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

(19) **World Intellectual Property Organization**
International Bureau

(43) **International Publication Date**
12 August 2010 (12.08.2010)

PCT

(10) **International Publication Number**
WO 2010/090569 A1

(51) **International Patent Classification**:
H04W 12/04 (2009.01) ***H04W 8/20*** (2009.01)
H04L 9/32 (2006.01)

(21) **International Application Number**:
PCT/SE2009/051092

(22) **International Filing Date**:
1 October 2009 (01.10.2009)

(25) **Filing Language**: English

(26) **Publication Language**: English

(30) **Priority Data**:
61/150,118 5 February 2009 (05.02.2009) US

(71) **Applicant** *(for all designated States except US)*: **Telefonaktiebolaget LM Ericsson (publ)** [SE/SE]; S-164 83 Stockholm (SE).

(72) **Inventors; and**

(75) **Inventors/Applicants** *(for US only)*: **BARRIGA, Luis** [SE/SE]; c/o Pena, Burspråksvägen 4, 1tr, S-121 47 Johanneshov (SE). **DYSENIUS, Per-Anders** [SE/SE]; Hagalundsvägen 52, S-374 40 Karlshamn (SE). **LINDSTRÖM, Magnus** [SE/SE]; Mölltorpsvägen 2, S-371 92 Karlskrona (SE).

(74) **Agents**: **BRANN AB** et al.; Västgötagatan 2, S-104 62 Stockholm (SE).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM,

[Continued on next page]

(54) **Title**: APPARATUSES AND A METHOD FOR PROTECTING A BOOTSTRAP MESSAGE IN A NETWORK

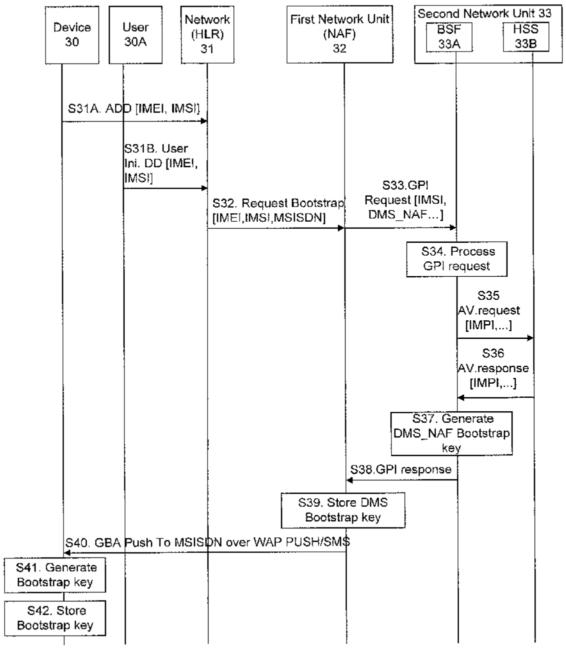

FIGURE 3

(57) **Abstract**: The embodiments of the present invention relate to apparatuses in the form of a first network unit and a device, and also relates to a method for enabling protection of a bootstrap message in a device management network system. The method comprises: receiving at the first network unit, a request to bootstrap the device; transmit a request for a bootstrap key, to a second network unit; receiving a message comprising the bootstrap key and further comprises trigger information and transmitting the trigger information to the device to trigger generation of the bootstrap key internally in the device. Thereafter a protected bootstrap message can be transmitted to the device from the first network unit, and when the device verifies and/or decrypts the bootstrap message, device management (DM) sessions can start between the device and the first network unit.

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

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

Published:

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

APPARATUSES AND A METHOD FOR PROTECTING A BOOTSTRAP MESSAGE IN A NETWORK

TECHNICAL FIELD

The present invention relates generally to the field of mobile or wireless communications network systems, and, more specifically, to apparatuses and a method for securely protecting a bootstrap message during the bootstrapping of a device in a device management network system.

BACKGROUND

Mobile devices need to be configured with various settings to control and to provide various functions and support various services. One known method of configuration of mobile devices with service related data is via, for example, short message service (SMS) or wireless application protocol (WAP). This is a unidirectional path and to be able to perform bidirectional service, open mobile alliance (OMA) has specified protocols, data models and policies for device management (DM). As an example, *OMA DM version 1.2.1 enabler release specifications* available at URL:http://www.openmobilealiance.org, defines how a DM session is established and maintained. One of the important functions in these specifications includes a bootstrap specification that describes methods for a device to be provisioned with OMA DM settings prior to initiating a management session. The OMA DM bootstrap technical specifications are described in *OMA DM Bootstrap version 1.2.., OMA-TS-DM_Bootstrap V1_2_1. Open Mobile Alliance, June 2008.*

Bootstrap is a process of provisioning a DM client of a mobile or a wireless device, to move the device from an un-provisioned, empty state, to a state where it is able to initiate a management session to a DM server and later to e.g. new DM servers. There are three different ways to perform a bootstrap process: customized bootstrap; server initiated bootstrap and bootstrap from a smartcard.

In the customized bootstrap process, devices are loaded with OMA DM bootstrap information at manufacture. This is also referred to as factory bootstrap.

In the server initiated bootstrap process, a server is configured to send out bootstrap information via some push mechanism e.g. WAP push. For this process, the server must receive the device address/phone number beforehand.

In the bootstrap process from the smartcard, the smartcard (e.g. subscriber identity module (SIM) or universal SIM (USIM)) is inserted in the device and the DM client is bootstrapped from the smartcard.

There are, however, several problems and drawbacks associated with systems using these processes. The customized bootstrap process requires that the basic parameters are known at the time of manufacture or at the time of selling the device. The server initiated bootstrap process specifies that the international mobile subscriber identity (IMSI) must be used to encode the basic DM parameters when the DM server performs a bootstrap over the air interface. This is done by sending an encrypted SMS with the basic parameters to the device. The key used for encryption is the IMSI for e.g. second generation/third generation network system, or the electronic serial number (ESN) for code division multiple access (CDMA) system. The IMSI or the ESN have however not been designed to be secret. This also means that the bootstrap message to be transmitted from the DM server to the device is weakly protected. As a result, an attacker can create its own bootstrap message in order to bootstrap a device that would be locked to a malicious DM server. Another drawback is that an attacker can eavesdrop the bootstrap message that is only integrity protected. Since the bootstrap message may contain credentials such as username and password, the attacker can impersonate the device.

Figure 1 illustrated a high level view of a server initiated bootstrap process, as defined in the above cited specifications *OMA DM Bootstrap version 1.2.1, OMA-TS-DM_Bootstrap V1_2_1*. The scenario of figure 1 describing the service initiated bootstrap, shows a device 10, a user 11, a network 12 and a DM server (DMS) 13. In *OMA-TS-DM_Bootstrap V1_2_1*, it is described that once the user 11 acquires the device 10 and personalizes it, e.g. by inserting a SIM, the prerequisites for the bootstrapping process are in place. The DMS 13 is notified or informed of the identity, address or phone number of the device 10 by e.g. the network 12 the first time the device 10 registers to the network 12. When this happens a request to bootstrap the device 10 can be sent from the (core) network 12 to the DMS 13 with the number used by the device 10. The DMS 13 is now in a position where it can send out an OMA DM bootstrap message. This bootstrap message contains information for the device 10 to be able to initiate a management session with DMS 13 that sent out the bootstrap message.

