(19) DANMARK

Patent- og
Varemærkestyrelsen

(10) DK/EP 2547134 T3

(12) Oversættelse af europæisk patentskrift

(51) Int.Cl.: ***H 04 W 12/06 (2009.01)*** *H 04 W 12/02 (2009.01)*

(45) Oversættelsen bekendtgjort den: **2017-05-08**

(80) Dato for Den Europæiske Patentmyndigheds
bekendtgørelse om meddelelse af patentet: **2017-03-08**

(86) Europæisk ansøgning nr.: **12187913.4**

(86) Europæisk indleveringsdag: **2005-04-08**

(87) Den europæiske ansøgnings publiceringsdag: **2013-01-16**

(30) Prioritet: **2004-04-26 US 831352**

(62) Stamansøgningsnr: **11182696.2**

(84) Designerede stater: **AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU MC NL PL PT RO SE SI SK TR**

(73) Patenthaver: **Nokia Technologies Oy, Karaportti 3, 02610 Espoo, Finland**

(72) Opfinder: **Eronen, Pasi, Neitojenranta 1 B 38, 00810 Helsinki, Finland**

(74) Fuldmægtig i Danmark: **RWS Group, Europa House, Chiltern Park, Chiltern Hill, Chalfont St Peter, Bucks SL9 9FG, Storbritannien**

(54) Benævnelse: **FORBEDRET ABONNENTAUTENTIFICERING FOR UAUTORISERET MOBILT ADGANGSSIGNALERING**

(56) Fremdragne publikationer:
EP-A1- 1 207 708
EP-A1- 1 257 141
EP-A1- 1 395 068
WO-A2-02/093811
WO-A2-2004/036770
US-A1- 2004 053 602
US-A1- 2004 116 120
US-A1- 2004 248 595

DESCRIPTION

Field of the Invention

[0001] The present invention relates to communications in an unlicensed mobile access network and particularly to authentication of user access during communication between a mobile station and a mobile network.

Background of the Invention

[0002] In unlicensed mobile access architecture, a mobile station uses unlicensed radio technology, such as wireless LAN (WLAN) or Bluetooth, to communicate with an unlicensed mobile access network. In such an arrangement, the unlicensed mobile access network replaces the Global System for Mobile Communication Base Station Subsystem (GSM BSS) used in the conventional Global System for Mobile Communication (GSM) arrangement. The interface between the mobile station and the unlicensed mobile access network uses Internet Protocol, at least partly run over unlicensed radio technology, and a new unlicensed radio resource protocol.

[0003] In a typical unlicensed mobile access deployment, the mobile station communicates with a WLAN access point that is connected to a broadband Internet connection. Since untrusted networks may be used in the connection between the mobile station and the unlicensed mobile access network, sufficient security features must be provided.

[0004] Therefore, in the unlicensed mobile access architecture, the unlicensed mobile access network authenticates the subscriber before any unlicensed radio resources signaling or higher-layer messages, such as Mobility Management, can be sent from the mobile station to the unlicensed mobile access network. The unlicensed mobile access network may authenticate a subscriber on a mobile station by using preexisting authentication methods, such as passwords, certificates or SIM cards. The signaling traffic between the mobile station and the unlicensed mobile access network is encrypted and integrity protected using, for example, IPsec or Transport Layer Security protocols. Optionally, user plane traffic may also be protected using either IPsec or Secure Real-time Transport Protocol.

[0005] After the subscriber is authenticated with the unlicensed mobile access network, the subscriber is then authenticated to the Core Network in the unlicensed mobile access architecture. To ensure that the Core Network is authenticating the right subscriber, the Core Network sends a challenge (RAND) to the mobile station. The mobile station uses a subscriber identity module (SIM) card to calculate a response (SRES) and an encryption key (Kc). The mobile station sends the response to the Core Network and if the response is correct, the Core Network activates encryption by sending a "BSSMAP Cipher Mode Command" message to the unlicensed mobile access network. The Cipher Mode Command message includes a list of permitted algorithms and the encryption key. Unlike the GSM arrangement where the BSS selects a suitable algorithm form the Cipher Mode Command message and commands the mobile station to start encryption by sending the selected algorithm to the mobile station, in the unlicensed mobile access architecture, the connection between the mobile station and the unlicensed mobile access network is already encrypted and the algorithms contained in the BSSMAP Cipher Mode Command message are not suitable for IPsec or TLS encryption used between the Mobile Station and the unlicensed mobile access network. Therefore, the unlicensed mobile access network uses neither the algorithm nor the key from the BSSMAP Cipher Mode Command message. Nevertheless, the unlicensed mobile access network forwards the list of algorithms in the Cipher Mode Command to the mobile station and the mobile station stores the parameters and key for later use when performing handover to a GSM network.

[0006] The authentication procedure used in the unlicensed mobile access architecture does not ensure that the identity that is authenticated to the unlicensed mobile access network is the same identity that is authenticated to the Core Network. This permits "a man-in-the-middle" attack wherein an attacker who has a valid subscription can, for instance, make calls that get billed to other subscribers.

