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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 August 2010 (05.08.2010)

PCT

(10) International Publication Number
WO 2010/086029 A1

(51) International Patent Classification:
H04W 12/02 (2009.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/EP2009/051161

(22) International Filing Date:
2 February 2009 (02.02.2009)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **NOKIA SIEMENS NETWORKS OY** [FI/FI]; Karaportti 3, FI-02610 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ROPOLYI, Robert** [HU/HU]; Kisfaludy u. 155, H-1196 Budapest (HU). **WOLFNER, Gyorgy Tamas** [HU/HU]; 13 Gvadanyi utca, H-1144 Budapest (HU).

(74) Common Representative: **NOKIA SIEMENS NETWORKS OY**; COO RTP IPR, Patent Administration, 80240 Munich (DE).

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

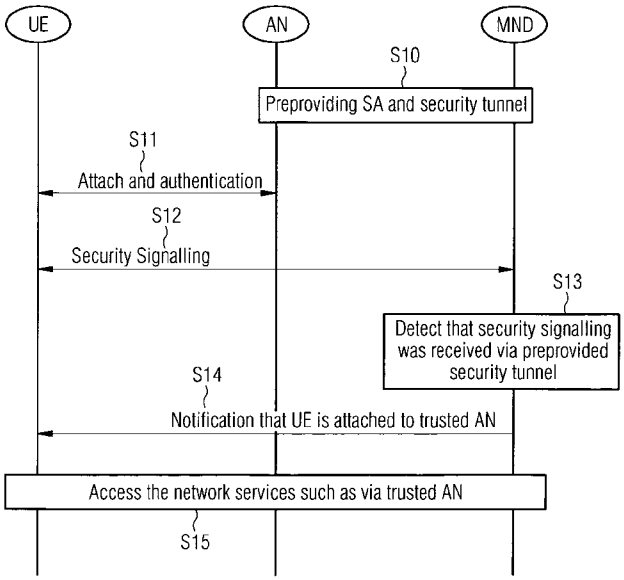
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS,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

Published:

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

(54) **Title**: METHOD AND RADIO COMMUNICATION SYSTEM FOR ESTABLISHING AN ACCESS TO A MOBILE NETWORK DOMAIN

FIG 1



(57) **Abstract**: The present inventions refers to a method for establishing an access of an user equipment to a mobile network domain via an initially unrecognized trusted access network, the method comprising: Preproviding a security association and a security tunnel between the mobile network and the access network; Conducting an attach procedure by the user equipment which indicates an access request to the access network; Setting-up a secure channel between the user equipment and the mobile network domain to execute a security signalling using the security tunnel; Detecting by the mobile network that security signals of the security signalling were received via the preprovisioned security tunnel; Notifying the user equipment by the mobile network domain that the user equipment is effectively attached to a trusted access network. The present inventions further refers to a radio communication system, comprising: at least one user equipment; a mobile network domain; an unrecognized trusted access network, wherein the user equipment, the mobile network and the access network are arranged such to supporting a method according to the present invention.

WO 2010/086029 A1

Method and radio communication system for establishing an access to a mobile network domain

FIELD OF THE INVENTION

The present invention refers to a method for establishing an access of an user equipment to a mobile network domain via an initially unrecognized trusted access network and a corresponding radio communication system.

BACKGROUND OF THE INVENTION

The current development toward truly mobile computing and networking has brought on the evolution of various access technologies, which also provide the users with access to the internet when they are outside their own home network. So far, the use of the internet has been dominated by person-to-machine communications, i.e. information services. The evolution towards so-called third generation (3G) wireless networks brings along mobile multimedia communications, which will also change the way IP-based services are utilized in public mobile networks. The IP Multimedia Subsystem (IMS), as specified by the 3rd Generation Partnership Project (3GPP), integrates mobile voice communications with internet technologies allowing IP-based multimedia services to be utilized in mobile networks.

Radio communication systems, such as cellular systems (e.g. spectrum systems (such as Code Division Multiple Access (CDMA) networks, or Time Division Multiple Access (TDMA) networks), provide users with a convenience of mobility along with a rich set of services and features. This convenience has lead to significant adoption by an ever-growing number of consumers as an accepted mode of communication for business and personal uses. To promote greater adoption, the telecommunication industry, from manufactures to service providers, has agreed to spend great efforts on developing standards for communication protocols that underlie the

various services and features. One key area of effort involves authentication to provide a secure communication. The authentication of a communication to be performed plays an important role in any communication system to ensure that communication is established between proper users or applications.

In order to provide an increasing set of internet protocol IP and multimedia services for their users, and to cover areas where their radio access technology and their own radio network does not allow it, telecommunication network operators may provide access to their networks, using alternative access types. Such access networks may be operated by different providers and also, may have been created based on a different set of industry standards than the network operated by the telecommunication operator. Depending on the used technologies and the business relationship between the access network operator and telecommunication operator, the desired security level of services (e.g. privacy in VoIP connections) may require that the network operator enforces usage of a secure IP connection between the mobile node and their own network.

In some environment, the result of the above mentioned evaluation is expressed as the alternative access network being a "trusted" or an "untrusted" access network, where the latter refers to the need of using the above mentioned IP security mechanisms.

The careful evaluation of the criteria, when the usage of such secure connections is needed - i.e. whether the alternative access network is "trusted" or "untrusted - is of high importance, as the applied security algorithms have their cost in the usage of computation resources both in the telecom network and the mobile equipment, and hence, have e.g. an effect to the battery consumption of the latter. Therefore, such decision may be applicable per each user or user services and the flexibility of the decision making is

an important factor in optimising the service provisioning via the alternative access networks.

It should be noted that in some cases, it may also be appropriate to use different interface points at the telecommunication network, where the traffic from the alternative access networks is received, depending on the alternative access being "trusted" or "untrusted". This means that the "trusted/untrusted" decision - if made dynamically, i.e. as part of the handling the service request - may influence the way the mobile terminal (i.e. the user equipment) shall connect to the network. If the user knows that the access network is untrusted, it connects to an interface point used for untrusted access, while if the user equipment knows that the access network is trusted, it connects to the interface point that is used for trusted access networks. The generic discovery methods like the so-called Domain Name System (DNS) may be utilized to enable the user equipment to find the correct interface points of the telecom network.

It should be noted that the above described methods require also user equipments to be prepared to adapt its service invocation procedures, according to the trusted/untrusted information received from the telecom network, during the service invocation itself.

3GPP, as a leading standardisation organization has specified a set of the above mentioned service security levels, IP security methods, evaluation criteria for an alternative access network being trusted/untrusted, to inform the user Equipment about the above identicated "trusted/untrusted" decision and several variants of the applicable service invocation procedures, depending on that decision.

Hereinafter, the invention and its underlying problem is described using the access of an user equipment such as a mobile phone to the 3GPP Evolved Packed Core (EPC) network

over non-3GPP access networks. However, it should be understood, that the present invention and the underlying problem is not restricted to this 3GPP application, but can be used for other applications.

First of all, some relevant 3GPP standards are mentioned and shortly described:

An user equipment (UE) may be connected to a 3GPP access network or a non-3GPP access network. Non-3GPP access networks are those that follow the standards laid down by another standardization organization than 3GPP, such as WiMAX networks specified by the WiMAX Forum or such as HRPD networks specified by 3GPP. Those non-3GPP access networks may be in the first instance as well untrusted and trusted access networks.

The technical specifications 3GPP TS 23.402 and TS 24.302 describes the architecture and procedures for providing IP-connectivity services for a user equipment when accessing the evolved 3GPP Packed Switched domain via non-3GPP access networks. In these standards, distinction is made between "unknown" and "known" non-3GPP access networks, where the term "known" refers to an access network, about which the mobile terminal has pre-configured information (e.g. provided by the home PLMN operator of the user). Due to today's environment, where the user equipment is provided with the possibility to invoke their subscribed services via another mobile operator's network - which is commonly referred to as roaming - it may not be feasible to provide pre-configured information in the mobile terminal for all the non-3GPP access network, via which the user may invoke the services. Therefore, the user equipment needs to be prepared to handle also the "unknown" non-3GPP access networks either trusted or untrusted, based on the respective decision received from the network.