The weak protection of the bootstrapping scenario described above, stems from the fact that the bootstrap message are, as mentioned above, only protected with a non-secret key (IMSI or ESN) as indicated in section 5.7.2.3.1 in *OMA Device Management Security 1.2.1, OMA-TS-DM_Security-V1_2_1, OMA, 2008*. Thus neither IMSI nor ESN is considered a shared secret from security standpoint. Similar OMA specifications also suffer from the same surety weaknesses, such as *Enable Release Definition for OMA Client Provisioning Specifications version 1.2. OMA-ERELD-ClientProvisioning-V1_1;* and *Provisioning Bootstrap 1.1. OMA-WAP-ProvBoot-V1_1.*

It should be mentioned that these security vulnerabilities are the reasons why the security group (SA3) in the 3rd generation partnership project (3GPP) has issued a strong recommendation to not use the server initiated bootstrap method/process as indicated in *3GPP LS reply S3-080262*.

Another prior art disclosed in US patent application US 2008/0155071 proposes a method and a system for bootstrap of a device in a communications network. In this prior art, a server initiated bootstrapping is used to first provision a smartcard of a device using over the air (OTA) technology so that the device can bootstrap from the smartcard. This is performed by combining bootstrap through the smartcard with the 3GPP automatic device detection (ADD) function. The 3GPP ADD, which is defined in the technical specification *3GPP TS 22.101*, enables automatic detection of a device when the device appears in the network. However, the method of this prior art still relies on the lack of security of the current OMA DM specified Server Initiated bootstrap as described earlier.

SUMMARY

It is thus an object of the exemplary embodiments of the present invention to address the above mentioned problems and to provide apparatuses and a method that allow secure and protected transmission of bootstrap messages from a DM server to a device thereby preventing eavesdroppers and/or attackers to impersonate the device and/or to hijack the device.

According to a first aspect of exemplary embodiments of the present invention, the above stated problems are solved by means of a first network unit of a DM network system, for enabling protection of a bootstrap message. The first network unit comprises a receiver configured to receive a first message comprising a request to bootstrap a device, the message comprising information identifying the device and information identifying a subscriber. The first network unit further comprises a transmitter configured to send a second message comprising the information identifying the subscriber, to a second network unit, the second message requesting the second network unit to provide the first network unit with a bootstrap key that is based on the information identifying the subscriber. The receiver is further configured to receive from the second network unit, a third message comprising the bootstrap key to be used for protection of the bootstrap message. The third message also comprises trigger information which is transmitted to the device to trigger generation of the bootstrap key in the device.

As the trigger information is received from the first network unit, the device generates internally the bootstrap key. When both the first network unit and the device are in possession of the bootstrap key, the first network unit protects, based on the bootstrap key, the bootstrap message and transmits the protected bootstrap message to the device. This way, an attacker cannot hijack or impersonate the device since the secret bootstrap key is known only to the DM network and to the device.

According to another aspect of exemplary embodiments of the present invention, the above stated problems are solved by means of a method in a first network unit of a DM network, for enabling protection of a bootstrap message. The method comprising: receiving a first message comprising a request to bootstrap a device, the first message comprising information identifying the device and a subscriber. The method further comprises, transmitting a second message comprising the information identifying the subscriber to a second network unit, requesting the second network unit to provide the first network unit with a bootstrap key that is based on the information identifying the subscriber. The method further comprises, receiving from the second network unit a third message comprising the bootstrap key, for enabling protection of the bootstrap message, the third message further comprising trigger information. The method further comprises, transmitting the trigger information to the device in order to trigger generation of the bootstrap key in the device.

According to yet another aspect of the exemplary embodiments of the present invention, the above stated problems are solved by means of a device capable in communicating with a first network unit of a DM network system for enabling protection of a bootstrap message. The device comprises means for notifying the first network unit of information identifying the device and a subscriber. The device further comprises a receiver configured to receive from the first network unit, trigger information to trigger generation of the bootstrap key in the device. The receiver is further configured to receive a protected bootstrap message protected based on the bootstrap key, and the device comprises means for verifying and/or decrypting the protected bootstrap message.

An advantage of the exemplary embodiments of the present invention is to prevent attackers from hijacking a device and/or impersonate the device.

Another advantage of the exemplary embodiments of the present invention is to make sure to use a truly secret bootstrap key that is known only to the network and the device.

Still other advantages, objects and features of the embodiments of the present invention will become apparent from the following detailed description in conjunction with the accompanying drawings, attention to be called to the fact, however, that the following drawings are illustrative only, and that various modifications and changes may be made in the specific embodiments illustrated as described within the scope of the appended claims. It should further be understood that the drawings are not necessarily drawn to scale and that, unless otherwise indicated, they are merely intended to conceptually illustrate the structures and procedures described herein.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a prior art high level view of signalling involved during a server initiated bootstrap procedure.

Figure 2 is a flow diagram for enabling secure server initiated bootstrapping of a device according to an exemplary embodiment of the present invention.

Figure 3 is another flow diagram for secure server initiated bootstrapping of a device according to another exemplary embodiment of the present invention

Figure 4 is a diagram illustrating a flowchart of a method for use in a first network unit according to exemplary embodiments of the present invention.

Figure 5 illustrates a block diagram of an exemplary network unit according to exemplary embodiments of the present invention.

Figure 6 illustrates a block diagram of an exemplary device according to exemplary embodiments of the present invention.

DETAILED DESCRIPTION

In the following description, for purposes of explanation and not limitation, specific details are set forth such as particular architectures, scenarios, techniques, etc. in order to provide thorough understanding of the present invention. However, it will be apparent from the following that the present invention and its embodiments may be practiced in other embodiments that depart from these specific details.

The exemplary embodiments of the present invention are described herein by way of reference to particular example scenarios. In particular the invention is described in a non-limiting general context in relation to server initiated bootstrap scenario in a device management (DM) network system comprising DM server (DMS) interacting with a generic bootstrapping architecture (GBA) according to GBA push specifications in the 3GPP technical specifications TS 33.223. The DMS is hereinafter denoted a first network unit. Note however that the first network unit may be any suitable network unit or node capable in implementing the exemplary embodiments of the present invention. Such a network unit can e.g. be represented by a DM proxy instead of a DMS.

Referring to figure 2 there is illustrated a flow diagram for enabling secure server initiated bootstrapping of a device in a network system, in accordance with an exemplary embodiment of the present invention. The entities that are shown are: the device 20, a network entity (or entities) 21 (e.g. a home location register), a first network unit 22 and a second network unit

23. As will be illustrated and described later, additional nodes/functions can also be used for the purpose of secure bootstrapping of a device.