[0007] Figure 1 illustrates how a subscriber with a valid subscription can perform a man-in-the-middle attack. In Step 1010, the subscriber connects to the unlicensed mobile access network and the unlicensed mobile access network authenticates the subscriber and establishes a secure channel. In Step 1020, unlicensed radio resources signaling is established between the mobile station and the unlicensed mobile access network. In Step 1030, the subscriber requests service with a message that contains the International Mobile Subscribe Identity (IMSI) or the Temporary Mobile Subscriber Identity (TMSI) identifying the subscriber to the Core Network. However, in this step, the subscriber performing the man-in-the-middle attack includes an IMSI or TMSI of another unsuspecting subscriber. In Step 1040, the unlicensed mobile access network forwards the request message to the Core Network without examining the contents of the request message. In Step 1050, in response to the request message, the Core Network sends an authentication request to the mobile station. In Step 1060, when the subscriber receives the request message, instead of calculating the response to the authentication request by using the subscriber's SIM or USIM, the subscriber pretends to be a BSS in a GSM network and forwards the authentication request to the other unsuspecting subscriber. The other unsuspecting subscriber uses its SIM card to calculate a response to the authentication request and sends the response to the subscriber that is pretending to be a BSS. If UMTS protocols are used, an additional "AUTN" parameter is sent by the Core Network and verified by the other unsuspecting subscriber. However, the AUTN parameter does not prevent the man-in-the-middle attack. Upon receiving the response from the other unsuspecting subscriber, the subscriber performing the man-in-the-middle attack forwards the response with the other subscriber's SIM to the unlicensed mobile access network, in Step 1070. In Step 1080, the unlicensed mobile access network forwards the response to the Core Network without examining the contents of the response. In Step 1090, the Core Network verifies the response, which is correct because the other unsuspecting subscriber is a valid subscriber, and sends the BSSMAP Cipher Mode Command message to the unlicensed mobile access network. Since the unlicensed mobile access network does not use the algorithms or key supplied by the Core Network in the Cipher Mode Command message, the unlicensed mobile access network simply forwards the list of permitted algorithms to the subscriber. In Steps 1100, URR Ciphering Mode is completed between the mobile station and the unlicensed mobile access network. In Step 1010, BSSMAP Cipher Mode Command is completed between the unlicensed mobile access network and the Core Network.

[0008] After the Cipher Mode setting has been completed with the other subscriber's information, the subscriber is then able to perform normal Mobility Management and Call Control signaling when setting up a call. This causes the Core Network to use the other subscriber's IMSI or TMSI for billing purposes.
EP1257141 describes a technique for DSPA between uncoordinated radio access networks having different RATs. EP1395068 describes a technique for optimising overall resource usage in areas where WLAN and usual radio networks are overlapping. US2004/0053602 describes a technique involving the integration of unlicensed spectrum. WO02/093811 describes a technique for providing access to PLMN networks for non-PLMN devices. EP1207708 describes a mobile communication network including a local BSS adapted to communicate with mobile terminals over an unlicensed radio interface.

[0009] There is hereby provided a method according to claim 1 and an apparatus according to claim 2.

[0010] A first subscriber in the unlicensed mobile access system is prevented from unauthorized use of a second subscriber's identity when the first subscriber requests services from the mobile station to the core network. The network comprises authenticating means for authenticating a mobile station to the unlicensed mobile access network before higher-layer mes- sages are sent from the mobile station to a core network; the mobile station com- prises a subscriber identity module that includes an identifying means for identi- fying the mobile station and a key; the network also comprises connecting means for connecting the mobile station to the core network and relaying means for re- laying signals between the mobile station and the core network; and during authentication between the mobile station and the core network, the mobile station passes the key to a IPsec or TLS layer to the unlicensed mobile access network, thereby ensuring that all further messages sent from the mobile station are pro- tected with the key or keys derived from key.

[0011] The method comprises authenticating a mobile station to an unlicensed mobile access network before higher-layer messages are sent from the mobile station; requesting service, by the mobile station, from the core network and including a IMSI for the mobile station in the request message; forwarding, by the unlicensed mobile access network, the request message to the core network without examination of the message by the unlicensed mobile access network; sending an authentication request from the core network to the mobile station through the unlicensed mobile access network; creating an authentication response, by the mobile station, in response to the authentication request and forwarding the authentication response to the core network through the unlicensed mobile access network; verifying the authentication response, by the core network, and sending a Cipher Mode Command message to the unlicensed mobile access network; forwarding, by the unlicensed mobile access network, the Cipher Mode Command Message to the mobile station; and passing a key to a IPsec or TLS layer, by the mobile station, thereby ensuring that all further messages sent from the mobile station are protected with the key or keys derived from key.

Brief Description of the Drawings

[0012] The accompanying drawings, which are included to provide a further understanding of the invention and are incorporated in and constitute a part of this specification, illustrate embodiments of the invention that together with the description serve to explain the principles of the invention.

[0013] In the drawings:

Figure 1 illustrates how a subscriber with a valid subscription can perform a man-in-the-middle attack;

Figure 2 illustrates the components of a system 200 implementing the unlicensed mobile access architecture in which the present invention is implemented;

Figure 3 illustrates a technique for preventing man-in-the-middle attacks by a valid subscriber;

Figure 4 illustrates another technique for preventing man-in-the-middle attacks in an unlicensed mobile access arrangement;

Figure 5 illustrates an embodiment of the claimed invention for preventing man-in-the-middle attacks in an unlicensed mobile access arrangement.

Description of embodiments

[0014] Reference will now be made in detail to a preferred embodiment of the present invention, an example of which is illustrated in Figure 5 of the accompanying drawings. The present invention described below extends the functionality of the inventive method for authenticating a mobile station with both an unlicensed mobile access network and a Core Network.