The security requirements and the allowed authentication methods when accessing trusted and untrusted non-3GPP access networks are defined in the technical specification 3GPP TS 33.402.

The technical specification 3GPP TS 24.303 describes the mobility management based on DSMIP V6.

The technical specification 3GPP TS 29.273 describes the so-called evolved packet system AAA-interfaces.

According to chapter 6.2.4 of 3GPP TS 24.302 an user equipment assumes that any unknown non-3GPP access network is untrusted unless this user equipment receives a trust indication during its access authentication. If the user equipment is attached to an untrusted non-3GPP access network, the user equipment will - under this circumstance - attempt to discover a ePDG (evolved Packed Data Gateway). This user equipment will further try to establish an IPSec tunnel to this ePDG. The ePDG is part of the evolved packet core EPC as defined in 3GPP TS 23.402. The functionality of the ePDG is defined in chapter 4.3.4 of this technical specification.

According to the technical specification 3GPP TS 33.402, chapter 6.1 it is possible to skip the EAP-AKA authentication as defined in chapter 6.2 of this specification for a trusted non-3GPP access network, if this non-3GPP access network meets a set of security requirements. Those security requirements are defined in chapter 9.2.2.1 of this specification.

If the user equipment is attached to such an unrecognized trusted non-3GPP access network (i.e. non-3GPP access network which is actually trusted, what, however, is not recognizable by the user equipment), there is currently no means to notify the user equipment that the non-3GPP access network it is attached to is in fact a trusted non-3GPP access network.

Therefore, after a successful authentication (e.g. using another method than defined by 3GPP) the user equipment shall discover an ePDG. Further, the user equipment has to establish an IPSec tunnel to this ePDG. After the authentication via the ePDG, the user equipment shall start using the EPS service in that way, as if the non-3GPP access network would be an untrusted non-3GPP access network. However, this means, that the ePDG and the IPSec tunnel shall be present between the user equipment and the public data network gateway (PDN GW) even though, they would not be required for security reasons.

As a consequence of this an user equipment using e.g. the DSMIPv6 mobility over an unrecognized trusted non-3GPP access network uses unnecessarily an IPSec tunnel across this trusted non-3GPP network to the ePDG. This unnecessarily consumes computing resources. The user equipment will only stop doing this, if it is informed by the AAA-(Authentication, Authorization, Accounting) server that the access network is a trusted non-3GPP access network. The present invention faces the underlying problem is how the AAA-server is able to know whether the non-3GPP access network is a trusted or an untrusted non-3GPP network. This is particularly difficult in roaming scenarios, where the access network is attached to a visited mobile network.

So far, there is no suitable method defined to avoid the invocation of additional computing resources when the user equipment is attached to an unrecognized trusted access network, which especially uses non-3GPP authentication.

SUMMARY OF THE INVENTION

In accordance with the present invention, a method having the features of claim 1 and a radio communication system having the features of claim 21 are provided.

Accordingly, it is provided:

A method for establishing an access of an user equipment to a mobile network domain via an initially unrecognized trusted access network, the method comprising: Preproviding a security association and a security tunnel between the mobile network and the access network; Conducting an attach procedure by the user equipment which indicates an access request to the access network; Setting-up a secure channel between the user equipment and the mobile network domain to execute a security signalling using the security tunnel; Detecting by the mobile network that security signals of the security signalling were received via the pre-provisioned security tunnel; Notifying the user equipment by the mobile network domain that the user equipment is effectively attached to a trusted access network.

A radio communication system, comprising: at least one user equipment; a mobile network domain; an unrecognized trusted access network, wherein the user equipment, the mobile network and the access network are arranged such to supporting a method according to the present invention.

The present invention is based on the finding, that in the above mentioned scenario, it may help if an element (such as a node) in the visited network is able to gain more information about the unrecognized trusted access network and make this information available, e.g. to the server of the home network (e.g. the AAA-server) and thus to the user equipment which tries to access this unknown trusted network.

The present patent application proposes the use of a pre-provisioned security association (SA) and a corresponding IPSEC tunnel between a security gateway (such as an ePDG) and those initially unrecognized trusted access networks. Those initially unrecognized trusted access networks may be trusted non-3GPP access networks that use other authentication methods than for example defined by 3GPP for IPS. When the user equipment secures the security association setup (for

example using IKE or IKE V2 authentication) to the ePDG the unrecognized trusted access network will forward all the IP packets using the pre-provisioned tunnel. When the security gateway recognizes this the security gateway has to signal to the AAA server that - despite of using EAP-AKA authentication over the SWm interface - the user equipment is actually attached to a trusted access network such as a trusted non-3GPP access network. Being informed of this, the AAA server will then notify the user equipment about being attached to the trusted access network using the already defined authentication means such as EAP-AKA. In this case, the user equipment is then able to release the security association that was set up to the security gateway. This security gateway then initiates the security setup for security signalling to the PDN gateway of which identity is received during authentication with the security gateway.

Another idea of the present invention therefore is, to provide an communication system and a method where the node in the visited network is the ePDG and the information from which the ePDG can tell whether the unrecognized trusted access network is trusted, is the existence of an IPSec tunnel between this ePDG and the unrecognized trusted access network.

Advantages, embodiments and further developments of the present invention can be found in the further subclaims and in the following description, referring to the drawings.

According to one embodiment of the present invention after the step of notifying, the user equipment carries out such network service invocation in the mobile network domain via the access network as this network service invocation can be done from a initially recognized trusted access network.

According to one embodiment of the present invention the mobile network domain provides different interface points for trusted access networks and untrusted access networks.

According to one embodiment of the present invention the interface point used for untrusted access networks is a security gateway, especially an ePDG, and/or wherein the interface point used for a trusted access networks is a data gateway, especially a PDN Gateway.

According to one embodiment of the present invention a user equipment which is connected to an unrecognized trusted access network is firstly connected to the corresponding interface point for untrusted access networks, and after the user equipment having been informed about the access network being a trusted access network, the user equipment then invokes the services of the mobile network domain via the interface point provided for trusted access networks.

According to one embodiment of the present invention the security signalling comprises an authentication procedure and the user equipment is notified about the access network being trusted as part of this authentication procedure.

According to one embodiment of the present invention the mobile network domain comprises two public land mobile networks, especially one visited public land mobile network where the access network is connected to and one home public land mobile network that provides data services for the user equipment based on a subscription.

According to one embodiment of the present invention the visited public land mobile network and the home public land mobile network are the same networks.

According to one embodiment of the present invention the visited public land mobile network and the home public land mobile network are separate networks.

According to one embodiment of the present invention the visited public land mobile network comprises a security gateway, especially an ePDG, and/or wherein the home public land mobile network comprises a mobile network authenticator, especially an AAA-server.

According to one embodiment of the present invention the step of detecting by the mobile network comprises the substep of sending authentication information and information that the access network is a trusted access network from the security gateway to the mobile network authenticator.

According to one embodiment of the present invention based on the received information from the security gateway the mobile network authenticator decides whether the access network is subsequently to be handled as a trusted access network or an untrusted access network.

According to one embodiment of the present invention the attach procedure comprises the further step of executing a discovery by the user equipment prior to the step of setting-up a secure channel in order to discover a security gateway within the mobile network domain.

According to one embodiment of the present invention the security association includes cryptographic keys, initialization vectors and/or digital certificates.

According to one embodiment of the present invention the security tunnel between the access network and the mobile network domain is an IPSec-tunnel.

According to one embodiment of the present invention the access network comprises a non-3GPP access network and/or wherein the mobile network domain comprises at least one 3GPP mobile network.

According to one embodiment of the present invention for the security signaling between the user equipment and the mobile network domain a key agreement protocol, in particular IKEv2 is used.

According to one embodiment of the present invention the authentication procedure used by the mobile network domain is EAP-AKA.

According to one embodiment of the present invention the authentication procedure comprises an authentication step and a subsequently or parallel conducted authorisation step.