As shown in figure 2, the device 20 notifies the network 21 of its availability (S21). This can be done by the user/subscriber turning on the device 20 attempting to attach to the network 21. Via e.g. known automatic device detection (ADD) methods, as disclosed in *3GPP TS 22.101*, or known user-initiated procedures as described in *GBA Push 3GPP TS 33.223*, the network 21 detects the presence/availability of the device 20 (S22). Upon attachment to the network 21, the device 20 sends information identifying the device i.e. its device identity e.g. IMEI and also sends information identifying the subscriber e.g. IMSI/ESN. In bootstrap request (S23) the network 21 requests the first network unit 22 to bootstrap the device 20. In the bootstrap request (S23), the network 21 (e.g. HLR) includes the information identifying the device (IMEI) and the information identifying the subscriber i.e. IMSI/ESN, MSISDN etc. When the first network unit 22 receives the request, and based on the information identifying the device and user/subscriber, the first network unit 22 determines if GBA PUSH can be used towards the device. If so, the first network unit 22 transmits a message (S24) to the second network unit 23 requesting the second network unit 23 to provide the first network unit 22 with a bootstrap key. The second network unit 23 which is part of the GBA subsystem comprises a bootstrapping server function (BSF) and a home subscriber server (HSS).

It should be mentioned that if the first network unit 22 determined that GBA PUSH can be used towards the device, a network application function (NAF) of the first network unit 22 is configured to contact the BSF using GBA PUSH procedures to request, using message (S24), at least a trigger information and a bootstrap key. The trigger information corresponds to GBA PUSH information (GPI). Message (S24) also comprises the NAF identity. Note however that the first network unit 22 is configured to select a method for bootstrapping the device 20, being then GBA PUSH based one of the secure ones. Should GBA PUSH be selected, based on information identifying the device and the subscriber, then NAF of the first network unit 22 handles the secure bootstrapping process. In the following it is described the case when GBA PUSH can be used towards the device 20 i.e. request message (S24) reaches the second network unit 23.

Referring back to figure 2, when the second network unit 23 receives the request message (S24), it generates the bootstrap key (S25) and sends or delivers the bootstrap key and at least the GPI to the first network unit (22) in a response message (S26) denoted here GPI response. Now that the first network unit 22 is in possession of the GPI response, it transmits or forwards the trigger information i.e. the GPI part in the GPI response to the device 20 (S27). The first network unit 22 can also store the bootstrap key prior to transmitting the GPI to the device 20. The GPI or trigger information can be transmitted over SMS, WAP, HTTP, SIP push or any bearer suitable for conveying the trigger information to trigger the generation of the bootstrap key in the device 20. Upon reception of the GPI, the device 20 generates the bootstrap key (S28) using suitable standard procedures.

In *GBA Push 3GPP TS 33.223,* it is disclosed that the GPI is protected. This is known as GPI integrity protection and GPI confidentiality protection. And that in GBA the bootstrap key is denoted Ks_NAF and this key is also known as key material or keying material. Ks_NAF is described in *3GPP TS 33.220 V8.5.0* which is referred to in the above mentioned prior art *GBA Push 3GPP TS 33.223.* Throughout the description, a bootstrap key is used to mean Ks_NAF or key/keying material.

Referring back to figure 2, when the device 20 generates the bootstrap key (S28) it stores the bootstrap key. Subsequently, a secure bootstrapping can be performed by the first network unit 22 by protecting and transmitting a bootstrap message which is protected based on the bootstrap key (S29). The first network unit 22 can directly protect the bootstrap message using the bootstrap key or can derive further keys using the bootstrap key and use these keys to protect the bootstrap message. Note that if the first network unit 22 has encrypted the bootstrap message prior to transmitting it to the device 20, the device 20 needs to first decrypt the bootstrap message and then verify the message. The bootstrap key can instead of IMSI/ESN, be used for integrity protection and/or can be used for confidentiality protection.
After successful and secure bootstrapping of the device, DM sessions can start between the device 20 and the first network unit 22. Note that the bootstrap key can also be used as a master key to further generate keys that can be used to protect one or more DM sessions between the device 20 and the first network unit 22 e.g. authentication, after successful verification/decryption of the bootstrap message.

Referring to figure 3, there is illustrated a flow diagram for enabling secure server initiated bootstrapping of a device in a network system, in accordance with another exemplary embodiment of the present invention. Similarly to figure 2, the network system comprises a device 30, a network 31 (e.g. HLR), a first network unit 32 (e.g. DMS with a NAF) and a second network unit 33 comprising a BSF 33A and a HSS 33B. Figure 3 also depicts a user 30A. In (S31A), upon attachment to the network 31, the device 30 sends information identifying the device, IMEI, and also sends information identifying the user/subscriber (e.g. IMSI). As mentioned earlier, this can be done using some form of ADD procedure and/or user initiated procedure. It should be mentioned that a user/subscriber 30A can alternatively notify the network 31 about the IMEI and IMSI (S31B). This can be performed by a seller at a point of sale consoles or by the end-user himself via a web interface or using e.g. DMTF tones.

In (S32), when the network 31 has detected the device/user/subscriber identified by e.g. IMSI/ESN, MSISDN and IMEI, the network 31 sends a request to bootstrap the device 30, to the first network unit 32 (e.g. DMS (NAF)) and includes in the request IMEI, IMSI (or ESN) and MSISDN. As mentioned earlier, the first network unit 32 or the NAF of the first network unit 32 first determines based on the device and user/subscriber information if GBA PUSH can be used towards the device 30. If so, the NAF part of the first network unit 32 sends a GPI request (S33) using GBA PUSH procedures, to the BSF 33A of the second network unit 33, to request a GPI response. The request (S33) comprises information indentifying the subscriber e.g. IMSI and at least the identity of the NAF (DMS_NAS_Id). When the BSF 33A receives the request it processes the request (S34) and identifies the user/subscriber. Thereafter, the BSF 33A sends a request (S35) to the HSS 33B of the second network unit 33, requesting the HSS 33B of an authentication vector (AV) for the device 30. In the AV request (S35), the IMPI is indicated. In (S36) the HSS 33B returns the requested AV in an AV response. The BSF 33A then generates (S37) a bootstrap key which is a DMS NAF bootstrap key and stores the key. The BSF 33A sends in (S38) a GPI response comprising the bootstrap key and at least a GPI comprising GPI parameters, to the first network unit 32. The first network unit 32 stores the bootstrap key (S39) and prepares a GPI package comprising the trigger information (i.e. GPI) prior to sending the GPI package to the device 30 (S40). As mentioned earlier any suitable bearer can be used to convey the GPI to the device 30 e.g. GPI over WAP PUSH or SMS or SIP etc. The MSISDN can be used to address the device 30.

When the device 30 receives the GPI, the device 30 generates internally the DMS NAF bootstrap key (S41) and the device 30 stores the bootstrap key (S42). Thereafter a bootstrap message is protected by the first network unit 32 based on the bootstrap key, and transmits the protected bootstrap message to the device 30 (not shown). The device then verifies and/or decrypts the bootstrap message. If verification and/or decryption is successful DM sessions begin between the device and the first network unit (not shown). This way only the first network unit and the device are aware of the bootstrap key thereby preventing eavesdroppers and attackers to hijack the device or to impersonate the device.

