provider with which device 110 has a secure relationship via a subscription, and device 110 may be willing to

trust access points that the access provider is willing to trust to the extent of providing access to authentication server 140.

[0035] Device 110 may be configured to provide, in pre-association messaging or post-association messaging, to AP 150 a nonce, by which it is meant a number generated or selected by device 110. This nonce may be known as a device nonce. A nonce may
5 comprise a random number, for example. Device 110 may also provide an identity of itself to AP 150. The identity of device 110 may comprise a subscription identity, such as a cellular telephone number, for example, or a device identifier, such as an international mobile station equipment identity, IMEI. The identity of device 110 may comprise an
10 identity associated with the authentication process performed between device 110 and authentication server 140. An example of such an identity is an EAP-RP identity. The identity of device 110 may comprise or be associated with an identifier of a security key generated in connection with the authentication procedure. Effectively the identity allows the authenticator or the authentication server to identify a suitable security key or keying
15 material from which the security key is derived from to be used for the verification process at hand. The security key may comprise, for example, an encryption key or another kind of key. In some embodiments, the nonce and the identity are provided from device 110 to AP 150 in the same message. Where the identity of device 110 is not associated with an identifier of a security key, or where an identity of device 110 is not provided, information
20 enabling an security key to be identified may be provided from device 110 to AP 150, for example in a same message as the device nonce and/or device 110 identity.

[0036] AP 150 may be configured to obtain a cryptographic signature, such that the device nonce received in AP 150 from device 110 is comprised in input to the cryptographic signature. AP 150 may obtain the cryptographic signature by transmitting a
25 request to authentication server 140, for example via connection 151, network 160 and connection 161. The request may comprise the input to be signed, or the request may comprise a request for the security key generated in connection with the authentication procedure to be provided to AP 150. Responsive to this request, authentication server 140 may provide the requested cryptographic signature or security key, depending on the
30 embodiment. AP 150 may also itself possess the required security key already, identified for example by a pairwise master key security association id, PMKSAID, for example. The AP 150 may then calculate the signature itself. A retrieved security key may be also used locally to derive a final security key used in the validation process.

[0037] AP 150 may provide to device 110 a response message, the response message comprising the cryptographic signature. Based on the response message, device 110 may determine, whether the cryptographic signature is correct. In detail, device 110 may derive the correct cryptographic signature based on the device nonce and a copy of the security key stored or derived locally in device 110, and then compare this correct signature to the signature received from AP 150 in the response message. In case the signature provided by AP 150 is correct, device 110 may consider the network selection information provided by AP 150 to be reliable and use it. In case the signature provided by AP 150 is incorrect, device 110 may be configured to discard the network selection information provided by AP 150. In case AP 150 fails to provide any signature to device 110, device 110 may, for example, use network selection information provided by AP 150 in case it is generic but not otherwise, or device 110 may ignore network selection information provided by AP 150.

[0038] On the other hand, AP 150 may be configured to verify that device 110 is reliable. This may be accomplished by providing, from AP 150, a network nonce to device 110. By network nonce it is meant a number generated or selected by a network node, such as, for example, AP 150 or authentication server 140. Device 110 may then generate a cryptographic signature using the security key with the network nonce as input, and provide this signature to AP 150 so AP 150 can verify it is correct. For example, AP 150 may provide the signature it has received, along with the network nonce, to authentication server 140, for example in the request message where AP 150 requests for the authentication server to sign the device nonce that device 110 has provided. Alternatively, in embodiments where authentication server 140 provides the security key to AP 150 or AP 150 already has the key locally, AP 150 can verify the signature it has received from device 110 locally in AP 150.

[0039] The network nonce may be provided from AP 150 to device 110 by including the network nonce in a broadcast message AP 150 transmits, for example periodically. This has the benefit that device 110 needs only one signal to the AP 150 to prove its identity. AP 150 may change the network nonce that is broadcast, for example once every second or once every five seconds. Alternatively, another kind of validable nonce can be used too, like current time of day or cellular frame number. Such a validable nonce may be referred to in general as a preselected public variable. Therefore, AP 150 may establish the network nonce by transmitting it to device 110, or deriving it from a preselected public

variable, for example. Alternatively, device 110 may request AP 150 to provide the network nonce to device 110 before device 110 transmits the message to AP 150 that comprises the device nonce. The request for the network nonce, and the provision of the network nonce in response, may be conducted by pre-association messaging. In case
5 device 110 knows the network nonce before transmitting the device nonce to AP 150, device 110 may include the cryptographic signature it generates using the network nonce to the same message that is used to convey the device nonce to AP 150. AP 150 may then send a single query to authentication server 140, to both obtain the cryptographic signature over the device nonce and to verify correctness of the cryptographic signature over the
10 network nonce. This single query would in this case comprise the network nonce, the cryptographic signature received from device 110 and the device nonce.

[0040] In some embodiments, device 110 may provide, for example in the same message as the device nonce, a cryptographic signature that device 110 has obtained using the security key with the device nonce as input. This way no separate network nonce is
15 needed to be obtained in device 110 prior to transmission of the device nonce to AP 150, however this method is open to playback-type attacks since the nonce used to obtain the cryptographic signature has been selected by device 110 itself. An attacker could record this message, and use the same nonce and signature in a subsequent message, to masquerade as device 110. However this would still provide an advantage over not
20 performing any steps to authenticate device 110, since an attacker would need to obtain a recording of a valid message from a device 110.

[0041] FIGURE 2 illustrates pre-association messaging in accordance with at least some embodiments of the present invention. On the vertical axes are disposed, on the left, device 110, and on the right, AP 150. Time advances from the top toward the bottom.

25 [0042] First pre-association message 210 may comprise, for example, a request for network selection information. Second pre-association message 220 may comprise the requested network selection information, which the access point provides as a response to the request of message 210.

[0043] Association process 230 comprises a procedure through which a non-
30 associated device becomes associated with the access point. As a result of association process 230, an association 240 between device 110 and AP 150 may result. During association 240, device 110 may obtain services via AP 150, such as, for example, a user

of device 110 may browse the world wide web using device 110. Therefore, as messages 210 and 220 take place outside of an actual association, they are referred to as pre-association messages. Alternatively to an association process 230 between device 110 and AP 150 leading to association of device 110 to AP 150, AP 150 may direct device 110 to become associated with a cellular network, instead of with AP 150.