According to one embodiment of the present invention the user equipment is a mobile communication device, especially a cell phone or a mobile stations or a PDA.

According to one embodiment of the present invention the system architecture of the radio communication system is the System Architecture Evolution (SAE).

According to one embodiment of the present invention the main component of the system architecture of the radio communication system is the Evolved Packet Core (EPC).

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and advantages thereof, reference is now made to the following description taken in conjunction with the accompanying drawings. The invention is explained in more detail below using exemplary embodiments which are specified in the schematic figures of the drawings, in which:

Figure 1 shows a flow diagram illustrating a method of a first, generalized embodiment of the present invention;

Figure 2 shows a flow diagram illustrating a method of a second, more specific embodiment of the present invention;

Figure 3 shows a flow diagram illustrating a method of a third, even more specific embodiment of the present invention;

Figure 4 shows a block diagram of a basic radio communication system as it is used for 3GPP;

Figure 5 shows a block diagram of a radio communication system for establishing a communication between an user equipment and a public network via an unrecognized trusted non-3GPP access network according to an embodiment of the present invention;

Figure 6 shows a flow diagram illustrating a method of a fourth, detailed embodiment of the present invention;

Figure 7 shows a flow diagram illustrating a method of a fifth, more detailed embodiment of the present invention.

In all figures of the drawings elements, features and signals which are the same or at least have the same functionality have been provided with the same reference symbols, descriptions and abbreviations unless explicitly stated otherwise.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE PRESENT INVENTION

Fig. 1 shows a flow diagram illustrating a method of a first, generalized embodiment of the present invention.

Fig. 1 shows an user equipment UE, an initially unrecognized access network AN and a mobile network domain MND.

The user equipment UE may be any kind of mobile communication devices (e.g. a cell phone, a mobile stations, etc.). The user equipment UE can also be such devices as personal digital assistants (PDA) with transceiver capability or personal computers with transceiver capability.

Initially unrecognized trusted access network AN means that this access network is actually accepted by the operator of the mobile network domain (MND) as a trusted access network, however, the user equipment (UE) does not know that this access network AN is a trusted network AN. Especially, since the access network AN is initially unrecognized, the user equipment UE initially assumes that this access network AN is an untrusted network AN. Initially means in this context after an initial attach of the user equipment to this access network (AN).

The mobile network domain MND may be any kind of mobile networks or an assembly of them. A mobile network domain MND may comprise a public land mobile network (PLMN). A PLMN is a network that is established and operated by an administration or by a recognized operating agency (ROA) for the specific purpose of providing land mobile telecommunications services to the public. Access to PLMN services is achieved by means of an air interface involving radio communications between wireless enabled user equipments and land based radio transmitters or radio base stations. In a converged fixed-mobile network architecture, or via the non-3GPP access networks, PLMNs may be accessed via wired access as well,

like twisted pair, coaxial cable or Ethernet access networks. PLMNs are often interconnected with other PLMNs and/or and public switched telephone networks (PSTN) for telephone communications or with internet service providers for data and internet access.

In initial step S10 a security association (SA) and a security tunnel are established between the specific interface point(s) of the trusted access network AN and the mobile network domain MND. This step S10 which is typically part of a so-called network providing procedure is typically done only once by the operator of the access network AN and the corresponding operator of the mobile network domain MND. It should be noted that such provisioning is considered appropriate and useful for those access networks (AN), which are expected to become an unrecognized trusted network, e.g. due to the reason that they do not support those specific authentication mechanisms that the mobile network domain (MND) could use to inform the user equipment. The security association shall be configured in a way that it recognizes and transports all security signalling that a user equipment (UE) shall send when setting up secure connection to the mobile network domain (MND). The configuration shall ensure that other data packets do not use this secure tunnel.

The security association SA denotes to the establishment of shared security information between two network entities (here: the access network AN and the security gateway SecGW) to support secure communication between them. The security association SA may include cryptographic keys, initialization vectors, digital certificates and the like.

In an embodiment the security tunnel may be an Internet Protocol Security-tunnel. Internet Protocol Security (IPSec) is a suite of protocols (or protocol stack) for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPSec may also

include protocols for establishing mutual authentication between two network entities at the beginning of the session and negotiation of cryptographic keys to be used during the session. Therefore, IPSec is often used to protect data flows between a pair of network entities. In tunnel mode of a communication between a pair of network entities, the entire IP packet (i.e. data, IP header, etc.) is encrypted and/or authenticated. It is then encapsulated into a new IP packet with a new IP header. The traffic selectors of an IPSec security association define the characteristics of the data packets that shall be transported via the security tunnel (while the rest of the traffic may be requested to bypass the security tunnel or be rejected).

After the user equipment UE executes an initial attach to the access network AN in step S11 an attach and authentication procedure is carried out between the user equipment UE and the access network AN.

In the next step S12 a security signalling is done. This step is required, due to the fact that the user equipment UE has not recognized the access network (AN) as trusted. The security signalling comprises a set-up step to establish a secure channel between the user equipment UE and the mobile network domain MND using the pre-provided security association and the security tunnel.

Next in step S13 the mobile network domain MND detects that the setup-signals of the security signalling were received via the pre-provisioned security tunnel.

Then, the mobile network domain MND informs the user equipment UE in step S14 that it is attached to a trusted access network AN.

Now, the user equipment UE can be sure of being attached to a trusted access network AN. The user equipment UE is consequently able to access the network services as it can be done from a trusted access network AN (step S15). Therefore, e.g. no secure channel needs to be used between the user equipment UE and the mobile network domain MND. Also no encryption of the data traffic, different data connection setup procedures, etc. between them are needed. It should be noted that this gain is achieved due to the fact that this regular data traffic will be configured to bypass the pre-provisioned security tunnel IPSec between the access network (AN) and the mobile network Domain (MND).

Figure 2 shows a flow diagram illustrating a method of a second, more specific embodiment of the present invention.

The flow diagram in Fig. 2 is a further embodiment of that in Fig. 1. Consequently, in Fig. 2 the step S20 corresponds mainly to step S10 in Fig. 1, the step S21 to step S11, step S22 to step S12, step S23 to step S13, step S26 to step S14 and step S27 to step S15.

In contrast to Fig. 1 in Fig. 2 the mobile network domain MND is composed of the security gateway SecGW, the data gateway DGW and the mobile network authenticator MNA. Here, the security gateway SecGW is a network element of the MND that is used to serve as interface point of the (mobile network domain MND to receive traffic from untrusted accesses, while the data gateway DGW is a network element of the mobile network domain MND that is used as an interface point to receive the data traffic from trusted alternative access networks. It should be noted that in such environments, the data traffic received at SecGW is forwarded to the data gateway DGW, where the service access is provided.)

Therefore, in step S20 the security association and security tunnel is established between the unrecognized trusted access network AN and the security gateway SecGW of the mobile network domain MND. The traffic selectors in the pre-provisioned security association may be omitted, if the access network AN is configured to send "regular" traffic directly to the other element in the mobile network domain MND, i.e. the Data GW.

Also the step S22 is performed between the user equipment UE and the security gateway SecGW wherein this step S22 comprises the security signalling such as described above and the authentication to the security gateway SGW.

The step S23 is done by the security gateway SecGW.

In Fig. 2 after step S23 two additional steps S24 and S25 are conducted within the mobile network domain MND. Here, in step S24 the security gateway SecGW sends authentication information and also additional information that the access network AN is a trusted access network AN to the mobile network authenticator MNA. Based on these information the mobile network authenticator MNA is then able to come to a decision whether the access network AN is to be handled as a trusted or an untrusted access network AN. Considering this information (besides the authentication information), the mobile network authenticator MNA comes to a corresponding decision, i.e. it declares the access network AN as trusted in step S25.

This decision of the mobile network authenticator MNA is then sent in the subsequent step S26 to the user equipment UE which then firstly notifies that it is actually attached to a trusted access network AN. Having this information, the user equipment UE shall send the data traffic directly to the data gateway DGW (as opposed to sending it encrypted to the security gateway SecGW, without receiving the information of the access network AN being trusted.)