Similarly to the previously described exemplary embodiment, both the first network unit and the device can use the bootstrap key to generate further keys. The first network unit uses the further keys to protect the bootstrap message and the device can use the further keys to verify and/or decrypt the bootstrap message.

Referring to figure 4 there is illustrated the main steps of the method or procedure, in a first network unit, for enabling protection of a bootstrap message in accordance with the previously described exemplary embodiments of the present invention. As shown in figure 4, the main steps of the method comprise:

(401) receiving, a first message (i.e. a request to bootstrap a device) comprising information identifying the device and information identifying a subscriber;

(402) transmitting a second message (i.e. a GPI request) comprising the information identifying the subscriber, to a second network unit, requesting the second network unit to provide the first network unit with a bootstrap key that is based on the information identifying the subscriber;

(403) receiving, from the second network unit, a third message (i.e. GPI response) comprising the bootstrap key and a trigger information (i.e. GPI), for enabling protection of the bootstrap message;

(404) transmitting the trigger information to the device to trigger generation of the bootstrap key internally in the device.

Additional method steps and functions of the first network unit have already been discussed and are therefore not repeated.

Referring to figure 5 there is illustrated a block diagram of an exemplary first network unit 500, e.g., a DMS, of a DM network system, for enabling protection of a bootstrap message, in accordance with previously described exemplary embodiments of the present invention. As shown in figure 5, the first network unit 500 comprises a receiver 510 (RX) configured to receive a first message comprising a request to bootstrap a device. The first message comprises information identifying the device and the subscriber. The first network unit 500 further comprises a transmitter 520 (TX) configured to transmit a second message (i.e. GPI request) comprising the information identifying the subscriber, to a second network unit (e.g. BSF+HSS), requesting the second network unit to provide it with the bootstrap key. The receiver 510 of the first network unit 500 is further configured to receive a third message (i.e. GPI response) comprising the bootstrap key for enabling protection of the bootstrap message. The third message further comprises a trigger information (i.e. GPI). The transmitter 520 of the first network unit 500 is further configured to transmit the trigger information to the device to trigger generation of the bootstrap key in the device. The first network unit 500 further comprises storage means 530 for storing the bootstrap key. The first network unit 500 further comprises a processing logic/unit 540 configured to determine if GBA PUSH can be used towards the device and is further configured to generate further/additional keys based on the bootstrap key, and to protect the bootstrap message. The storage means 530 and the processing logic/unit 540 are shown as being part of a processing system 550, although this is not necessary.

Although figure 5 shows exemplary components of the first network unit 500, in other implementations, the first network unit 500 may contain fewer, different, or additional components than depicted in figure 5. In still other implementations, one or more components of unit 500 may perform the tasks described as being performed by one or more other components of the first network unit 500.

Referring to figure 6 there is illustrated a diagram of exemplary components of device 600 in accordance with some exemplary embodiments of the present invention. As illustrated, the device 600 comprises a transceiver 610 comprising means for notifying a first network unit (of figure 5) of the DM network system of information identifying the device and the subscriber for enabling protection of a bootstrap message. The means for notifying can be viewed as a transmitter of the transceiver 610. The transceiver 610 further comprises a receiver configured to receive from the first network unit trigger information (i.e. GPI) to trigger generation of a bootstrap key internally in the device. The receiver of the transceiver 610 is further configured to receive a protected bootstrap message which the first network unit protected based on the bootstrap key. An antenna 620 is also shown connected to the transceiver 610. The device 600 further comprises means for verifying and/or decrypting the protected bootstrap message. Processing unit/means 630 of the device 600 is configured to generate the bootstrap key and to perform the verification/decryption of the protected bootstrap message. The device 600 may include several antennas (only one antenna 620 is shown) a memory or storage means 640 for storing the bootstrap key, an input device(s) 650, an output device(s) 660, and a bus 670. Although figure 6 shows exemplary components of device 600, in other implementations, device 600 may contain fewer, different, or additional components than depicted in figure 6.

The present invention and its exemplary embodiments can be realized in many ways. For example, one embodiment of the present invention includes a computer-readable medium having program instructions stored thereon that are executable by a computer of the first network unit to perform the method steps of the exemplary embodiments of the present invention as previously described.

While the invention has been described in terms of several preferred embodiments, it is contemplated that alternatives, modifications, permutations and equivalents thereof will become apparent to those skilled in the art upon reading of the specifications and upon study of the drawings. It is therefore intended that the following appended claims include such alternatives, modifications, permutations and equivalents as fall within the scope of the present invention.

CLAIMS

1. A first network unit (500) of a device management, DM, network system, for enabling protection of a bootstrap message, the first network unit (500) comprising:

   - a receiver (510) configured to receive a first message comprising a request to bootstrap a device (600), said first message comprising information identifying said device (600) and information identifying a subscriber;

   - a transmitter (520) configured to send a second message comprising the information identifying said subscriber, to a second network unit, said second message requesting the second network unit to provide the first network unit (500) with a bootstrap key that is based on the information identifying the subscriber;

   - said receiver (510) is further configured to receive from the second network unit, a third message comprising said bootstrap key, for enabling protection of the bootstrap message, said third message further comprising trigger information; and

   - said transmitter (520) is further configured to transmit the trigger information to the device (600) to trigger generation of the bootstrap key in the device (600).

2. The first network unit (500) according to claim 1 further comprises storage means (530) configured to store the bootstrap key; said first network unit (500) is further configured to protect, based on the bootstrap key, the bootstrap message prior to said transmitter (520) transmitting the protected bootstrap message to the device (600).

3. The first network unit (500) according to claim 1 or claim 2 wherein said transmitter (520) is configured to transmit the trigger information in a generic bootstrapping architecture push information, GPI, message, and wherein said receiver (510) is configured to receive said third message comprising the bootstrap key in a GPI response message.

4. The first network unit (500) according to anyone of claims 1-3 is further configured to use the bootstrap key as a master key to generate additional keys for protection at least one message during at least one DM session between the device (600) and the DM network system, after verification of the bootstrap message.

5. A device (600) capable in communicating with a first network unit (500) of a device management, DM, network system for enabling protection of a bootstrap message, the device (600) comprising:

- means (610) for notifying the first network unit (500) of information identifying the device and information identifying a subscriber ;

- a receiver (610) configured to receive from the first network unit (500), trigger information to trigger generation of a bootstrap key in the device;

- said receiver (610) is further configured to receive a protected bootstrap message, said bootstrap message is protected based on the bootstrap key; and

- means (630) for verifying and/or decrypting the protected bootstrap message.

6. The device (600) according to claim 5 wherein said receiver (610) is configured to receive the trigger information in a generic bootstrapping architecture, GBA, push information, GPI, message.