[0015] The present invention relates to authentication of a mobile station in a system implementing the unlicensed mobile access architecture so as to prevent "man-in-the-middle" attacks. The unlicensed mobile access arrangement extends the Global System for Mobile Communication/ General Packet Radio Service (GSM/ GPRS) mobile services by tunneling certain GSM/GPRS protocols from a Core Network over a broadband Internet Protocol (IP) to a customer's premise, and then relaying them over an unlicensed radio link inside the customer's premises. Unlicensed mobile access is designed as a complement to traditional GSM/GPRS radio coverage and is used to enhance customer premise coverage, increase network capacity and potentially lower cost. The unlicensed mobile access network in the unlicensed mobile access arrangement is designed to coexists with the GSM/GPRS radio access network and to interconnect the GSM Core Network and the mobile station via the same interfaces used by the standard GSM Base Station Subsystem (GSM BSS). Therefore, the unlicensed mobile access network appears to the GSM/GPRS Core Network as a GSM BSS and is managed and operated as such. It should be noted that unlicensed mobile access could be used with UMTS protocols instead of GSM protocols. In this case the unlicensed mobile access network appears to be a Radio Access Network to the Core Network.

[0016] Figure 2 illustrates the components of a system 200 implementing the unlicensed mobile access architecture in which the present invention is implemented. System 200 includes three primary components: a mobile station 202, an unlicensed mobile access network 204, and a Core Network 206. As is apparent to those skilled in the art, mobile station 202 may include a telephone, a laptop, a PDA or any other device that is used by a subscriber in an unlicensed mobile access arrangement. Mobile station 202 is present on a customer premise 201 and mobile station 202 includes a mobile terminal 208 and a Subscriber Identity Module (SIM) 210. Unlicensed mobile access network 204 provides the functional equivalents of a GSM/GPRS base station controller in that unlicensed mobile access network 204 connects mobile station 202 to Core Network 206 and communicates with Mobile Station 202 via the standard GSM A-interface for circuit and switched voice services and the standard GPRS G_b-interface for packet data services. Core Network 206 implements the principle elements of transaction control and user services. A broadband IP network 205 provides connectivity between customer premise 201 and unlicensed mobile access network 204 and an access point 203 provides unlicensed radio link to mobile station 202. An IP transport network extends from unlicensed mobile access network 204 to Mobile Station 202 through access point 203 in customer premise 201, thus enabling a single interface, Ut, to be defined between unlicensed mobile access network 204 and mobile station 202.

[0017] Specifically, in mobile station 202, SIM 210 is a smart card that provides personal mobility so that a user can have access to subscribed services when SIM 210 is inserted into any terminal. Therefore, when SIM 210 is inserted into a terminal, the user is able to receive calls at that terminal, make calls from that terminal and receive other subscribed services. A International Mobile Equipment Identity (IMEI) uniquely identifies mobile station 202 and SIM 210 includes, among other information, the International Mobile Subscriber Identity (IMSI), that is used to identify the subscriber to the system, and a secret key Kc for authentication. The IMEI and IMSI are independent, thereby allowing for personal mobility. As is known to those of ordinary skill in the art, SIM 210 may be protected against unauthorized use by a password or a personal identity number.

[0018] In the unlicensed mobile access architecture, mobile station 202 provides dual mode, i.e. licensed and unlicensed, radios and the capability to switch between them. An access mode switch is provided to switch between the GSM mode and the unlicensed mobile access mode. Mobile station 202 supports an IP interface to access point 203, thereby enabling the IP network from unlicensed mobile access network 204 to extend to mobile station 202. Access point 203 preferably does not provide any unlicensed mobile access specific gateway functions. Therefore, any standard access point may be used to interconnect mobile station 202 to unlicensed mobile access network 204 via broadband IP network 205. Access point 203 provides unlicensed radio link toward mobile station 202 and it connects through broadband IP network 205 to unlicensed mobile access network 204.

[0019] As noted above, unlicensed mobile access network 204 provides the functions equivalent to that of a GSM/GPRS base station controller. It connects via an IP transport network to customer premise 201 and through access point 203 to mobile station 202. Unlicensed mobile access network 204 maintains end-to-end communications with mobile station 203 and relays GSM/GPRS signal to Core Network 206. In particular, it maps voice from customer premise 201 to PCM voice when a Mobile Switching Center in Core Network 206 is not using certain features.

[0020] Core Network 206 includes a Mobile Switching Center (MSC) 212, a Home Location Register (HLR) 214, a Visitor Location Register (VLR) 216, an Equipment Identity Register (EIR) 218 and an Authentication Center 220. MSC 212 acts like a normal switching node of the PSTN or ISDN and provides all of the functionality for handling a mobile subscriber, such as registration, authentication, location updating, handovers and call routing to a roaming subscriber. MSC 212 also provides the connection to fixed networks, such as PSTN or ISDN. HRL 214 works with MSC 212 and VLR 216 to provide the call routing and roaming capabilities of GSM. HRL 214 includes all of the administrative information of each subscriber that is registered in the corresponding GMS network and the current location of mobile station 202. VLR 216 includes selected administrative information, from HLR 214, that are necessary for call control and provision of the subscribed services for each mobile station that is currently located in the geographical area controlled by VLR 216. EIR 218 is a database that includes a list of all valid mobile equipment on the network, wherein each mobile station is identified by its IMEI. Authentication Center 220 is a protected database that stores a copy of the secret key that is stored in each subscriber's SIM 210 card, wherein the secret key is used for authentication and encryption over the radio channel.