[0044] After association 240 ceases, device 110 may once more exchange pre-association messages with AP 150. Thus a prior, ended association does not preclude the possibility of exchanging pre-association messages. Pre-association message 250 may comprise a request for a network nonce, for example. Pre-association message 260 may comprise a message conveying the network nonce to device 110, and pre-association message 270 may comprise a message that comprises a device nonce, a cryptographic signature obtained, at least in part, on the network nonce and, optionally, an identity which allows AP 150 or authentication server 140 to identify or derive the security key used by device 110. Pre-association messages 250, 260 and 270 may be followed by a second association process 280, which may lead to a new association. Such a new association is not illustrated in FIGURE 2.

[0045] FIGURE 3 illustrates an example apparatus capable of supporting at least some embodiments of the present invention. Illustrated is device 300, which may comprise, for example, a unit such as device 110 or, where applicable, AP 150 of FIGURE 1. Comprised in device 300 is processor 310, which may comprise, for example, a single- or multi-core processor wherein a single-core processor comprises one processing core and a multi-core processor comprises more than one processing core. Processor 310 may comprise more than one processor. A processing core may comprise, for example, a Cortex-A8 processing core manufactured by ARM Holdings or a Steamroller processing core produced by Advanced Micro Devices Corporation. Processor 310 may comprise at least one Qualcomm Snapdragon and/or Intel Atom processor. Processor 310 may comprise at least one application-specific integrated circuit, ASIC. Processor 310 may comprise at least one field-programmable gate array, FPGA. Processor 310 may be means for performing method steps in device 300. Processor 310 may be configured, at least in part by computer instructions, to perform actions.

[0046] Device 300 may comprise memory 320. Memory 320 may comprise random-access memory and/or permanent memory. Memory 320 may comprise at least one RAM

chip. Memory 320 may comprise solid-state, magnetic, optical and/or holographic memory, for example. Memory 320 may be at least in part accessible to processor 310. Memory 320 may be at least in part comprised in processor 310. Memory 320 may be means for storing information. Memory 320 may comprise computer instructions that processor 310 is configured to execute. When computer instructions configured to cause processor 310 to perform certain actions are stored in memory 320, and device 300 overall is configured to run under the direction of processor 310 using computer instructions from memory 320, processor 310 and/or its at least one processing core may be considered to be configured to perform said certain actions. Memory 320 may be at least in part comprised in processor 310. Memory 320 may be at least in part external to device 300 but accessible to device 300.

[0047] Device 300 may comprise a transmitter 330. Device 300 may comprise a receiver 340. Transmitter 330 and receiver 340 may be configured to transmit and receive, respectively, information in accordance with at least one cellular or non-cellular standard. Transmitter 330 may comprise more than one transmitter. Receiver 340 may comprise more than one receiver. Transmitter 330 and/or receiver 340 may be configured to operate in accordance with global system for mobile communication, GSM, wideband code division multiple access, WCDMA, long term evolution, LTE, IS-95, wireless local area network, WLAN, Ethernet and/or worldwide interoperability for microwave access, WiMAX, standards, for example.

[0048] Device 300 may comprise a near-field communication, NFC, transceiver 350. NFC transceiver 350 may support at least one NFC technology, such as NFC, Bluetooth, Wibree or similar technologies.

[0049] Device 300 may comprise user interface, UI, 360. UI 360 may comprise at least one of a display, a keyboard, a touchscreen, a vibrator arranged to signal to a user by causing device 300 to vibrate, a speaker and a microphone. A user may be able to operate device 300 via UI 360, for example to accept incoming telephone calls, to originate telephone calls or video calls, to browse the Internet, to manage digital files stored in memory 320 or on a cloud accessible via transmitter 330 and receiver 340, or via NFC transceiver 350, and/or to play games.

[0050] Device 300 may comprise or be arranged to accept a user identity module 370. User identity module 370 may comprise, for example, a subscriber identity module,

SIM, card installable in device 300. A user identity module 370 may comprise information identifying a subscription of a user of device 300. A user identity module 370 may comprise cryptographic information usable to verify the identity of a user of device 300 and/or to facilitate encryption of communicated information and billing of the user of device 300 for communication effected via device 300.

[0051] Processor 310 may be furnished with a transmitter arranged to output information from processor 310, via electrical leads internal to device 300, to other devices comprised in device 300. Such a transmitter may comprise a serial bus transmitter arranged to, for example, output information via at least one electrical lead to memory 320 for storage therein. Alternatively to a serial bus, the transmitter may comprise a parallel bus transmitter. Likewise processor 310 may comprise a receiver arranged to receive information in processor 310, via electrical leads internal to device 300, from other devices comprised in device 300. Such a receiver may comprise a serial bus receiver arranged to, for example, receive information via at least one electrical lead from receiver 340 for processing in processor 310. Alternatively to a serial bus, the receiver may comprise a parallel bus receiver.

[0052] Device 300 may comprise further devices not illustrated in FIGURE 3. For example, where device 300 comprises a smartphone, it may comprise at least one digital camera. Some devices 300 may comprise a back-facing camera and a front-facing camera, wherein the back-facing camera may be intended for digital photography and the front-facing camera for video telephony. Device 300 may comprise a fingerprint sensor arranged to authenticate, at least in part, a user of device 300. In some embodiments, device 300 lacks at least one device described above. For example, some devices 300 may lack a NFC transceiver 350 and/or user identity module 370.

[0053] Processor 310, memory 320, transmitter 330, receiver 340, NFC transceiver 350, UI 360 and/or user identity module 370 may be interconnected by electrical leads internal to device 300 in a multitude of different ways. For example, each of the aforementioned devices may be separately connected to a master bus internal to device 300, to allow for the devices to exchange information. However, as the skilled person will appreciate, this is only one example and depending on the embodiment various ways of interconnecting at least two of the aforementioned devices may be selected without departing from the scope of the present invention.

[0054] FIGURE 4 illustrates messaging in accordance with at least some embodiments of the present invention. Disposed on the vertical axes are disposed, on the left, device 110, in the middle, AP 150, and on the right authentication server 140. Time advances from the top toward the bottom.

5 [0055] In optional phase 410, device 110 requests AP 150 to provide a network nonce to device 110. In optional phase 420, AP 150 provides a network nonce to device 110. Where phase 410 is present, the message of phase 420 may be directed to device 110. Where phase 410 is absent, the provision of the network nonce in phase 420 may take place by broadcasting or be a preselected public variable, as described above.