Fig. 3 shows a flow diagram illustrating a method of a third, even more specific embodiment of the present invention.

The flow diagram in Fig. 3 is a further embodiment of that in Fig. 2. Consequently, in Fig. 3 the step S30 corresponds mainly to step S20 of Fig. 2, the step S31 to step S21, step S33 to step S22, step S34 to step S23, step S35 to step S24, step S36 to step S25, step S37 to step S26 and step S38 to step S27.

In Fig. 3 the access network (AN) is a Non-3GPP Access Network. The security gateway SecGW is an ePDG (evolved Packet Data Gateway) within a visited public land mobile network (VPLMN). The mobile network authenticator MNA is an AAA-server within a home public land mobile network (HPLMN).

Since the access network AN is initially not recognized to be a trusted access network AN, the user equipment UE initially assumes that this access network AN is an untrusted access network AN. The user equipment UE therefore executes a discovery step S32 after the step 31 to discover the GPDG within the VPLMN. Having received the notification on the access network AN being trusted, the user equipment UE will start a step to discover a PDN gateway.

The PDN is a network to which the user equipment UE wants to establish a network access via the trusted access network AN. For example the PDN can be the public internet or it can also be the network that provides MMS (multimedia message services) to the users. If the S2c interface is used, the DSMIP is the IP mobility protocol. In a 3GPP network the PDN gateway plays the role of the home agent. The DSNIP is an IP mobility protocol that the home agent uses to provide an mechanism that ensures that while the terminal is moving it is still be seen to be "stable". This means that the IP

address of the user equipment UE should not be changed while the user equipment UE is moving.

Hereinafter, a specific embodiment of the method according to the present invention is described on the basis of a radio communication system employing at least partially access network that follows other set of standards than defined by 3GPP but fulfilling standards to be connected to an evolved 3GPP core network. Firstly, the general system architecture of this communication system is described using Figure 4 and after that a more specific system overview is described using Fig. 5.

Fig. 4 shows a block diagram of a basic radio communication system as it is used for 3GPP.

In Fig. 4 the radio communication system is denoted by reference sign RCS.

The radio communication system RCS comprises one user equipment UE and four networks, i.e. two access a networks AN_A, AN_B and two public land mobile networks VPLMN, HPLMN. The two access networks AN_A, AN_B differ from each other in their network access technology. The first access network AN_A is for example implemented in a 3GPP access technology, whereas the second access network AN_B is implemented in another access technology such as WiMAX, DSL or WLAN, and is therefore non-3GPP network access technology. These access networks AN_A, AN_B are communicating with the user equipment UE via a radio interface using base stations BS within the corresponding access networks AN_A, AN_B.

Each user equipment UE is assigned to a home PLMN, the so-called HPLMN. The base station BS of the corresponding access network AN_N, AN_B are for example coupled with the home network HPLMN of the user equipment UE by means of a gateway

GW and optionally a visited network VPLMN. In the embodiment shown in Fig. 4 a home agent HA of the user equipment UE is located in the home network HPLMN. In an alternative embodiment this home agent HA is e.g. located in the visited network VPLMN (see dotted line).

In mobile IP the home agent HA denotes a router on the network of a user equipment UE which tunnels datagrams for delivery to the user when it is away from its network home and maintains current location information for the corresponding user equipment UE.

The home network HPLMN typically comprises an AAA server AAA which performs an access control policy enforcement and auditing framework for the home network's HPLMN computing system. Further, there is a home subscriber server HSS within the home network HPLMN. The HSS denotes a component of the IP multimedia system which comprises a central database for subscriber information. The HSS is a database that e.g. supports the EMS network entities that actually handle data. It contains the subscription related information (such as user profiles), performs authentication and authorisation of the user and provides information about the users' physical location.

Figure 5 shows a block diagram of a radio communication system for establishing a communication between a user equipment and a public network via an unrecognized trusted network according to an embodiment of the present invention.

The radio communication system in Fig. 5 comprises three networks, the home network HPLMN, the visited network VPLMN and a non-3GPP access network AN. Each of these networks comprise an own operator OP.

It is assumed that the access network AN is an initially "unrecognized" trusted non-3GPP access network AN. That means

that after an attached request by the user equipment UE the user equipment UE actually does not know that this access network AN is trusted or untrusted.

The access network AN is a non-3GPP access network AN. The other two networks HPLMN, VPLMN support 3GPP access technologies.

The visited network VPLMN comprises two gateways, a PDN data gateway PDNGW and a security gateway an ePDG. Both of these gateways PDNGW, ePDG form an interface point to the unrecognized trusted access network AN. This is described in more detail hereinafter, especially with regard to the embodiments in Figs. 6 and 7. The visited network VPLMN further comprises a 3GPP AAA-proxy which is connected to the two gateways PDNGW and ePDG via corresponding connecting means S6b and SWm, respectively.

The home network HPLMN comprises a AAA server which is connected to the home subscriber server HSS via connection lines SWx. The AAA-server forms the interface point to the AAA-proxy of the visited network VPLMN via connecting lines SWd.

The user equipment UE is connected to the visited network VPLMN via the unrecognized trusted network AN: For this the user equipment UE is firstly connected to the ePDG of the visited network VPLMN by means of a first coupling interface. This coupling interface comprises a first radio interface I1 from the user equipment UE to the access network AN and then a second interface I2 from this access network directly to the ePDG. This second interface I2 comprises a preconfigured security-tunnel IPSec. Further, the user equipment UE is connected to the PDN gateway via a third interface S2c using the unrecognized trusted network AN.

Reference is now made to Fig. 6 which shows a message flow diagram illustrating a method of a forth, detailed embodiment

of the present invention. This method employs a system architecture of a radio communication system RCS as shown in Fig. 5. Fig. 6 shows a complete message flow for an attach of a user equipment to an initially unrecognised trusted non-3GPP access network which is not supporting 3GPP access technologies such as 3GPP authentication.

Hereinafter the different steps of these methods are described in detail:

Step S40:

A key aspect in the described method according to the present invention is the preprovision of a security association (SA) and an IPSec tunnel between the gateway trusted non-3GPP access network AN and the ePDG gateway of the visited network VPLMN. The security association employs an internet key exchange (IKE or IKEv2) which is a kryptographic protocol used to set up the security association in the IKEv2 protocol suite. The internet key exchange IKE typically uses a Diffie-Hellmann key exchange to set up a shared session secret from which kryptographic keys are derived. Here, public key techniques or, alternatively, a pre-shared key are used to mutually authenticate the communicating parties of the internet key exchange.

Since the ePDG is always in the visited network VPLMN, this represents a relatively small number of security associations SA. Consequently, the 3GPP operator can administrate these security associations SA based on the network interconnection agreements with the operator OP of the trusted non-3GPP access network AN.

It is important that the security association has to be marked as belonging to a trusted non-3GPP access network AN in order that the functionality as will be described below in detail can be executed properly.

Steps 41 - S44:

The user equipment UE executes an inititial attach to the trusted access network AN (step S41). The user equipment is then authenticated using non-3GPP authentication techniques (step S42). The user equipment UE then executes another so-called IP layer attach L3 and receives the local IP address configuration from the trusted access network AN (step 43).

Since the user equipment UE holds no pre-provisioned information regarding the access network AN being trusted or not, the user equipment UE firstly handles the access network AN as an untrusted access network. Therefore, the user equipment UE executes an ePDG discovery to discover the corresponding ePDG within the visited network VPLMN. This ePDG discovery may be performed as described in chapter 6.3 of 3GPP of TS 24.302 step S44).