[0021] The Ut interface between unlicensed mobile access network 204 and mobile station 202 operates over an IP transport network and relays GSM/GPRS signaling from the Public Land Mobile Network (PLMN) Core Network 206 towards mobile station 202. The Ut interface enables GSM Mobility Management protocols and protocols above that level in Core Network 206 to be carried transparently between mobile station 202 and MSC 212. This allows mobile station 202 to derive all GSM services as if it were in a GSM BSS. In the unlicensed mobile access architecture, Unlicensed Mobile Access-Radio Resource (UMA-RR) protocol replaces the conventional GSM-RR protocol since an unlicensed radio link presents different characteristics from that of a licensed radio link. A transport and multiplexing Unlicensed Mobile Access Transport Protocol (UMA-TP) is defined to carry the UMA-RR messages over a secure tunnel between mobile station 202 and unlicensed mobile access network 204. The unlicensed mobile access secure tunnel uses SSL/TCP over IP and is responsible for setting up the secure tunnel. The unlicensed mobile access secure tunnel is also responsible for managing the unlicensed radio link with the standard access point 203. In the unlicensed mobile access architecture, standard IP technology is used in mobile station 202 to access the unlicensed radio link.

[0022] Prior to receiving any unlicensed radio resources signaling or higher-layer messages from the mobile station, unlicensed mobile access network 204 authenticates a subscriber on mobile station 202 by using preexisting authentication methods, such as passwords, certificates or SIM cards. The signaling traffic between mobile station 204 and unlicensed mobile access network 206 is encrypted and integrity protected using, for example, IPsec or Transport Layer Security protocols. After the subscriber is authenticated with unlicensed mobile access network 204, the subscriber may then be authenticated to Core Network 206.

[0023] Figure 3 illustrates a technique for preventing man-in-the-middle attacks by a valid subscriber. In Step 3010, the subscriber connects to unlicensed mobile access network 204 and unlicensed mobile access network 204 authenticates the subscriber and establishes a secure channel. In Step 3020, unlicensed radio resources signaling is established between unlicensed mobile access network 204 and mobile station 202. In Step 3030, the subscriber requests service from Core Network 206 with a message that includes the International Mobile Subscribe Identity (IMSI) or the Temporary Mobile Subscriber Identity (TMSI) identifying the subscriber to Core Network 206. In Step 3040, unlicensed mobile access network 204 forwards the request message to Core Network 206 without examining the contents of the request message. In Step 3050, in response to the request message, Core Network 206 sends an authentication request to mobile station 202. In Step 3060, the subscriber creates a response message using SIM 210 in mobile station 202. In Step 3070, mobile station 202 sends the response message to unlicensed mobile access network 204 and unlicensed mobile access network 204 forwards the response message to Core Network 206 without examining the contents of the response message. In Step 3080, Core Network 206 verifies the response and sends the BSSMAP Cipher Mode Command message to unlicensed mobile access network 204. Since unlicensed mobile access network 204 does not use the algorithms or key supplied by Core Network 206 in the Cipher Mode Command message, unlicensed mobile access network 204 simply forwards the list of permitted algorithms to the subscriber. In Step 3090, after the Cipher Mode setting has completed, unlicensed mobile access network 204 examines the Mobility Management messages that are sent from mobile station 202 to Core Network 206. The Mobility Management messages include CM Service Request, CM Reestablishment Request, Identity Response, IMSI Detach Indication, Location Updating Request and Attach Request messages. In Step 3100, unlicensed mobile access network 204 maps the identity of mobile station 202 from the previous authentication steps between mobile station 202 and unlicensed mobile access network 204 with the IMSI of the mobile station sending the Mobility Management message. If the IMSI was not used during the authentication steps between mobile station 202 and unlicensed mobile access network 204, then unlicensed mobile access network 204 may fetch the subscriber profile from the HLR and obtain the IMSI from the HLR. In Step 3010, if the Mobility Management message includes a Mobile Identity field and if the mobile identify field does not include the IMSI of mobile station 202 that was previously authenticated with unlicensed mobile access network 204, unlicensed mobile access network 204 copies the IMSI for mobile station 202 from the authentication process into the mobile identify field. This ensures that one subscriber cannot use a second unsuspecting subscriber's IMSI or TMSI in higher-level messages that are sent from mobile station 202 to core network 204.

[0024] Figure 4 illustrates another technique for preventing man-in-the-middle attacks in an unlicensed mobile access arrangement. In Step 4010, the subscriber connects to unlicensed mobile access network 204 and unlicensed mobile access network 204 authenticates the subscriber and establishes a secure channel. In Step 4020, unlicensed mobile access network 204 and mobile station 202 establish unlicensed radio resources signaling. In Step 4030, the subscriber requests service from Core Network 206 with a message that includes the International Mobile Subscribe Identity (IMSI) or the Temporary Mobile Subscriber Identity (TMSI) identifying the subscriber to Core Network 206. In Step 4040, unlicensed mobile access network 202 forwards the request message to Core Network 206 without examining the contents of the request message. In Step 4050, in response to the request message, Core Network 206 sends a challenge to the mobile station. In Step 4060, mobile station 202 calculates an encryption key and creates a response message using SIM 210. In Step 4070, mobile station 202 sends the response message to unlicensed mobile access network 204. In Step 4080, unlicensed mobile access network 204 forwards the response message to Core Network 206 without examining the contents of the response message. In Step 4090, Core Network 206 verifies the response and sends the BSSMAP Cipher Mode Command message to unlicensed mobile access network 204. In Step 4100, unlicensed mobile access network 204 includes a randomly selected challenge, and possibly additional information, in the Cipher Mode Command message before forwarding the Cipher Mode Command message to the subscriber. In Step 4110, in response to the challenge from unlicensed mobile access network 204 in step 4100, mobile station 202 includes a Message Authentication Code (MAC) that is calculated using the encryption key the challenge, and possible the additional information in the message from unlicensed mobile access network 204. Since the encryption key is not sent over a radio link, the technique prevents man-in-the-middle attacks by ensuring that each subscriber has to know the encryption key that is associated with Core Network 206 challenge. In an alternative technique, the MAC may include the identity of mobile station, i.e., the IMSI associated with the mobile station, and the identity of unlicensed mobile access network 204 from the authentication, in Step 4010, between mobile station 202 and unlicensed mobile access network 204. In another alternative technique, the MAC may include messages related to secure tunnel (IPsec or TLS) established between mobile station 202 and unlicensed mobile access network 204.