7. The device (600) according to claim 5 or 6 further comprises storage means (640) configured to store the bootstrap key.

8. A method in a first network unit (500) of a device management, DM, network system, for enabling protection of a bootstrap message, the method comprising:

- (401) receiving at said first network unit, a first message comprising a request to bootstrap a device, said first message comprising information identifying said device and information identifying a subscriber;

- (402) transmitting a second message comprising the information identifying said subscriber to a second network unit, said second message requesting the second network unit to provide the first network unit with a bootstrap key that is based on the information identifying the subscriber;

- (403) receiving from the second network unit, a third message comprising said bootstrap key, for enabling protection of the bootstrap message, said third message further comprising trigger information; and

- (404) transmitting said trigger information, to the device, to trigger generation of the bootstrap key in the device.

9. The method according to claim 8 further comprises storing the bootstrap key in said first network unit and protecting, based on the bootstrap key, the bootstrap message prior to transmitting the bootstrap message to the device.

10. The method according to claim 8 or claim 9 wherein said transmitting (404) of the trigger information comprises transmitting said trigger information in a generic bootstrapping architecture push information, GPI, message, and wherein said receiving (403) of the third message comprises receiving said third message in a GPI response message

11. The method according to anyone of claims 8-10 further comprises using the bootstrap key as a master key to generate additional keys for protecting at least one message during at least one DM session between the device and the DM network system, after verification of the bootstrap message.

12. A computer program comprising program instructions for causing a computer to perform the method of anyone of method claims 8-11 when said program is run on a computer.

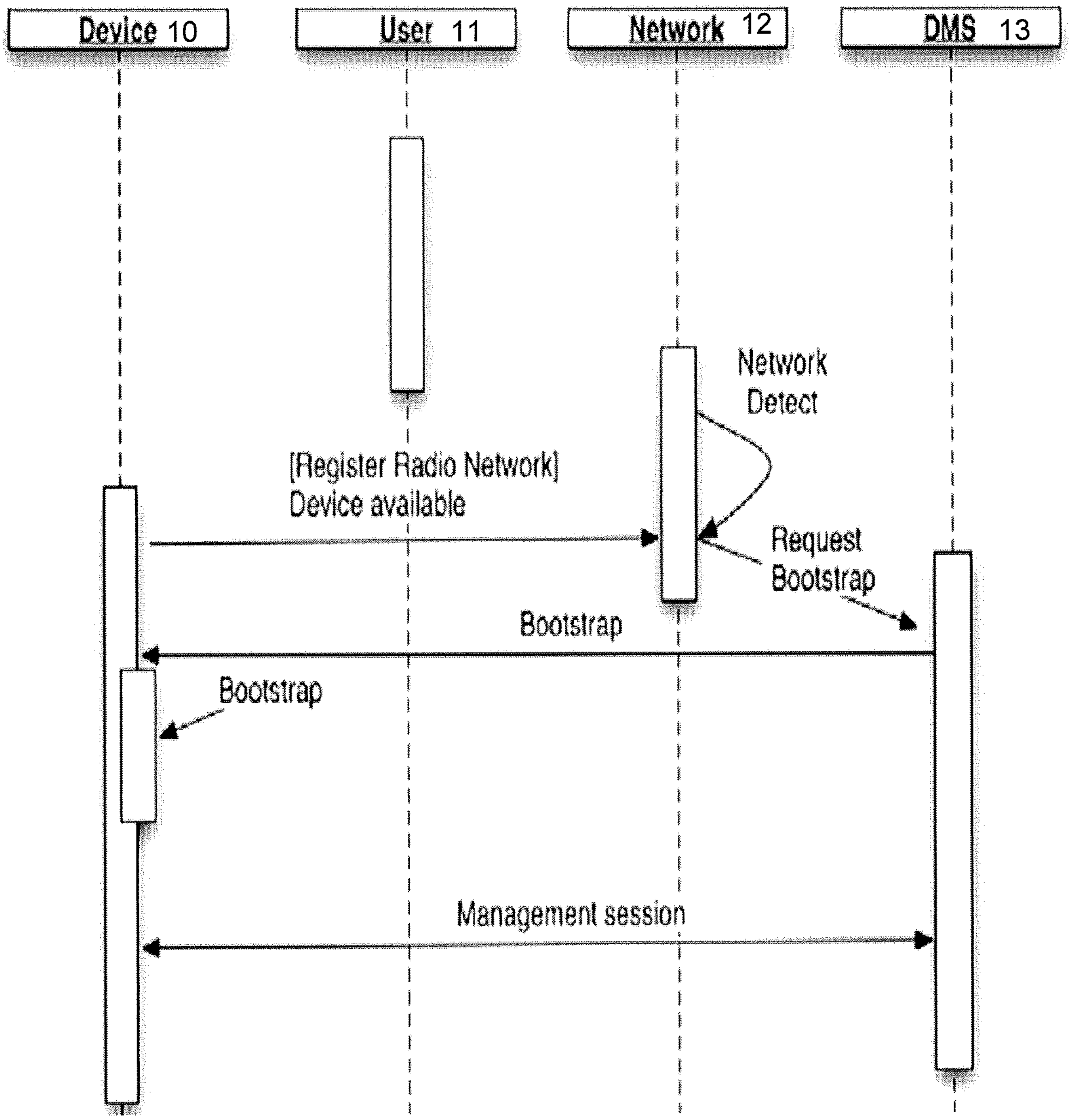
Device 10
User 11
Network 12
DMS 13
Network Detect
[Register Radio Network] Device available
Request Bootstrap
Bootstrap
Bootstrap
Management session