Steps S45 - 549):

The user equipment UE then executes an access authentication and a tunnel setup procedure. This access authentication and tunnel setup may be executed according to chapter 7.3 of 3GPP TS 24.402, chapter 8.2.2 of 3GPP TS 33.402, chapter 6.5 of 3GPP TS 24.302 and chapter 7.1.2.1 and 7.1.2.2 of 3GPP TS 29.273. However, this access authentication and tunnel setup according to the method of the present invention has the following additional embodiments:

a) all IKE messages which were sent from the user equipment UE to the ePDG are encapsulated to the pre-provisioned IPSEC tunnel between the trusted access network AN and the ePDG (step S46). This encapsulation is carried out by the trusted access network AN and the ePDG based on the destination addresses. This allows that the ePDG identifies that the user equipment UE is attached to an actually trusted access network AN. This is important for subsequent steps and especially for the security gateway

and the AAA server to be able to detect that the messages the ePDG received via the IPSec tunnel are forwarded from a trusted access network AN.

The ePDG within the visited network VPLMN detects that the IKE authentication of the security signalling is received by means of the pre-provided security association and the corresponding IPSec tunnel (step S47).

b) The ePDG inserts an information regarding to the trusted network, i.e. an information that the access network is a trusted access network AN, to the authentication request that is sent from the ePDG to the 3GPP AAA server. This authentication request further comprises the user ID and some APN information (step S48). Over the SWm interface this "trusted access network" information can be encoded into a new AVP (attribute value pair) or a new flag in the PNIP6 feature vector.

In one optimal embodiment also the identity of the access network AN belonging to the trusted access network AN are included. This can help the AAA server within the home network HPLMN to decide about accepting this "proposal" of the ePDG within the visited network VPLMN for handling the access network AN as a trusted access network.

c) The 3GPP AAA server retrieves the authentication vectors and the user profiles from the ePDG (step S49). The AAA server then executes the authentication typically using an EAP-AKA procedure. The EAP-AKA is an authentication mechanism which allows that the 3GPP network checks whether the user equipment is really who it claims to be.

Optionally, it is also possible that the AAA server processes the authentication using an EAP-AKA' procedure if the option of using the ID of the access network AN is selected. The AAA server then decides whether the access network AN is accepted to be a trusted or an untrusted

access network AN. This authentication procedure has to be executed within the home network HPLMN where the AAA server is located.

Step 41x:

If the AAA server accepts the access network AN, i.e. if the AAA server decides that the access network is a trusted network, the AAA server then informs the user equipment UE about this decision (step 410).

Step 42x:

The step 420 corresponds mainly to the steps S15, S27 and S38 in the embodiments described in Figs. 1, 2 and 3, respectively. Since the user equipment UE now can be sure of being attached to a trusted access network AN it is consequently able to access the network services as they can be done from a trusted access network AN (step 420).

Fig. 7 shows a flow diagram illustrating a method of a fifth, more detailed embodiment of the present invention.

In Fig. 7 the steps S40 - S49 are identical tothe corresponding steps S40-S49 of Fig. 6. In Fig. 7 the step 41x of indicating to the user equipment about the decision of the AAA server is described in more detail. The step 41x of Fig. 6 comprises the following sub-steps 410 - S419:

In step 410' the AAA server sends an EAP-AKA request to the ePDG. This request contains a so-called trusted "access network" information which contains the decision of the AAA server that the access network is the trusted access network AN. Subsequently, the ePDG sends an IKE authentication response to the user equipment UE which contains the header, an ePDG identification, a certificate, an authentication and the EAP/AKA request of the AAA server. This IKE authentication response is transmitted using the security

association and the IPSEC tunnel (step 411). The user equipment then sends for a subsequent authorisation procedure an IKE authentication request (step S412) which contains a header and a EAP/AKA request to ePDG (step 412). This EAP/AKA request is then forwarded from the ePDG to the AAA server (step S413).

The AAA server then sends back an authentication answer (step 414) which contains an information about the EAP success together with some key information and an IP mobility mode selection.

The ePDG then sends an authorisation request containing an information about the access point, i.e. the access point name (APN) to the AAA server (step 415).

The AAA server then checks in step S416 if the IPSec tunnel which was used for the challenge response authentication is an allowed IPSec tunnel.

The APN defines the type of service that is provided in the packed data connection. This APN service may include an IPv6 or IPv4 connection to the public internet, a connection to a wireless application protocol (WAP) gateway to present translated internet pages, a bearer service for the delivery of messages, such as SMS or MMS. The access point name identifies an external network that is accessible from a mobile terminal such as the user equipment UE.

The AAA server then sends back an answer to the ePDG (step S417). This answer may contain an international mobile subscriber identity (IMSI) which denotes a unique number associated with all GSM and UMTS network mobile phone users. Typically, this IMSI is stored in the SIM-card inside a user equipment and is sent by the user equipment to the visited network. It is also used to acquire other details of the user equipment in the so-called home location register (HLR) or as locally copied in the visited local register (VLR). The

answer further contains the access point name, the address of the home agent and optionally the profile of the quality of a service (QoS).

In the subsequent step S418 the ePDG computes the authentication payload using the master session key (MSK) of the extensible authentication protocol (EAP).

The ePDG then sends the IKE authentication response to the user equipment (step S419). This response is again transmitted using the security association SA and the IPSec tunnel. This response contains the header, information about the EAP success and information about the IP mobility node selection (i.e. DSMIP). The response further comprises the address of the home agent and the "trusted access network" information which was sent in step S410' from the AAA server to the ePDG.

When the user equipment UE receives this notification while doing an IKEv2 authentication to an ePDG the user equipment UE has to identify this situation that - in spite of having not used EAP-AKA' for access authentication when attaching to the access network AN - it is in fact attached to a trusted access network AN.

In the step S410 the AT_TRUST_IND attribute can be used as being defined in chapter 8.2.3.1 of 3GPP TS 24.302. This attribute can be included to the EAP success message since at this stage the encryption of the whole communication path between the AAA server and the user equipment UE is already ensured. It should be noted that the AT_IPNS_RES (i.e. DSNIPV6) can be signalled in the same IKEv2 message as the identication of the "trusted access network" information. Here, only DSNIPv6 can be used since there is not mechanism for network based mobility due to the lack of EAP-AKA support by the trusted access network AN.

Since the user equipment UE is now attached to a trusted access network (step S420), this means that the security association to the ePDG is no more needed for obtaining an IP connectivity. Therefore, the security association SA (i.e. IKEV2 SA and any child of this security association) which is created during the authentication procedure is terminated. The user equipment UE then is able to discover the PDN gateway via DNS or DHCPv6. This is only needed if the PDN IP address was not received during the previous steps. Then the DSNIPv6 authentication and authorisation is executed. This procedure is similar to those described in chapter 9.2.2 of 3GPP 33.402, chapter 5.1.2 of 3GPP DS 24.303 and chapter 9.1.2.1 of 3GPP TS 29.273.

The procedure to be followed in the case of handover from 3GPP access to the trusted access network AN does not support 3GPP authentication (i.e. non-3GPP access) is similar to the above-described procedure. The main difference is that the PDN gateway address shall be available (ePDG shall receive the PDN gateway identity from the home subscriber server via the AAA server) and, therefore, the PDN gateway discovery is then not needed. The IP address configuration is either not needed since the user equipment shall preserve its remote IP address.

The PDN is a network to which the user equipment UE wants to establish a network access via the trusted access network AN. For example the PDN can be the public internet or it can also be the network that provides MMS (multimedia message services) to the users. If the S2c interface is used, the DSMIP is the IP mobility protocol. In a 3GPP network the PDN gateway plays the role of the home agent. The DSNIP is an IP mobility protocol that the home agent uses to provide an mechanism that ensures that while the terminal is moving it is still be seen to be "stable". This means that the IP address of the user equipment UE should not be changed while the user equipment UE is moving.

While embodiments and applications of this invention have been shown and described above, it should be apparent to those skilled in the art, that many more modifications (than mentioned above) are possible without departing from the inventive concept described herein. The invention, therefore, is not restricted except in the spirit of the appending claims. It is therefore intended that the foregoing detailed description is to be regarded as illustrative rather than limiting and that it is understood that it is the following claims including all equivalents described in these claims that are intended to define the spirit and the scope of this invention. Nor is anything in the foregoing description intended to disavow the scope of the invention as claimed or any equivalents thereof.