[0025] Figure 5 illustrates the steps implemented in an embodiment of the claimed invention for preventing man-in-the-middle attacks in an unlicensed mobile access arrangement. In Step 5010, the subscriber connects to unlicensed mobile access network 204 and unlicensed mobile access network 204 authenticates the subscriber and establishes a secure channel. In Step 5020, unlicensed radio resources signaling is established between mobile station 202 and unlicensed mobile access network 204. In Step 5030, the subscriber requests service with a message that includes the International Mobile Subscribe Identity (IMSI) or the Temporary Mobile Subscriber Identity (TMSI) identifying the subscriber to Core Network 206. In Step 5040, unlicensed mobile access network 202 forwards the request message to Core Network 206 without examining the contents of the request message. In Step 5050, in response to the request message, Core Network 206 sends an authentication request to the mobile station. In Step 5060, the subscriber creates a response message using SIM 210 in mobile station 202 and a key Kc. In Step 5070, mobile station 202 sends the response message to unlicensed mobile access network 204. In Step 5080, unlicensed mobile access network 204 forwards the response to Core Network 206 without examining the contents of the response. In Step 5090, Core Network 206 verifies the response and sends the BSSMAP Cipher Mode Command message to unlicensed mobile access network 204. In Step 5100, unlicensed mobile access network 204 forwards the Cipher Mode Command message to the subscriber. In Step 5110, mobile station 202 passes the key Kc to the IPsec or TLS layer. By passing the key to the IPsec or TLS layer, this embodiment ensures that all further messages are protected with the key Kc or keys derived from key Kc and prevents man-in-the-middle attacks because one subscriber cannot obtain another subscribers keys by pretending to be a BSS.

[0026] The foregoing description has been directed to specific embodiments of this invention. It will be apparent, however, that other variations and modifications may be made to the described embodiments within the scope of the claims

Annex

[0027] The reference numbers of Figures 1, 3, 4 and 5 are explained as follows.

1010 = The subscriber connects to the unlicensed mobile access network and the unlicensed mobile access network authenticates the subscriber and establishes a secure channel

1020 = Unlicensed radio resources signalling is established between the mobile station and the unlicensed mobile access network

1030 = The subscriber performing the man-in-the-middle attack includes and IMSI or TMSI of another unsuspecting subscriber

1040 = The unlicensed mobile access network forwards the request message to the Core Network without examining the contents of the request message

1050 = In response to the request message, the Core Network sends an authentication request to the mobile station

1060 = The subscriber pretends to be a BSS in a GSM network and forwards the authentication request to the other unsuspecting subscriber and the other unsuspecting subscriber uses its SIM card to calculate a response to the authentication request and sends the response to the subscriber that is pretending to be a BSS

1070 = The subscriber performing the man-in-the-middle attack forwards the response with the other subscriber's SIM to the unlicensed mobile access network 1080 = The unlicensed mobile access network forwards the response to the Core Network without examining the contents of the response

1090 = The Core Network verifies the response and sends the BSSMAP Cipher Mode Command message to the unlicensed mobile access network and the unlicensed mobile access network simply forwards the list of permitted algorithms to the subscriber

1100 = URR Ciphering Mode is completed between the mobile station and the unlicensed mobile access network

1110 = BSSMAP Cipher Mode Command is completed between the unlicensed mobile access network and the Core Network

3010 = The subscriber connects to the unlicensed mobile access network and the unlicensed mobile access network authenticates the subscriber and establishes a secure channel

3020 = Unlicensed radio resources signalling is established between the mobile station and the unlicensed mobile access network

3030 = The subscriber requests services from the Core Network with a message that includes the subscribers IMSI or TMSI

3040 = The unlicensed mobile access network forwards the request message to the Core Network without examining the contents of the request message

3050 = In response to the request message, the Core network sends an authentication request to the mobile station

3060 = The subscriber creates a response message using the SIM in the mobile station

3070 = The mobile station sends a response message to the unlicensed mobile access network and the unlicensed mobile access network forwards the response to the Core Network without examining the contests of the response

3080 = the Core Network verifies the response and sends the BSSMAP Cipher Mode Command message to the unlicensed mobile access network and the unlicensed mobile access network simply forwards the list of permitted algorithms to the subscriber

3090 = After the Cipher mode Command setting has complete the unlicensed mobile access examines the Mobility messages that are sent from the mobile station to the Core Network

3100 = The unlicensed mobile access network maps the identity of the mobile station from previous authentication steps between the mobile station and unlicensed mobile access network with the IMSI of the mobile station sending the Mobility Management message

3110 = If the mobile identity field in the Mobility Management message does not include the IMSI of the mobile station, the unlicensed mobile access network stores the IMSI in the mobile identity field

4010 = The subscriber connects to the unlicensed mobile access network and the unlicensed mobile access network authenticates the subscriber and establishes a secure channel

4020 = Unlicensed radio resources signalling is established between the mobile station and the unlicensed mobile access network