10 [0056] In phase 430, device 110 provides to AP 150 a device nonce and, optionally, an identifier of device 110 and/or information enabling identification of a security key. The security key may, for example, be a key generated in connection with an authentication procedure between device 110 and authentication server 140. Where phase 420 is present, device 110 may provide, in phase 430, a cryptographic signature derived using the security
15 key, with the network nonce from phase 420 among input data to the cryptographic signature algorithm. Phase 430 may comprise one or two messages, for example.

[0057] Phase 440 comprises AP 150 transmitting a request to authentication server 140. The request comprises the device nonce, and where phase 420 was present, also the network nonce and the cryptographic signature received from device 110. The request of
20 phase 440 may comprise the identifier of device 110 or the information enabling identification of the security key, to enable authentication server 140 to use a correct key when preparing a response to the request.

[0058] Phase 450 comprises authentication server 140 processing the request of phase 440. In detail, a cryptographic signature may be generated, using the security key, wherein the device nonce is among the input data provided to the cryptographic signature
25 algorithm. In embodiments where phase 420 is present, the cryptographic signature provided to AP 150 by device 110 may be verified, using the security key and the network nonce.

[0059] In phase 460, authentication server 140 informs AP 150 of the results of the
30 processing of phase 450. Optionally, in some embodiments the processing described above in connection with phase 450 take place in AP 150, rather than authentication server 140.

In this case, authentication server 140 may enable this by providing the security key to AP 150 in phase 460. In these cases, the processing described above in connection with phase 450 takes place in AP 150 in optional phase 470. In these cases, the request of phase 440 may comprise a request for the security key, the nonces and/or signature not being needed
5 in the request as AP 150 in these embodiments performs the processing of phase 450 in phase 470.

[0060] In phase 480, AP 150 may provide to device 110 the cryptographic signature obtained using the security key and the device nonce. In some embodiments, responsive to the cryptographic signature provided by device 110 being determined to be wrong, phases
10 480, and consequently also phases 490 and 4100, are absent.

[0061] In phase 490, device 110 may verify that the cryptographic signature provided by AP 150 in phase 480 is correct. To verify this, device 110 may derive, as described above, the correct signature using the security key and the device nonce, and compare the correct signature to the signature provided by AP 150. In case the verification
15 indicates the cryptographic signature is correct, device 110 may utilize network selection information provided by AP 150. The network selection information may be delivered to device 110 in phase 480, or in a separate phase, illustrated as 4100, for example.

[0062] The messaging illustrated in FIGURE 4 between device 110 and AP 150 may comprise pre-association signalling.

20 [0063] FIGURE 5 is a first flow graph illustrating a first method in accordance with at least some embodiments of the present invention. The phases of the illustrated method may take place in device 110, for example, or in a control device configured to control the functioning of device 110, when implanted therein.

[0064] Phase 510 comprises storing a first nonce. Phase 520 comprises causing
25 transmission, to a wireless access point, of a first message, the first message comprising the first nonce. The transmission may take place via a pre-association message, for example. Phase 530 comprises verifying a correctness of a first cryptographic signature comprised in a response to the first message. Finally, phase 540 comprises using information from the wireless access point in network selection responsive to the
30 cryptographic signature being verified as correct.

[0065] FIGURE 6 is a second flow graph illustrating a second method in accordance with at least some embodiments of the present invention. The phases of the illustrated method may take place in AP 150, for example, or in a control device configured to control the functioning of AP 150, when implanted therein.

5 [0066] Phase 610 comprises receiving, in an apparatus, from a user equipment, a first message, the first message comprising first nonce. Phase 620 comprises obtaining a first cryptographic signature based at least in part on the first nonce. Phase 630 comprises causing provision, to the user equipment, of the first cryptographic signature comprised in a response to the first message. Finally, phase 640 comprises causing provision, to the user
10 equipment, of network selection information. Although illustrated last, phase 640 need not take place after the other phases of the illustrated method have taken place.

[0067] It is to be understood that the embodiments of the invention disclosed are not limited to the particular structures, process steps, or materials disclosed herein, but are extended to equivalents thereof as would be recognized by those ordinarily skilled in the
15 relevant arts. It should also be understood that terminology employed herein is used for the purpose of describing particular embodiments only and is not intended to be limiting.

[0068] Reference throughout this specification to one embodiment or an embodiment means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present
20 invention. Thus, appearances of the phrases “in one embodiment” or “in an embodiment” in various places throughout this specification are not necessarily all referring to the same embodiment. Where reference is made to a numerical value using a term such as, for example, about or substantially, the exact numerical value is also disclosed.

[0069] As used herein, a plurality of items, structural elements, compositional
25 elements, and/or materials may be presented in a common list for convenience. However, these lists should be construed as though each member of the list is individually identified as a separate and unique member. Thus, no individual member of such list should be construed as a de facto equivalent of any other member of the same list solely based on their presentation in a common group without indications to the contrary. In addition,
30 various embodiments and example of the present invention may be referred to herein along with alternatives for the various components thereof. It is understood that such embodiments, examples, and alternatives are not to be construed as de facto equivalents of one another, but are to be considered as separate and autonomous representations of the

present invention.

[0070] Furthermore, the described features, structures, or characteristics may be combined in any suitable manner in one or more embodiments. In the following description, numerous specific details are provided, such as examples of lengths, widths, shapes, etc., to provide a thorough understanding of embodiments of the invention. One skilled in the relevant art will recognize, however, that the invention can be practiced without one or more of the specific details, or with other methods, components, materials, etc. In other instances, well-known structures, materials, or operations are not shown or described in detail to avoid obscuring aspects of the invention.

[0071] While the forgoing examples are illustrative of the principles of the present invention in one or more particular applications, it will be apparent to those of ordinary skill in the art that numerous modifications in form, usage and details of implementation can be made without the exercise of inventive faculty, and without departing from the principles and concepts of the invention. Accordingly, it is not intended that the invention be limited, except as by the claims set forth below.

[0072] The verbs “to comprise” and “to include” are used in this document as open limitations that neither exclude nor require the existence of also un-recited features. The features recited in depending claims are mutually freely combinable unless otherwise explicitly stated. Furthermore, it is to be understood that the use of "a" or "an", that is, a singular form, throughout this document does not exclude a plurality.

INDUSTRIAL APPLICABILITY

[0073] At least some embodiments of the present invention find industrial application in network selection, such as, for example, wireless access point selection or radio access technology selection.