Although only one user equipment is shown in the previous figures for the purpose of explanation, it is contemplated that multiple user equipments are typically employed. The same applies for the trusted access networks, mobile networks, ePDGs, PDNs, VPLMNs, HPLMNs, etc.

The user equipments may also be denoted as mobile devices (e.g. mobile telephones), mobile stations, and mobile communication devices. The user equipment can also be such devices as personal digital assistants (PDA) with transceiver capability or personal computers with transceiver capability.

The content of the above mentioned 3GPP technical specifications (i.e. 3GPP TS) and especially the mentioned chapters are hereinafter fully incorporated by reference into the disclosure of the present patent application.

It should be noted that if the trusted non-3GPP access network does not suppor EAP-AKA - authentication, only DSMIP mobility protocol can be used if there is no other means to inform the trusted access network in security gateway about the IP address allocated to the user equipment. This IP address however would be required for the network based

mobility. This also means that the proposed method that avoids using the ePDG and the security association overhead to it can be used only if the user equipment UE supports DSMIP. The supported (and preferred) mobility protocols are typically signalled by the user equipment during the authentication procedure. If no support for DSMIP is signalled by the user equipment UE, the 3GPP AAA server will not be able to utilize the method as proposed above. In this case, the user equipment will be attached using network based mobility via the ePDG. In this case, however, the ePDG is considered to be a network element that is really required to provide the IP connectivity for that type of user equipment UE.

Used abbreviations and reference numbers:

3GPP:	3rd Generation Partnership Project
AAA	Authentication, Authorization, Accounting
AGW:	Access Gateway
AKA:	Authentication and Key Agreement
AN, AN_A, AN_B	Access network
BS	Base station
DGW	Data gateway
DSMIP:	Dual Stack MIP
EAP:	Extensible Authentication Protocol
EPC	Evolved Packet Core
ePDG:	evolved Packet Data Gateway
EPS:	Evolved Packet System
GW	Gateway
HA	Home Agent
HLR	home location register
HPLMN:	Home PLMN
HSS	Home Subscriber Server
I1, I2	Interfaces
IKE	Internet Key Exchange
IP:	Internet Protocol
IPSec:	Internet Protocol Security
MIP:	Mobility Internet Protocol
MND	mobile network domain
MS:	Mobile Station
MSK	master session key
OP	Operator
PDA:	personal digital assistant
PDN GW:	PDN Gateway
PDN:	Packet Data Network
PLMN:	public land mobile network
PSTN	public switched telephone networks
RCS	radio communication system
ROA	recognized operating agency

S6b, S6c	Interfaces
SA:	security association
SecGW	Security gateway
SWx, SWm, SWd	Interfaces
UE:	User Equipment
VLR	visited local register
VPLMN:	visited PLMN
S10-S15	steps
S20-S27	steps
S30-S39	steps
S40-S420	steps

CLAIMS

1. Method for establishing an access of an user equipment (UE) to a mobile network domain (MND) via an initially unrecognized trusted access network (AN), the method comprising:

Preproviding a security association (SA) and a security tunnel (IPSec) between the mobile network (MND) and the access network (AN);

Conducting an attach procedure by the user equipment (UE) which indicates an access request to the access network (AN);

Setting-up a secure channel between the user equipment (UE) and the mobile network domain (MND) to execute a security signalling using the security tunnel (IPSec);

Detecting by the mobile network (MND) that security signals of the security signalling were received via the pre-provisioned security tunnel (IPSec);

Notifying the user equipment (UE) by the mobile network domain (MND) that the user equipment (UE) is effectively attached to a trusted access network (AN).

2. Method according to claim 1,
wherein after the step of notifying, the user equipment (UE) carries out such network service invocation in the mobile network domain (MND) via the access network (AN) as this network service invocation can be done from a initially recognized trusted access network (AN).

3. Method according to at least one of the preceding claims, wherein the mobile network domain (MND) provides different interface points (SecGW, ePDG; DGW, PDN GW) for trusted access networks (AN) and untrusted access networks.

4. Method according to claim 3,
wherein the interface point used for untrusted access networks is a security gateway (SecGW, ePDG), especially an ePDG, and/or wherein the interface point used for a trusted access networks (AN) is a data gateway (DGW, PDN GW), especially a PDN Gateway (PDN GW).

5. Method according to claim 4,
wherein a user equipment (UE) which is connected to an unrecognized trusted access network (AN) is firstly connected to the corresponding interface point (SecGW, ePDG) for untrusted access networks, and after the user equipment (UE) having been informed about the access network (AN) being a trusted access network (AN), the user equipment (UE) then invokes the services of the mobile network domain (MND) via the interface point (DGW, PDN GW) provided for trusted access networks (AN).

6. Method according to at least one of the preceding claims,
wherein the security signalling comprises an authentication procedure and the user equipment (UE) is notified about the access network (AN) being trusted as part of this authentication procedure.

7. Method according to at least one of the preceding claims,
wherein the mobile network domain (MND) comprises two public land mobile networks (PLMN), especially one visited public land mobile network (VPLMN) where the access network (AN) is connected to and one home public land mobile network (HPLMN) that provides data services for the user equipment (UE) based on a subscription.

8. Method according to claim 7,
wherein the visited public land mobile network (VPLMN) and the home public land mobile network (HPLMN) are the same networks.

9. Method according to claim 7,
wherein the visited public land mobile network (VPLMN) and the home public land mobile network (HPLMN) are separate networks.

10. Method according to at least one of the claims 7 to 9,
wherein the visited public land mobile network (VPLMN) comprises a security gateway (SecGW), especially an ePDG, and/or wherein the home public land mobile network (HPLMN) comprises a mobile network authenticator (MNA), especially an AAA-server.

11. Method according to at least one of the preceding claims, wherein the step of detecting by the mobile network (MND) comprises the substep of sending authentication information and information that the access network (AN) is a trusted access network (AN) from the security gateway (SecGW, ePDG) to the mobile network authenticator (MNA).

12. Method according to claim 11,
wherein based on the received information from the security gateway (SecGW, ePDG) the mobile network authenticator (MNA) decides whether the access network (AN) is subsequently to be handled as a trusted access network (AN) or an untrusted access network.

13. Method according to at least one of the preceding claims, wherein the attach procedure comprises the further step of executing a discovery by the user equipment (UE) prior to the step of setting-up a secure channel (IPSec) in order to discover a security gateway (ePDG, SGW) within the mobile network domain (MND)

14. Method according to at least one of the preceding claims,

wherein the security association (SA) includes cryptographic keys, initialization vectors and/or digital certificates.

15. Method according to at least one of the preceding claims, wherein the security tunnel (IPSec) between the access network (AN) and the mobile network domain (MND) is an IPSec-tunnel (IPSec).

16. Method according to at least one of the preceding claims, wherein the access network (AN) comprises a non-3GPP access network (AN) and/or wherein the mobile network domain (MND) comprises at least one 3GPP mobile network (VPLMN, HPLMN).

17. Method according to at least one of the preceding claims, wherein for the security signaling between the user equipment (UE) and the mobile network domain (MND) a key agreement protocol, in particular IKEv2, is used.

18. Method according to at least one of the preceding claims, wherein the authentication procedure used by the mobile network domain (MND) is EAP-AKA.

19. Method according to any of claim 18 wherein the authentication procedure comprises an authentication step and a subsequently or parallel conducted authorisation step.

20. Method according to at least one of the preceding claims, wherein the user equipment (UE) is a mobile communication devices, especially a cell phone or a mobile stations or a PDA.