4030 = The subscriber requests services from the Core Network with a message that includes the subscribers IMSI or TMSI

4040 = The unlicensed mobile access network forwards the request message to the Core Network without examining the contents of the request message

4050 = In response to the request message, the Core network sends an authentication request to the mobile station

4060 = The mobile station calculates an encryption key and creates a response message using the SIM in the mobile station

4070 = The mobile station sends the response message to the unlicensed mobile access network

4080 = The unlicensed mobile access network forwards the response to the Core Network without examining the contents of the response

4090 = The Core Network verifies the response and sends the BSSMAP Cipher mode Command message to the unlicensed mobile access network

4100 = The unlicensed mobile access network includes a randomly selected challenge in the Cipher mode Command message before forwarding it to the mobile station

4110 = The mobile station includes a MAC that is calculated with the key and challenge in a response to the challenge

5010 = The subscriber connects to the unlicensed mobile access network and the unlicensed mobile access network authenticates the subscriber and establishes a secure channel

5020 = Unlicensed radio resources signalling is established between the mobile station and the unlicensed mobile access network

5030 = The subscriber requests services from the Core Network with a message that includes the subscribers IMSI or TMSI

5040 = The unlicensed mobile access network forwards the request message to the Core Network without examining the contents of the request message

5050 = In response to the request message, the Core network sends an authentication request to the mobile station

5060 = The mobile station calculate an encryption key and creates a response message using the SIM and the key

5070 = The mobile station sends a response message to the unlicensed mobile access network

5080 = The unlicensed mobile access network forwards the response to the Core Network without examining the contents of the response

5090 = The Core Network verifies the response and sends the MSSMAP Cipher Mode Command message to the unlicensed mobile access network

5100 = The unlicensed mobile access network forwards the Cipher Mode Command message to the mobile station

5110 = the mobile station passes the key to the Ipsec or TLS layer

REFERENCES CITED IN THE DESCRIPTION

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

Patent documents cited in the description

- EP1257141A **[0008]**
- EP1395068A **[0008]**
- US20040053602A **[0008]**
- WO02093811A **[0008]**

- EP1207708A [0003]

Patentkrav

1. Indretning (210, 208) til en mobil station (202), der omfatter:
middel (208) til, efter autentificering af den mobile station med et uautoriseret mobilt adgangsnet ("unlicensed mobile access network" ("UMA-net")) før kommunikation af beskeder fra højere lag fra den mobile station til et kernenet (206), at sende en forespørgselsbesked gennem det uautoriserede mobile adgangsnet, der forespørger om en tjeneste fra kernenettet, og indbefatter en mobil abonnentidentifikator;
middel til at anvende en nøgle for at skabe et autentificeringssvar som reaktion på en autentificeringsforespørgsel fra kernenettet; og
middel til at sende autentificeringssvaret til kernenettet gennem det uautoriserede mobile adgangsnet;
og kendetegnet ved middel til at videresende nøglen til et lag, ved hvilket beskyttelse af trafik mellem den mobile station og det uautoriserede mobile adgangsnet udføres, til beskyttelse af yderligere beskeder, der er sendt fra den mobile station med nøglen eller nøgler, som er afledt fra nøglen.

2. Fremgangsmåde, der er udført med en mobil station (202), der omfatter:
efter autentificering af den mobile station med et uautoriseret mobilt adgangsnet før kommunikation af beskeder fra højere lag fra den mobile station til et kernenet (206), gennem det uautoriserede mobile adgangsnet at sende
en forespørgselsbesked, der forespørger om en tjeneste fra et kernenet og indbefatter en mobil abonnentidentifikator;
at anvende en nøgle for at skabe et autentificeringssvar som reaktion på en autentificeringsforespørgsel fra kernenettet; og
at sende autentificeringssvaret til kernenettet gennem det uautoriserede mobile adgangsnet;
og kendetegnet ved at videresende nøglen til et lag, ved hvilket beskyttelse af trafik mellem den mobile station og det

uautoriserede mobile adgangsnet udføres, til beskyttelse af yderligere beskeder, der er sendt fra den mobile station med nøglen eller nøgler, som er afledt fra nøglen.