ACRONYMS LIST

3GPP	3 rd generation partnership project
AP	Access point
EAP	Extensible authentication protocol
EAP-AKA	EAP-authentication and key agreement

	EAP-AKA'	EAP-AKA prime (variant of EAP-AKA)
	EAP-RP	EAP-re-authentication
	EAP-SIM	EAP-subscriber identity module
	EMSK	Extended Master Session Key
5	IEEE	Institute of electrical and electronics engineers
	IMEI	International mobile station equipment identity
	LTE	Long term evolution
	MSK	Master Session Key
	NFC	Near-field communication
10	PMKSA	Pairwise Master Key Security Association
	PMKSAID	PMKSA Identifier
	RAT	Radio access technology
	UI	User interface
	WCDMA	Wideband code division multiple access
15	Wi-Fi	Wireless local area network (WLAN)
	WiMAX	Wireless interoperability for microwave access
	WWW	World wide web

REFERENCE SIGNS LIST

110	Device of FIGURE 1
120	Base station
130	Network node
140	Authentication server
150	Access point, AP (also Authenticator)
160	Network (FIGURE 1)

210-280	Phases of FIGURE 2
300	Device of FIGURE 3
310	Processor
320	Memory
330	Transmitter
340	Receiver
350	NFC transceiver
360	User interface, UI
370	User identity module
410-4100	Phases of FIGURE 4
510-540	Phases of FIGURE 5
610-640	Phases of FIGURE 6

CLAIMS:

1. An apparatus comprising:
 - 5 – a memory configured to store a first nonce, and
 - at least one processing core configured to cause transmission, to a wireless access point, of a first message, the first message comprising the first nonce, to verify a correctness of a first cryptographic signature comprised in a response to the first message, and to use information from the wireless access point in network selection
10 responsive to the first cryptographic signature being verified as correct.
2. The apparatus according to claim 1, wherein the at least one processing core is configured to discard without using in network selection the information from the wireless access point responsive to the first cryptographic signature being verified as incorrect or
15 not present.
3. The apparatus according to any of claims 1 – 2, wherein the at least one processing core is further configured to obtain a second nonce, to calculate a second cryptographic signature based at least in part on the second nonce, and to include the second
20 cryptographic signature in the first message.
4. The apparatus according to claim 3, wherein the at least one processing core is configured to obtain the second nonce from a broadcast transmission originating in the wireless access point.
25
5. The apparatus according to claim 3, wherein the at least one processing core is configured to obtain the second nonce by requesting for it from the wireless access point.
6. The apparatus according to claim 3, wherein the at least one processing core is
30 configured to obtain the second nonce from a preselected public variable.
7. The apparatus according to any of claims 1 – 2, wherein the at least one processing core is further configured calculate a second cryptographic signature based at least in part on the first nonce, and to include the second cryptographic signature in the first message.

8. The apparatus according to any of claims 1 – 7, wherein the at least one processing core is configured to verify the correctness of the first cryptographic signature based, at least in part, on the first nonce and a security key.

5

9. The apparatus according to claim 8, wherein the at least one processing core is further configured to cause the apparatus to participate in an authentication procedure between the apparatus and an authentication server, and to store the security key in connection with the authentication procedure.

10

10. The apparatus according to any of claims 1 – 9, wherein the first message and the response to the first message are pre-association messages.

11. An apparatus comprising at least one processing core, at least one memory including computer program code, the at least one memory and the computer program code being configured to, with the at least one processing core, cause the apparatus at least to:

- receive, from a user equipment, a first message, the first message comprising a first nonce;
- obtain a first cryptographic signature based at least in part on the first nonce, and
- cause provision, to the user equipment, of the first cryptographic signature comprised in a response to the first message, and to cause provision, to the user equipment, of network selection information.

12. The apparatus according to claim 11, wherein the at least one memory and the computer program code are configured to, with the at least one processing core, cause the apparatus to obtain the first cryptographic signature based at least in part on the network selection information.

13. The apparatus according to claim 11 or 12, wherein the at least one memory and the computer program code are configured to, with the at least one processing core, cause the apparatus to obtain the first cryptographic signature, at least in part, by transmitting a request to an authentication server.

14. The apparatus according to any of claims 11 – 13, wherein the at least one memory and the computer program code are configured to, with the at least one processing core, cause the apparatus to establish a second nonce, and to verify, at least in part based on the second nonce, a second cryptographic signature, the second cryptographic signature being
5 received in the apparatus from the user equipment.

15. The apparatus according to claim 14, wherein the first message comprises the second cryptographic signature.

10 16. The apparatus according to any of claims 11 – 15, wherein the first message and the response to the first message are pre-association messages.

17. The apparatus according to any of claims 14 – 16, wherein the at least one memory and the computer program code are configured to, with the at least one processing core, cause
15 the apparatus to verify the correctness of the second cryptographic signature based, at least in part, on a security key.

18. The apparatus according to claim 17, wherein the at least one memory and the computer program code are configured to, with the at least one processing core, cause the
20 apparatus to obtain the security key from a node that has participated in an authentication procedure with the user equipment.

19. A method comprising:

- storing a first nonce;
- 25 – causing transmission, to a wireless access point, of a first message, the first message comprising the a first nonce;
- verifying a correctness of a first cryptographic signature comprised in a response to the first message, and
- using information from the wireless access point in network selection responsive to
30 the first cryptographic signature being verified as correct.

20. The method according to claim 19, further comprising discarding without using in network selection the information from the wireless access point responsive to the cryptographic signature being verified as incorrect.
- 5 21. The method according to any of claims 19 – 20, further comprising obtaining a second nonce, calculating a second cryptographic signature based at least in part on the second nonce, and including the second cryptographic signature in the first message.
22. The method according to claim 21, wherein the second nonce is obtained from a
10 broadcast transmission originating in the wireless access point.
23. The method according to claim 21, wherein the second nonce is obtained by requesting for it from the wireless access point.
- 15 24. The method according to any of claims 19 – 23, wherein the second nonce is obtained from a preselected public variable.
25. The method according to any of claims 19 – 20, further comprising calculating a second cryptographic signature based at least in part on the first nonce, and including the
20 second cryptographic signature in the first message.
26. The method according to any of claims 19 – 25, further comprising verifying the correctness of the first cryptographic signature based, at least in part, on the first nonce and a security key.
25
27. The method according to claim 26, further comprising causing the apparatus to participate in an authentication procedure between the apparatus and an authentication server, and storing the security key in connection with the authentication procedure.
- 30 28. The method according to any of claims 19 – 27, wherein the first message and the response to the first message are pre-association messages.
29. A method comprising:

- receiving, in an apparatus, from a user equipment, a first message, the first message comprising first nonce;
- obtaining a first cryptographic signature based at least in part on the first nonce;
- causing provision, to the user equipment, of the first cryptographic signature
- 5 comprised in a response to the first message, and
- causing provision, to the user equipment, of network selection information.