FIGURE 1

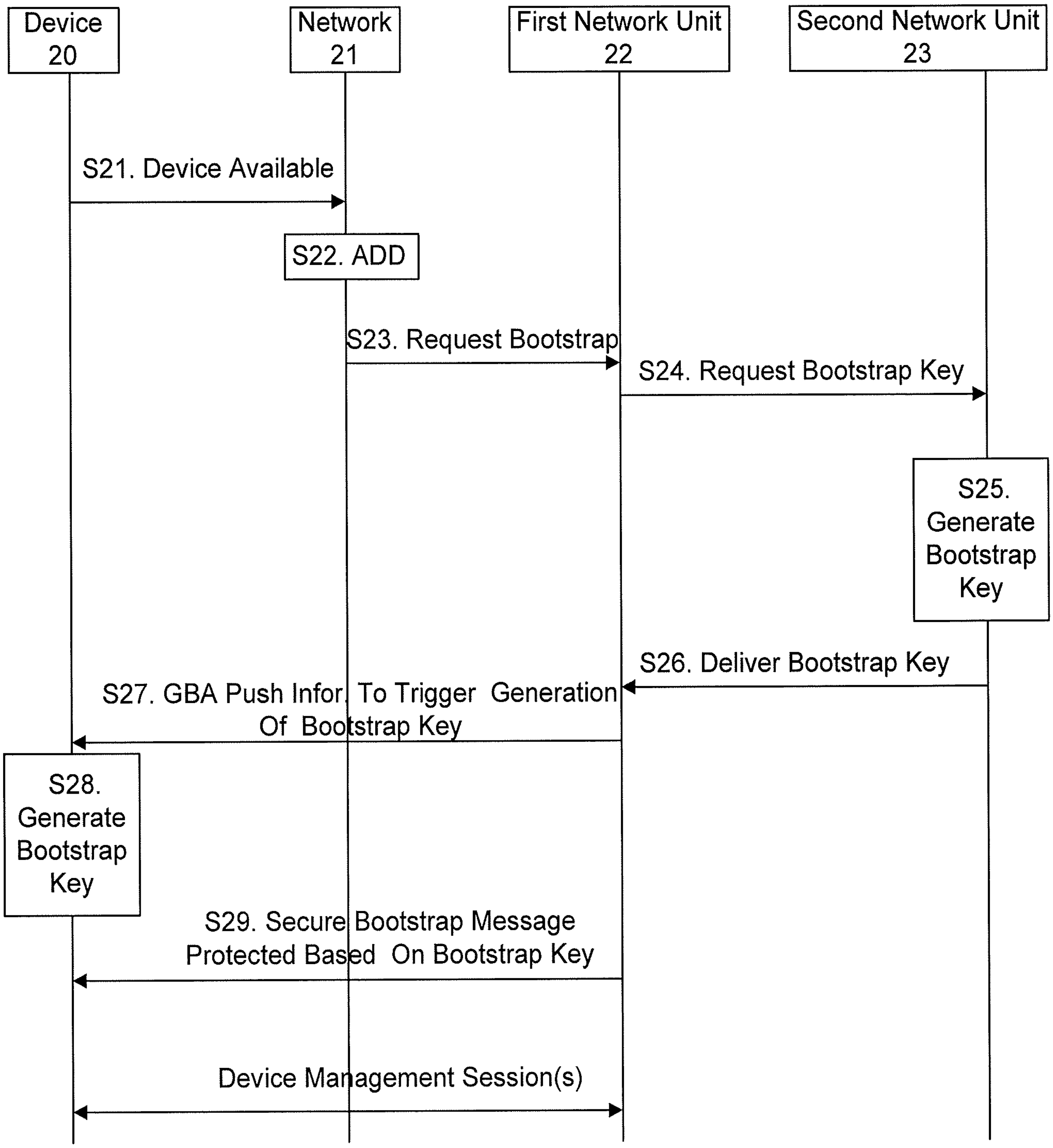
Device
20
Network
21
First Network Unit
22
Second Network Unit
23
S21. Device Available
S22. ADD
S23. Request Bootstrap
S24. Request Bootstrap Key
S25. Generate Bootstrap Key
S26. Deliver Bootstrap Key
S27. GBA Push Infor. To Trigger Generation Of Bootstrap Key
S28. Generate Bootstrap Key
S29. Secure Bootstrap Message Protected Based On Bootstrap Key
Device Management Session(s)

FIGURE 2

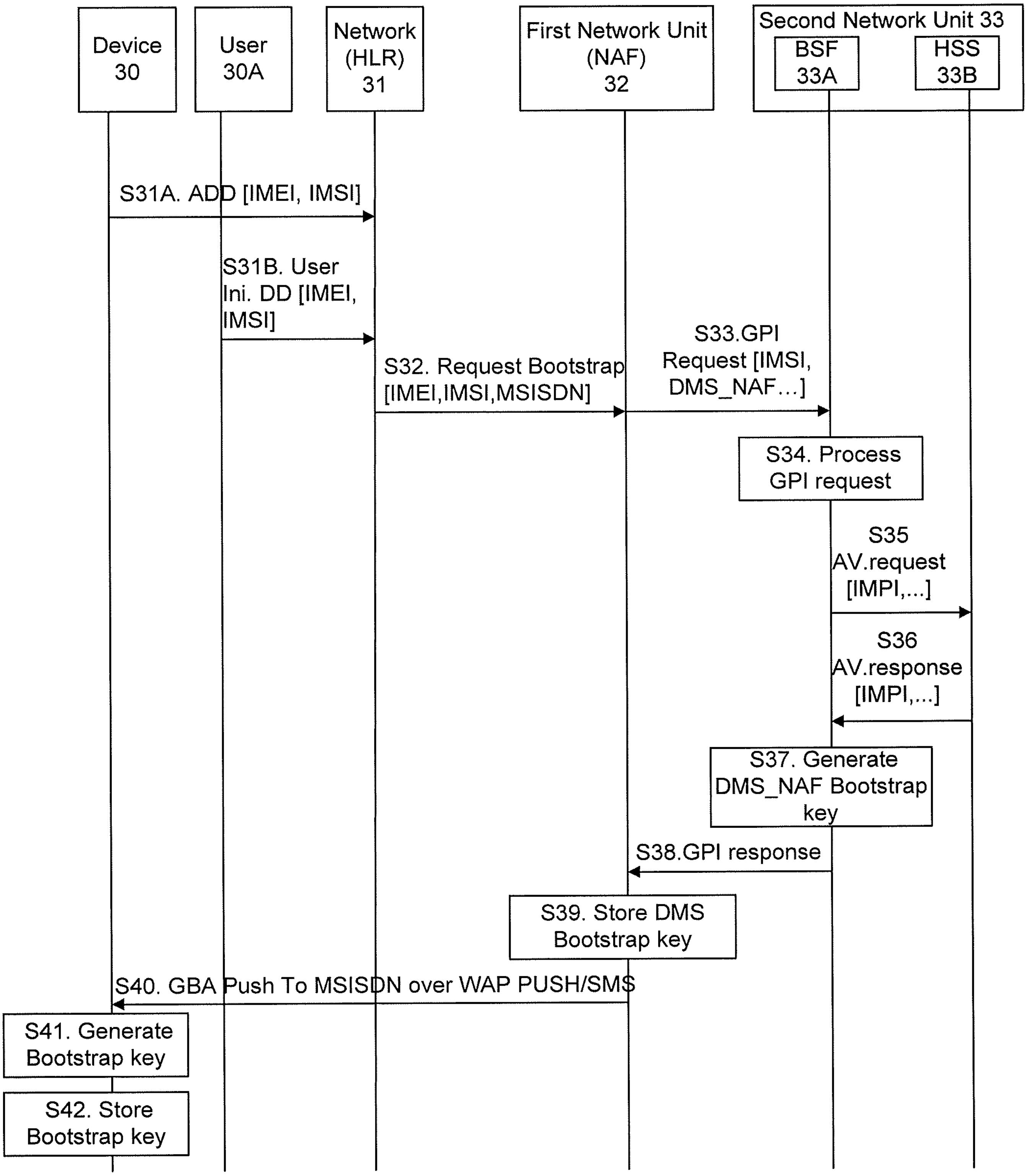
Device 30
User 30A
Network (HLR) 31
First Network Unit (NAF) 32
Second Network Unit 33
BSF 33A
HSS 33B
S31A. ADD [IMEI, IMSI]
S31B. User Ini. DD [IMEI, IMSI]
S32. Request Bootstrap [IMEI,IMSI,MSISDN]
S33.GPI Request [IMSI, DMS_NAF…]
S34. Process GPI request
S35 AV.request [IMPI,...]
S36 AV.response [IMPI,...]
S37. Generate DMS_NAF Bootstrap key
S38.GPI response
S39. Store DMS Bootstrap key
S40. GBA Push To MSISDN over WAP PUSH/SMS
S41. Generate Bootstrap key
S42. Store Bootstrap key