DRAWINGS

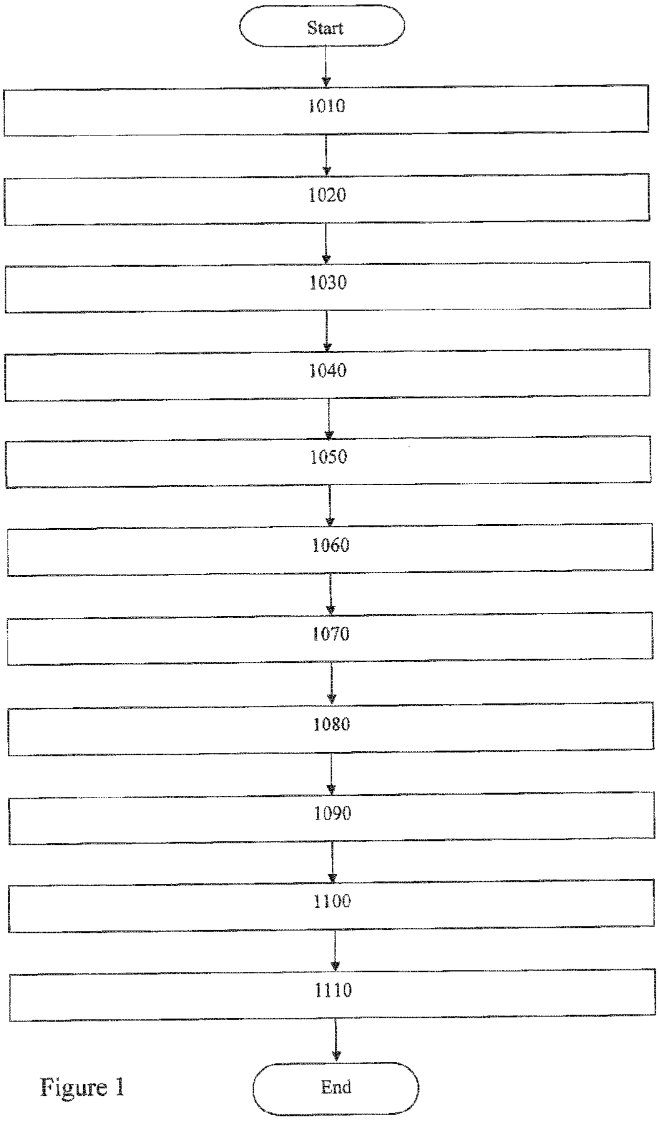

Figure 1

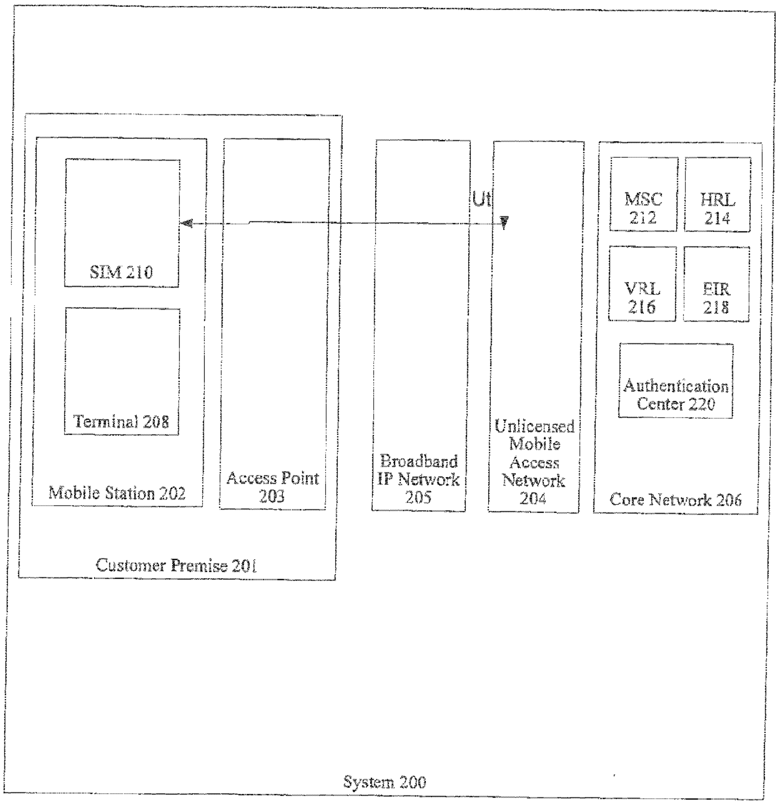
Ut
SIM 210
Terminal 208
Mobile Station 202
Access Point 203
Customer Premise 201
Broadband IP Network 205
Unlicensed Mobile Access Network 204
MSC 212
HRL 214
VRL 216
EIR 218
Authentication Center 220
Core Network 206
System 200

Figure 2

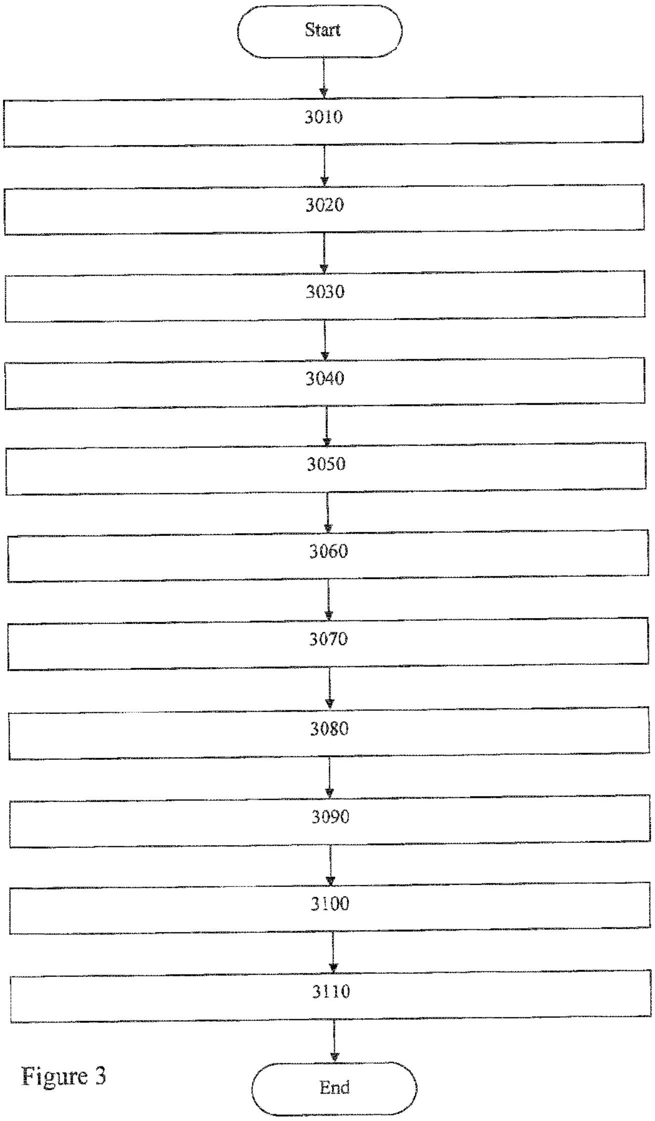
Start
3010
3020
3030
3040
3050
3060
3070
3080
3090
3100
3110
End