30. The method according to claim 29, wherein the first cryptographic signature is obtained based at least in part on the network selection information.

10

31. The method according to claim 29 or 30, wherein the first cryptographic signature is obtained by transmitting a request to an authentication server.

32. The method according to any of claims 29 – 31, further comprising causing the

15 apparatus to establish a second nonce, and verifying, at least in part based on the second nonce, a second cryptographic signature, the second cryptographic signature being received in the apparatus from the user equipment.

33. The method according to claim 32, wherein the first message comprises the second

20 cryptographic signature.

34. The method according to any of claims 29 – 33, wherein the first message and the response to the first message are pre-association messages.

25 35. The method according to any of claims 32 – 34, wherein the correctness of the second cryptographic signature is verified based, at least in part, on a security key.

36. The method according to claim 35, further comprising causing the apparatus to obtain the security key from a node that has participated in an authentication procedure with the

30 user equipment.

37. An apparatus comprising:

- means for storing a first nonce;

- means for causing transmission, to a wireless access point, of a first message, the first message comprising the first nonce;
- means for verifying a correctness of a first cryptographic signature comprised in a response to the first message, and
- 5 – means for using information from the wireless access point in network selection responsive to the first cryptographic signature being verified as correct.

38. An apparatus comprising:

- 10 – means for receiving, in an apparatus, from a user equipment, a first message, the first message comprising a first nonce;
- means for obtaining a first cryptographic signature based at least in part on the first nonce;
- means for causing provision, to the user equipment, of the first cryptographic signature comprised in a response to the first message, and
- 15 – means for causing provision, to the user equipment, of network selection information.

39. A non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least:

- 20 – store a first nonce;
- cause transmission, to a wireless access point, of a first message, the first message comprising the first nonce;
- verify a correctness of a first cryptographic signature comprised in a response to the first message, and
- 25 – use information from the wireless access point in network selection responsive to the first cryptographic signature being verified as correct.

40. A non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least:

- 30 – receive, in an apparatus, from a user equipment, a first message, the first message comprising a first nonce;

- obtain a first cryptographic signature based at least in part on the first nonce;
- cause provision, to the user equipment, of the first cryptographic signature comprised in a response to the first message, and
- cause provision, to the user equipment, of network selection information