FIGURE 3

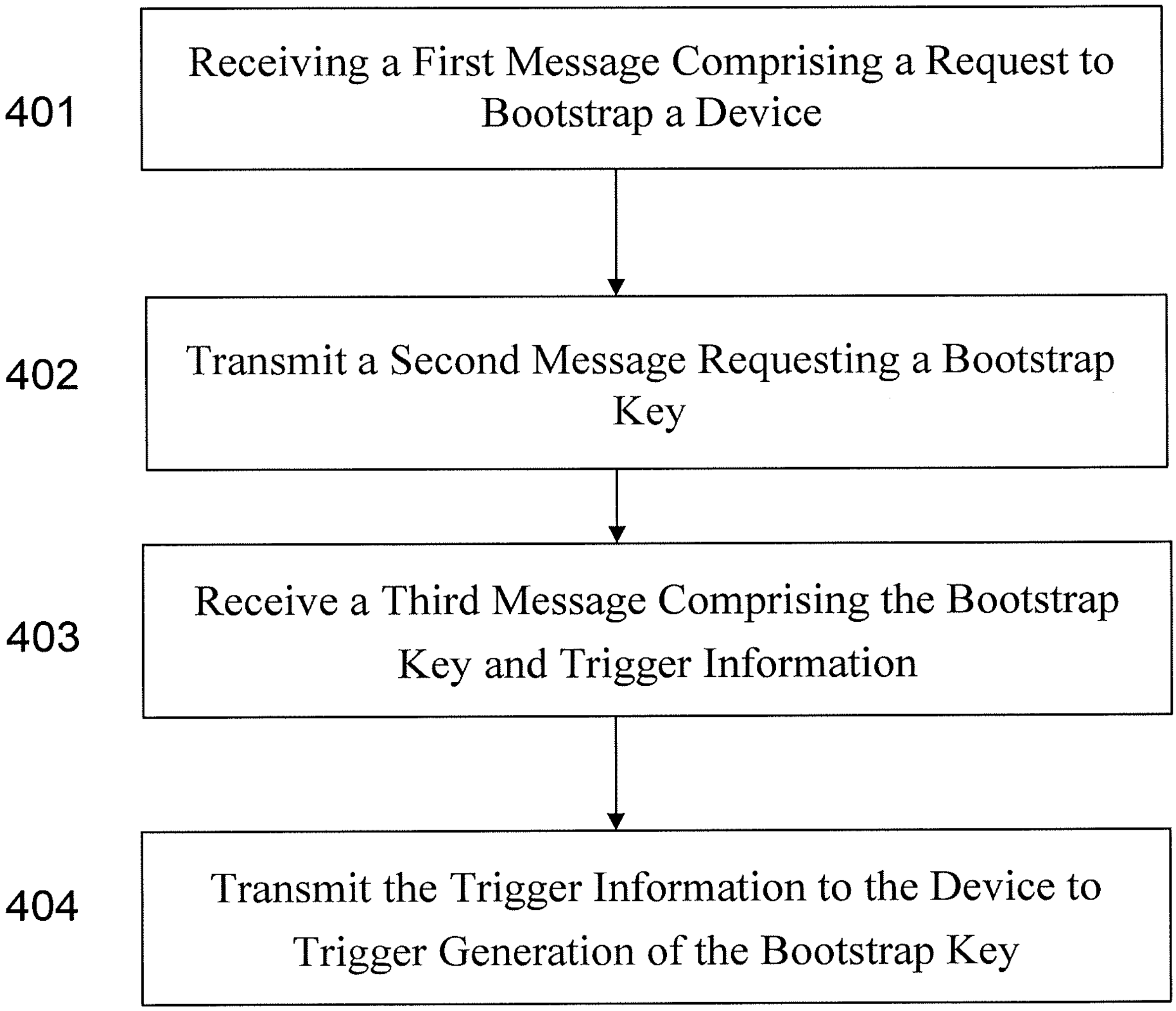
401
Receiving a First Message Comprising a Request to Bootstrap a Device
402
Transmit a Second Message Requesting a Bootstrap Key
403
Receive a Third Message Comprising the Bootstrap Key and Trigger Information
404
Transmit the Trigger Information to the Device to Trigger Generation of the Bootstrap Key

FIGURE 4

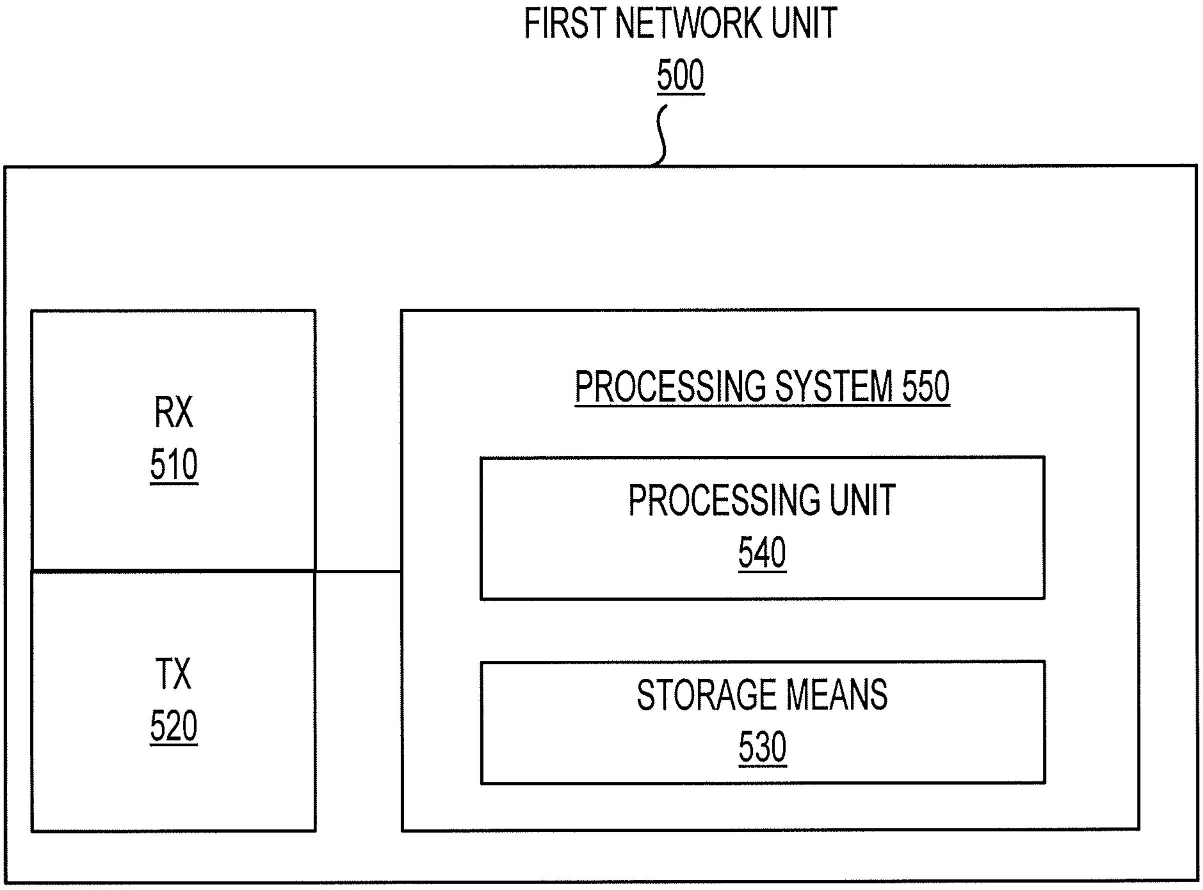
FIRST NETWORK UNIT
500
RX
510
TX
520
PROCESSING SYSTEM 550
PROCESSING UNIT
540
STORAGE MEANS
530