Figure 3

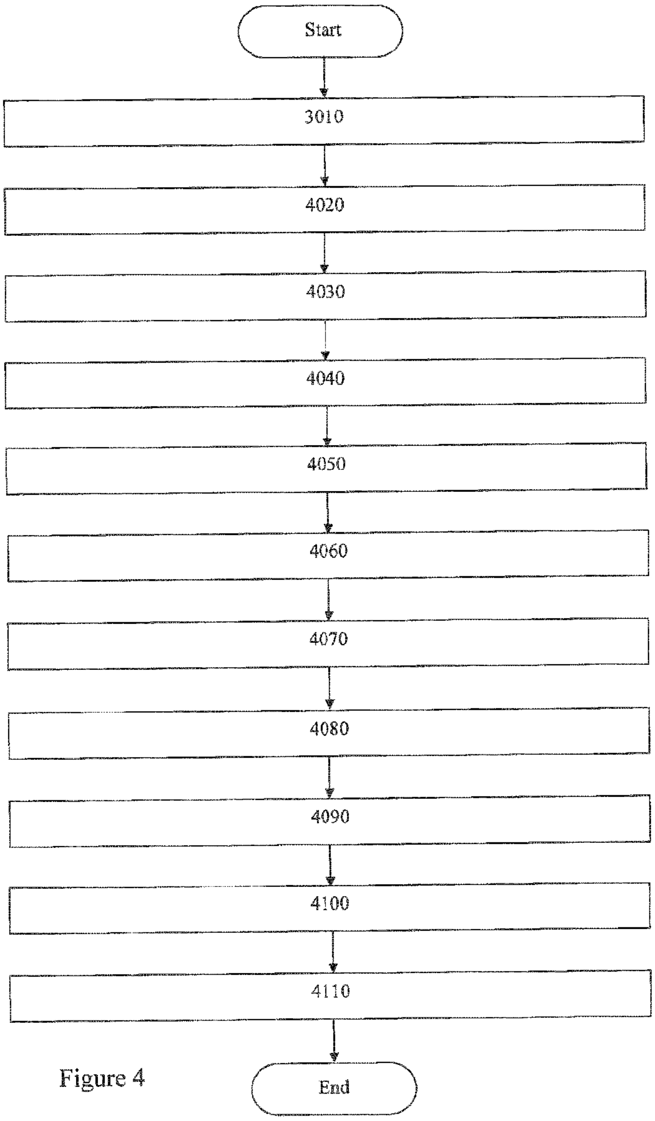
Start
3010
4020
4030
4040
4050
4060
4070
4080
4090
4100
4110
End

Figure 4

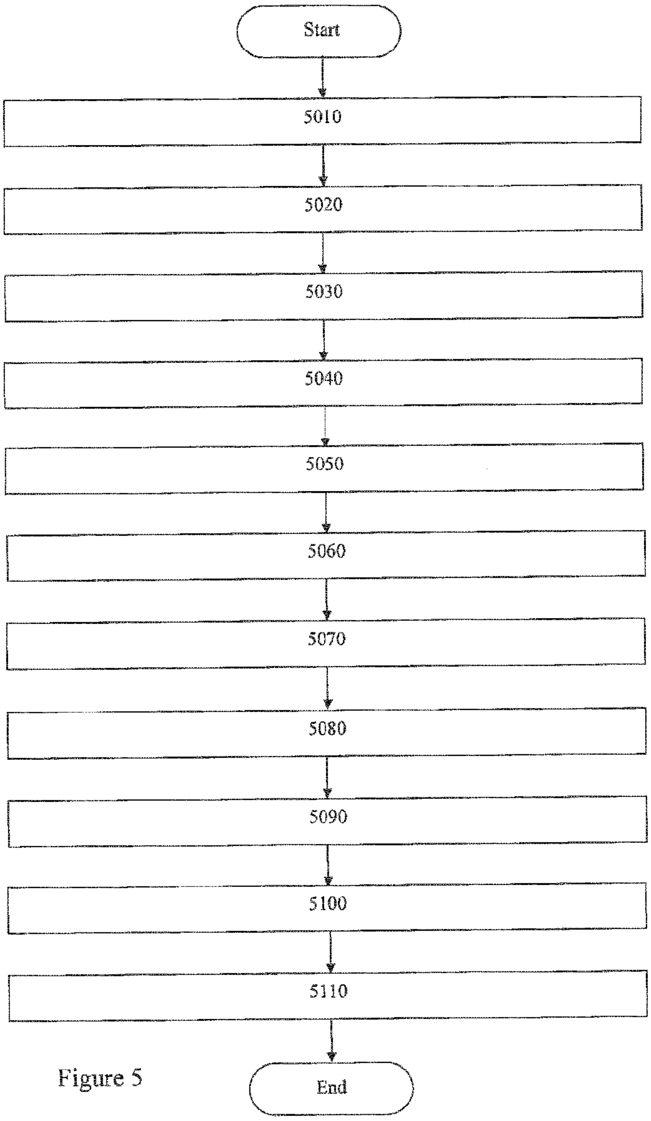
Start
5010
5020
5030
5040
5050
5060
5070
5080
5090
5100
5110
End

Figure 5