5

41. A computer program configured to cause a method in accordance with at least one of claims 19 - 36 to be performed.

10

1/6

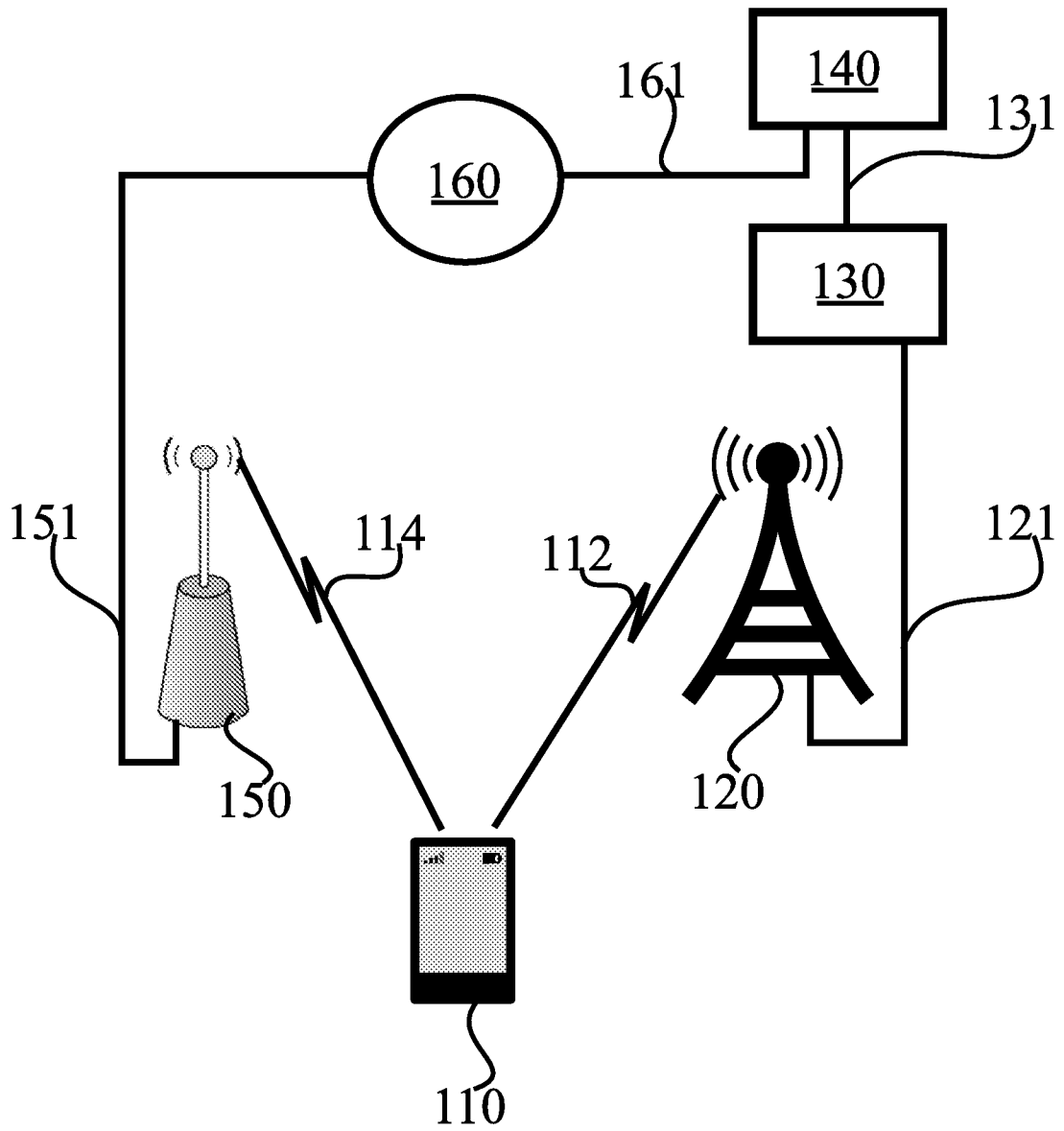


FIGURE 1

2/6

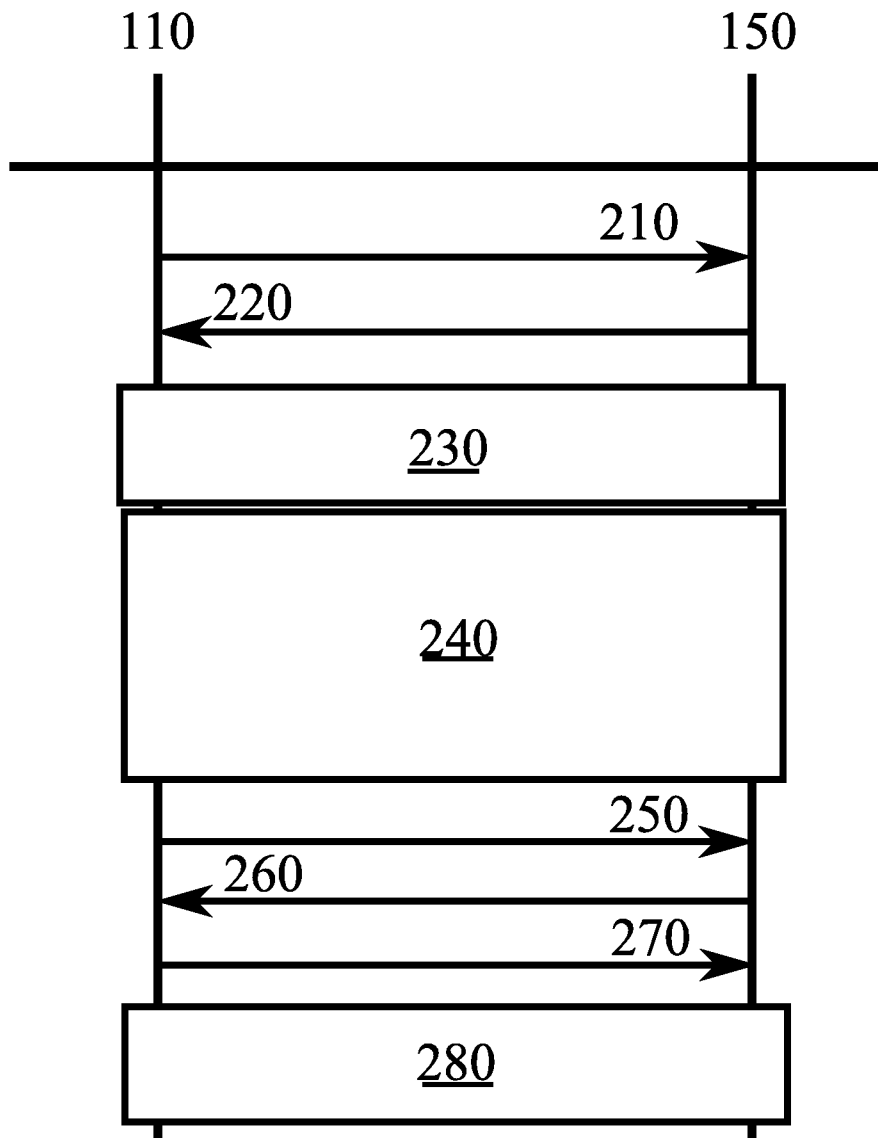


FIGURE 2

3/6

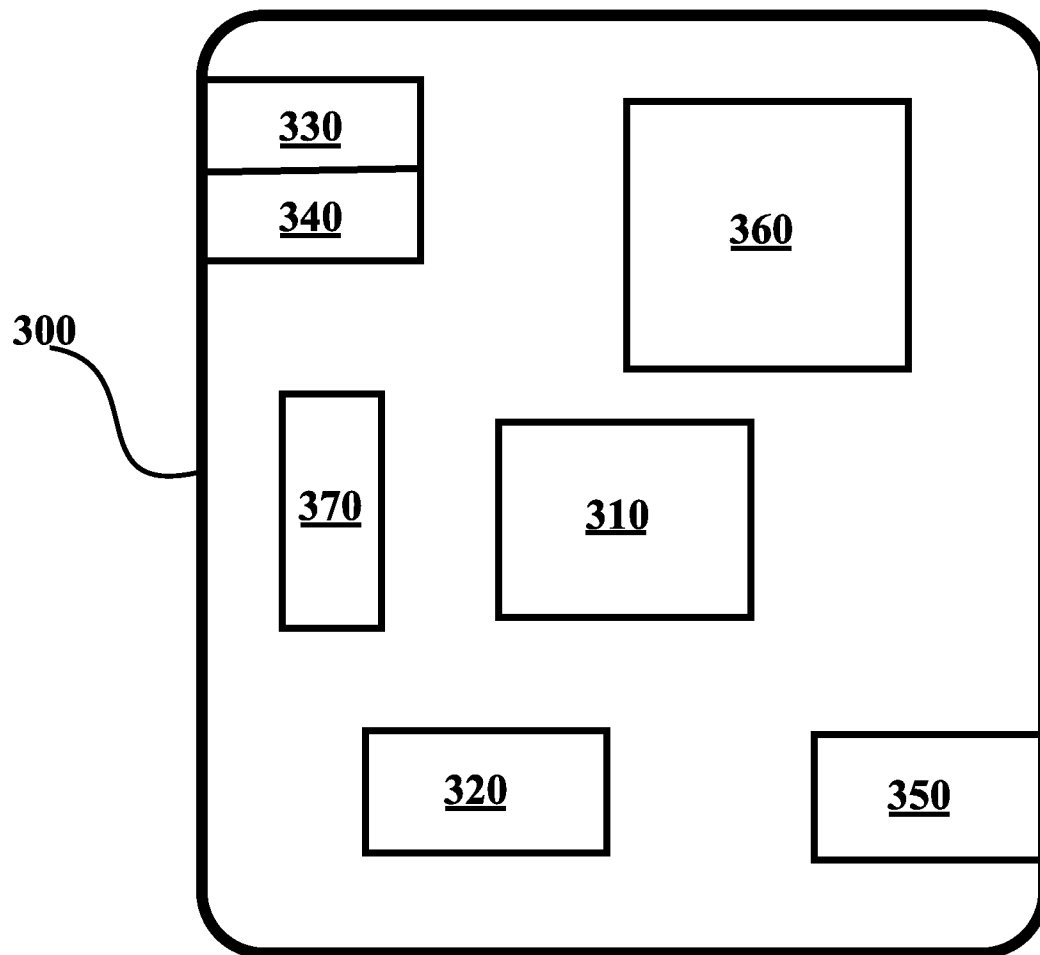


FIGURE 3

4/6

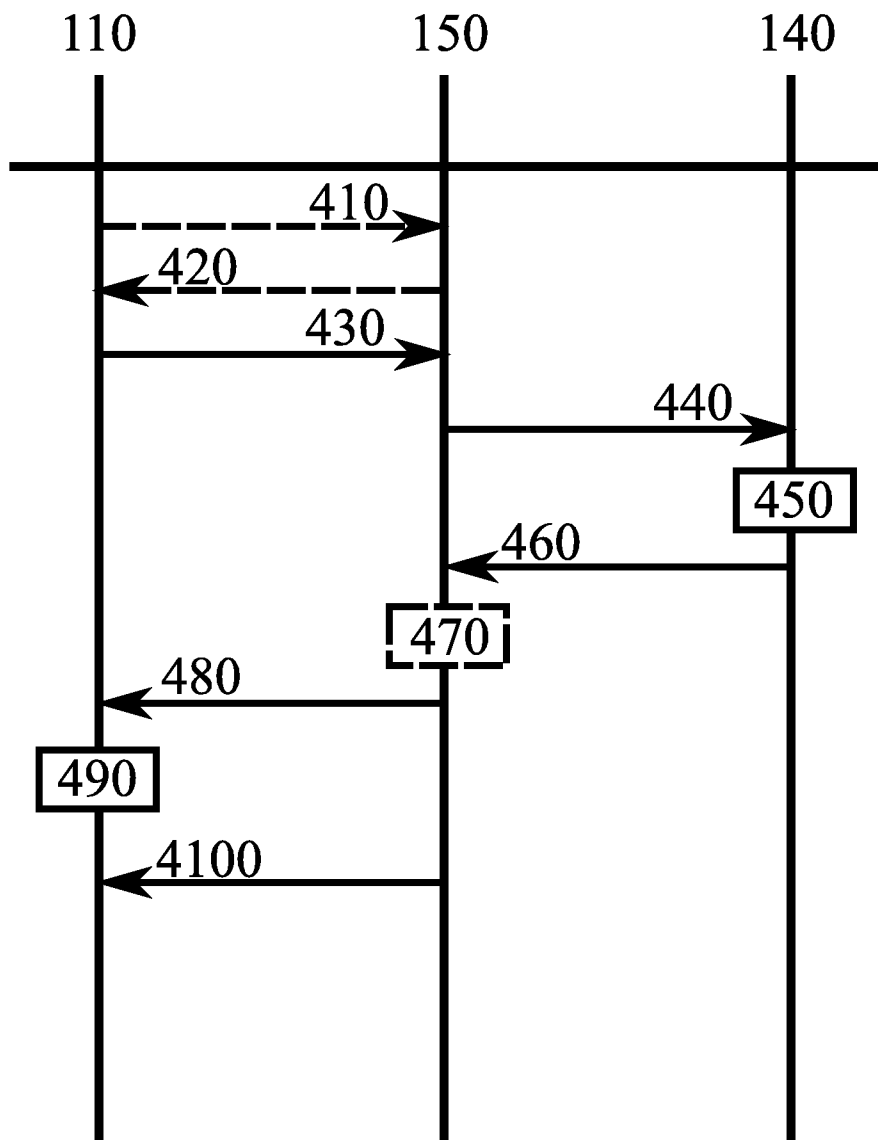


FIGURE 4

5/6

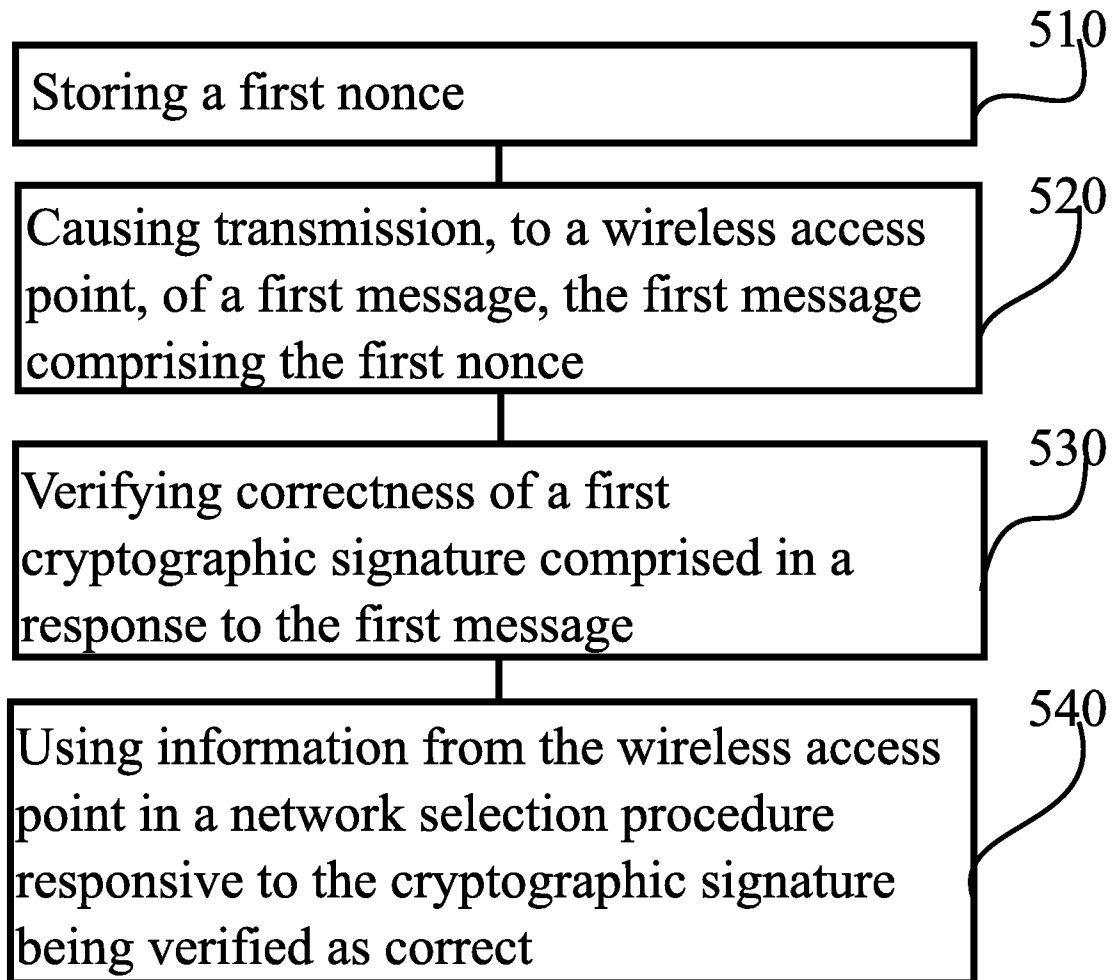


FIGURE 5

6/6

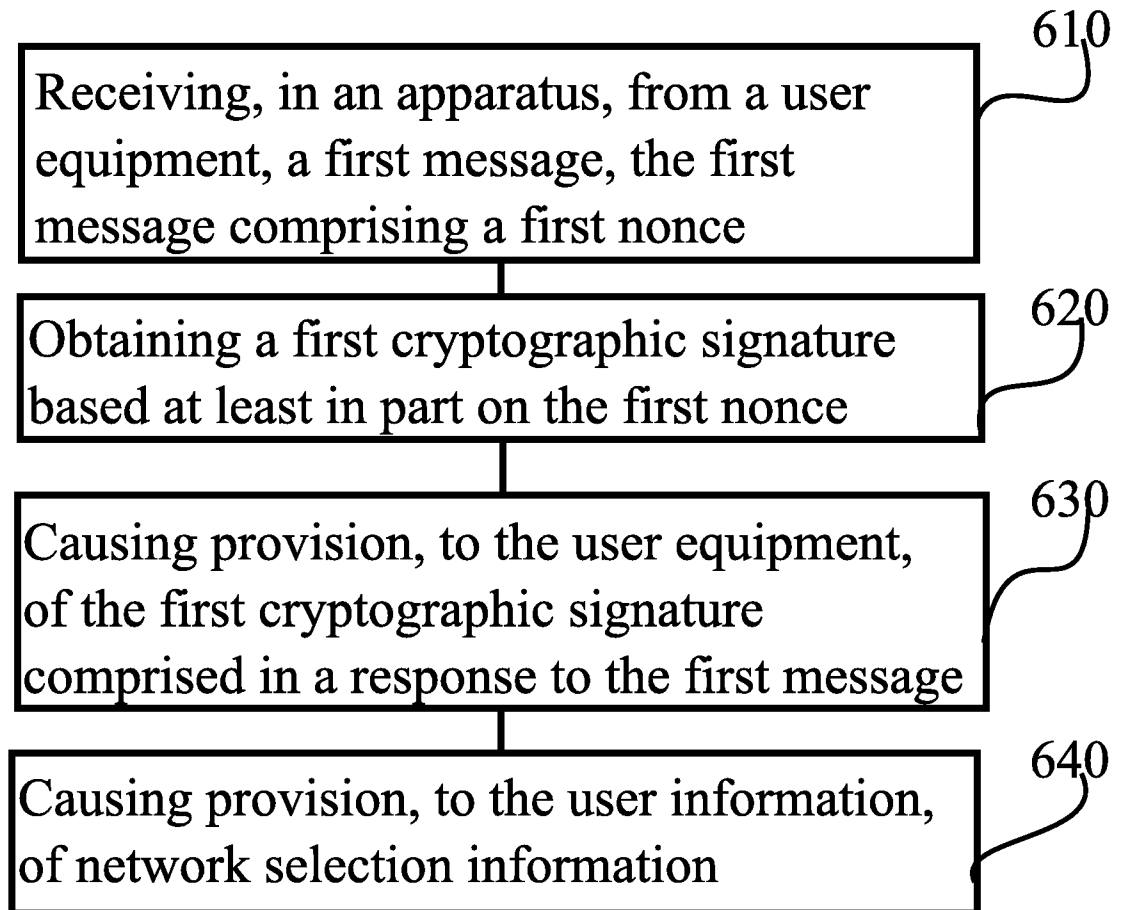


FIGURE 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2015/050434

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

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)

IPC: H04L, H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
FI, SE, NO, DK

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

EPO-Internal, WPIAP