FIGURE 5

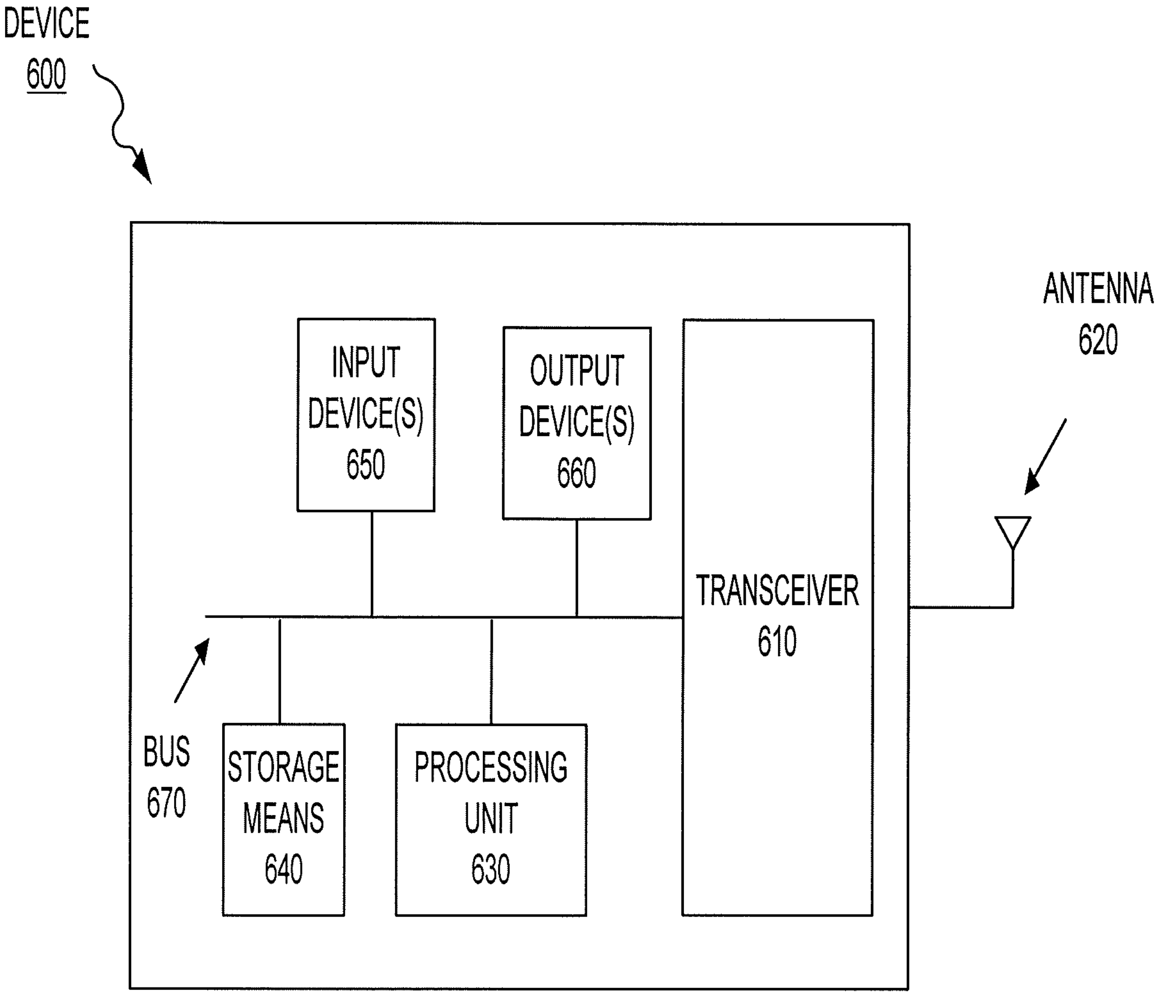
DEVICE
600
ANTENNA
620
INPUT
DEVICE(S)
650
OUTPUT
DEVICE(S)
660
TRANSCEIVER
610
BUS
670
STORAGE
MEANS
640
PROCESSING
UNIT
630

FIGURE 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2009/051092

A. CLASSIFICATION OF SUBJECT MATTER

IPC: 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, H04Q, H04W

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

SE,DK,FI,NO classes as above

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

EPO-INTERNAL, WPI DATA, PAJ, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2009004590 A2 (NOKIA CORPORATION), 8 January 2009 (08.01.2009), page 1, line 5 - line 12, figure 1, abstract --	1-12
A	WO 2007063420 A2 (NOKIA CORPORATION), 7 June 2007 (07.06.2007), abstract, paragraph (0044) --	1-12
A	US 20060196931 A1 (S. HOLTMANNS ET AL), 7 Sept 2006 (07.09.2006), abstract, paragraphs (0012), (0049) --	1-12

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

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search 12 May 2010	Date of mailing of the international search report 20-05-2010
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Predrag Pajovic / MRo Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2009/051092

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 20070234041 A1 (S. LAKSHMESHWAR ET AL), 4 October 2007 (04.10.2007), abstract, paragraph (0013) -- --------	1-12

International patent classification (IPC)

H04W 12/04 (2009.01)
H04L 9/32 (2006.01)
H04W 8/20 (2009.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded:

- From "Cited documents" found under our online services at www.prv.se (English version)
- From "Anförda dokument" found under "e-tjänster" at www.prv.se (Swedish version)

Use the application number as username. The password is **JCFXQRRWAJ.**

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/SE2009/051092

WO	2009004590	A2	08/01/2009	NONE
WO	2007063420	A2	07/06/2007	NONE
US	20060196931	A1	07/09/2006	NONE
US	20070234041	A1	04/10/2007	NONE