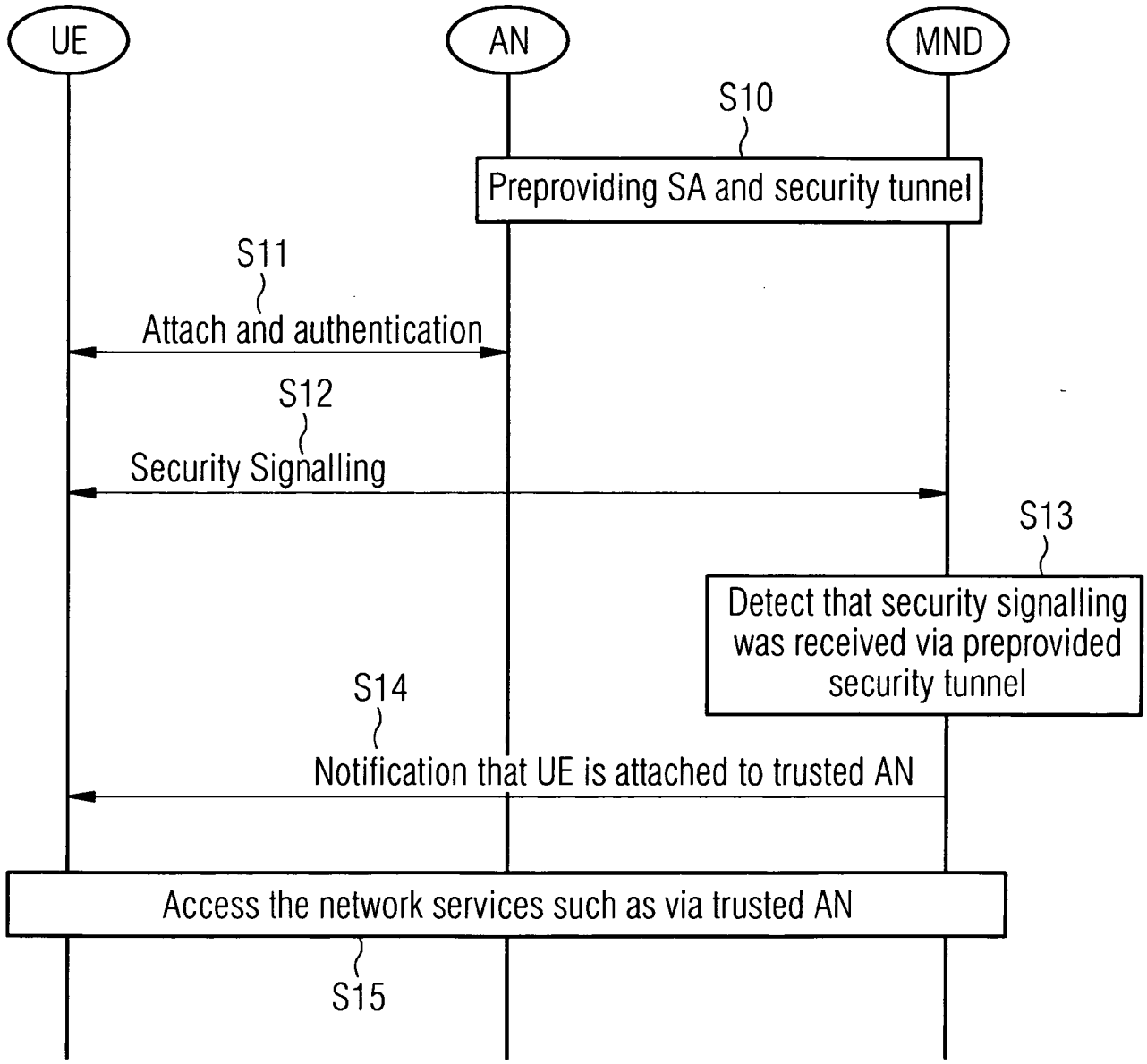
21. Radio communication system (RCS), comprising:
- at least one user equipment (UE),
- a mobile network domain (MND),
- an unrecognized trusted access network (AN),

wherein the user equipment (UE), the mobile network (MND) and the access network (AN) are arranged such to supporting a method according to one of the claims 1 to 20.

22. System according to claim 21,
wherein the system architecture of the radio communication system (RCS) is the System Architecture Evolution.

23. System according to claim 22,
wherein the main component of the system architecture of the radio communication system (RCS) is the Evolved Packet Core.

FIG 1


UE
AN
MND
S10
Preproviding SA and security tunnel
S11
Attach and authentication
S12
Security Signalling
S13
Detect that security signalling was received via preprovided security tunnel
S14
Notification that UE is attached to trusted AN
Access the network services such as via trusted AN
S15

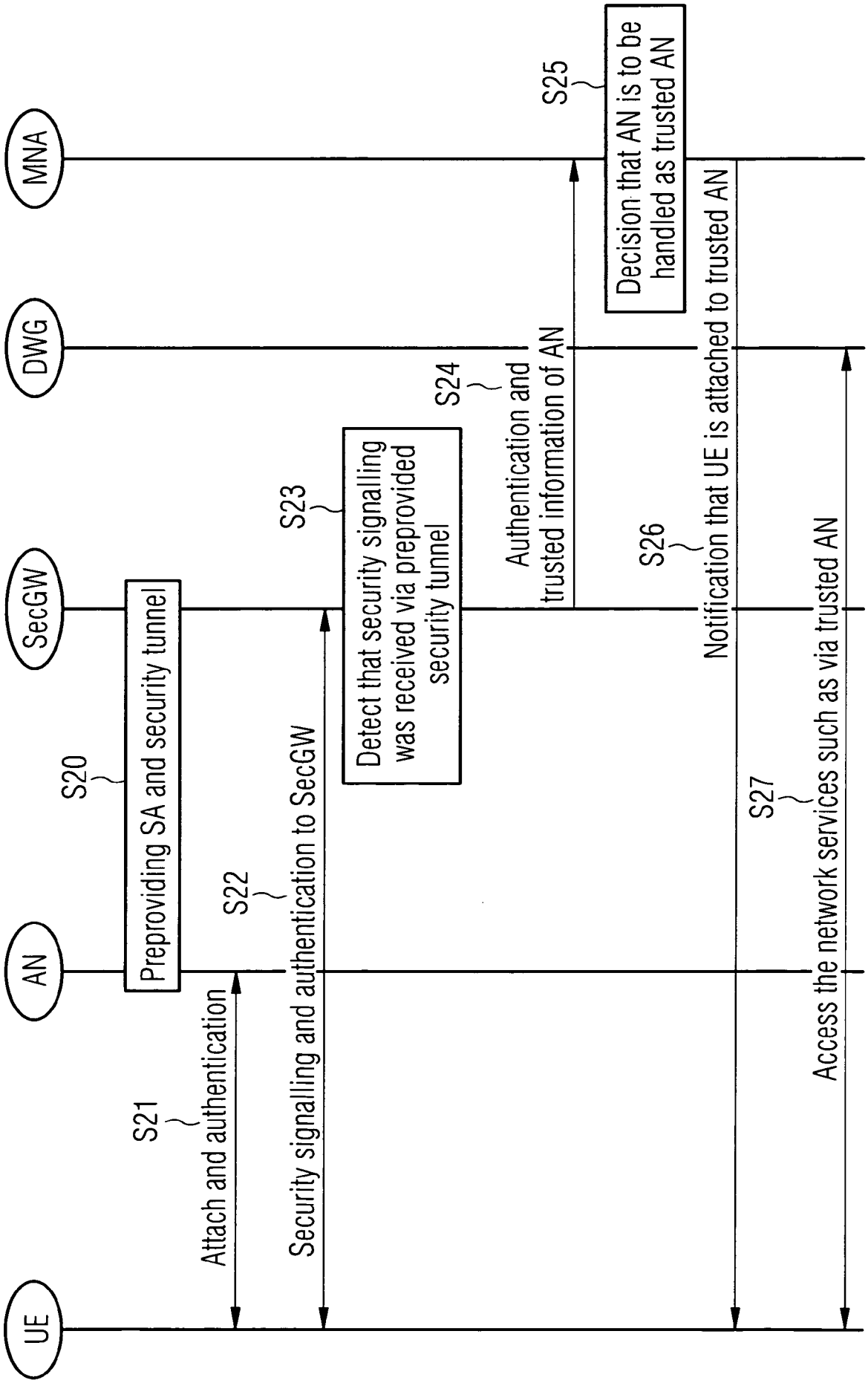
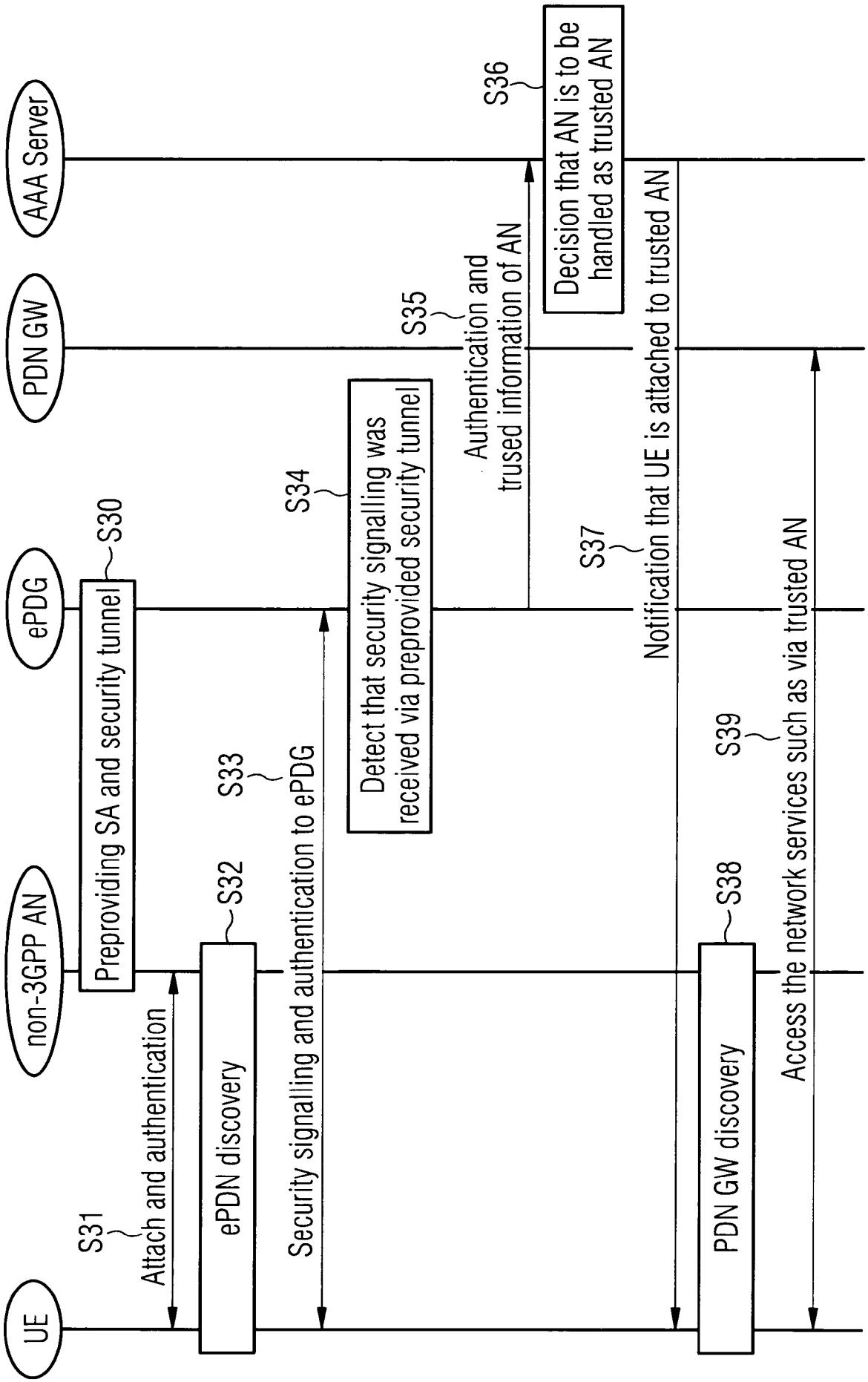