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2424192 A2 (CISCO TECH INC [US]) 29 February 2012 (29.02.2012) abstract; pars. [0019], [0032]-[0034], [0037], [0047]-[0049], [0076]-[0090]; figs. 3A, 6, 11, 12	1-41
X	WO 2007080490 A1 (NOKIA CORP [FI]) 19 July 2007 (19.07.2007) abstract; pars. [0034]-[0036]; fig. 4	1, 11, 19, 29, 37-41
A	US 2009217043 A1 (METKE ANTHONY E [US] et al.) 27 August 2009 (27.08.2009) abstract; pars. [0032]-[0036]; fig. 3	1-41
A	US 2014033288 A1 (WYNN SIMON [US] et al.) 30 January 2014 (30.01.2014) the whole document	1-41
A	WO 2011134496 A1 (NOKIA SIEMENS NETWORKS OY [FI]) 03 November 2011 (03.11.2011) the whole document	1-41

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search

21 September 2015 (21.09.2015)

Date of mailing of the international search report

23 September 2015 (23.09.2015)

Name and mailing address of the ISA/FI
Finnish Patent and Registration Office
P.O. Box 1160, FI-00101 HELSINKI, Finland
Facsimile No. +358 9 6939 5328

Authorized officer
Petri Bergholm
Telephone No. +358 9 6939 500

INTERNATIONAL SEARCH REPORT
Information on Patent Family Members

International application No.
PCT/FI2015/050434

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
EP 2424192 A2	29/02/2012	US 2012054106 A1 US 8566596 B2 US 2014122242 A1	01/03/2012 22/10/2013 01/05/2014
WO 2007080490 A1	19/07/2007	US 2007184832 A1	09/08/2007
US 2009217043 A1	27/08/2009	US 8001381 B2 EP 2272271 A2 KR 20100103721 A WO 2009108523 A2	16/08/2011 12/01/2011 27/09/2010 03/09/2009
US 2014033288 A1	30/01/2014	US 2014095406 A1 WO 2014018808 A1	03/04/2014 30/01/2014
WO 2011134496 A1	03/11/2011	EP 2564639 A1 US 2013034019 A1	06/03/2013 07/02/2013

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2015/050434

CLASSIFICATION OF SUBJECT MATTER

IPC
H04L 29/06 (2006.01)
H04W 48/18 (2009.01)