UE
AN
SecGW
DWG
MNA
S20
Preproviding SA and security tunnel
S21
Attach and authentication
S22
Security signalling and authentication to SecGW
S23
Detect that security signalling was received via preprovided security tunnel
S24
Authentication and trusted information of AN
S25
Decision that AN is to be handled as trusted AN
S26
Notification that UE is attached to trusted AN
S27
Access the network services such as via trusted AN

FIG 2

FIG 3


UE
non-3GPP AN
ePDG
PDN GW
AAA Server
S31
Attach and authentication
S30
Preproviding SA and security tunnel
S32
ePDN discovery
S33
Security signalling and authentication to ePDG
S34
Detect that security signalling was received via preprovided security tunnel
S35
Authentication and trused information of AN
S36
Decision that AN is to be handled as trusted AN
S37
Notification that UE is attached to trusted AN
S38
PDN GW discovery
S39
Access the network services such as via trusted AN

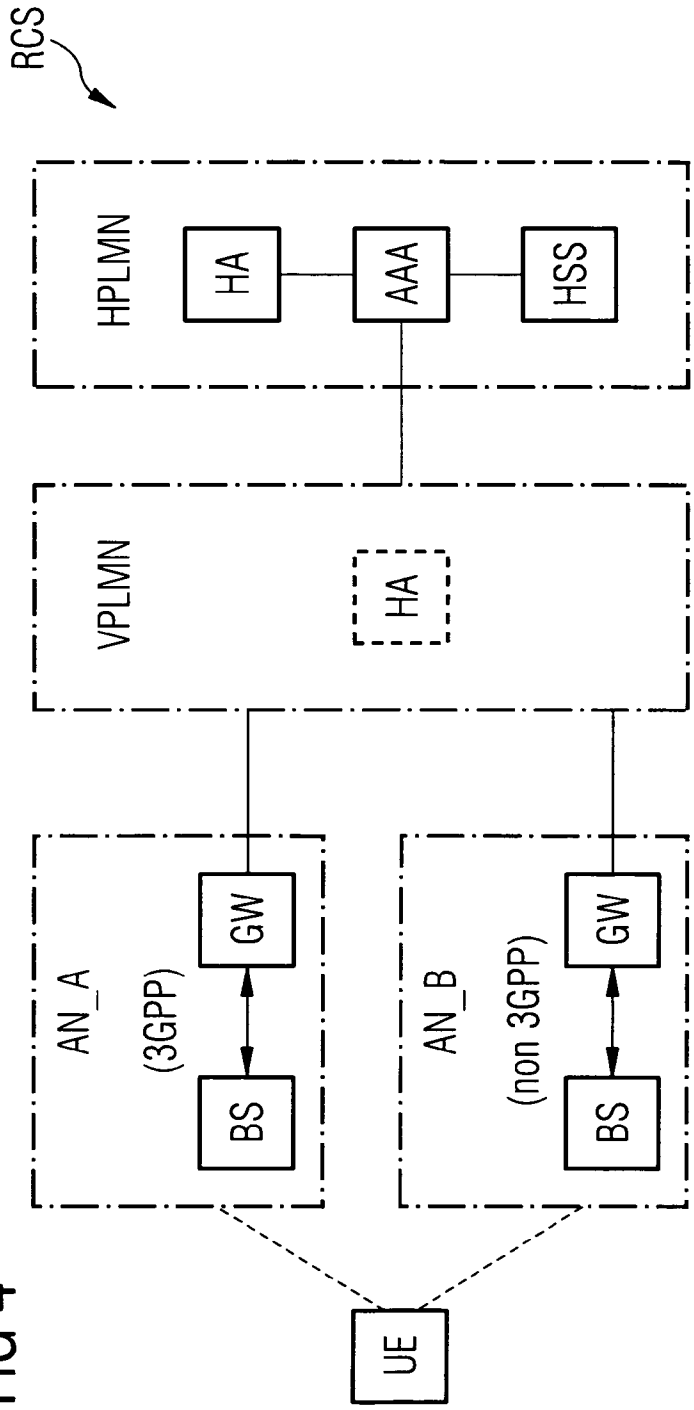

RCS
HPLMN
HA
AAA
HSS
VPLMN
HA
AN_A
(3GPP)
GW
BS
AN_B
(non 3GPP)
GW
BS
UE

FIG 4

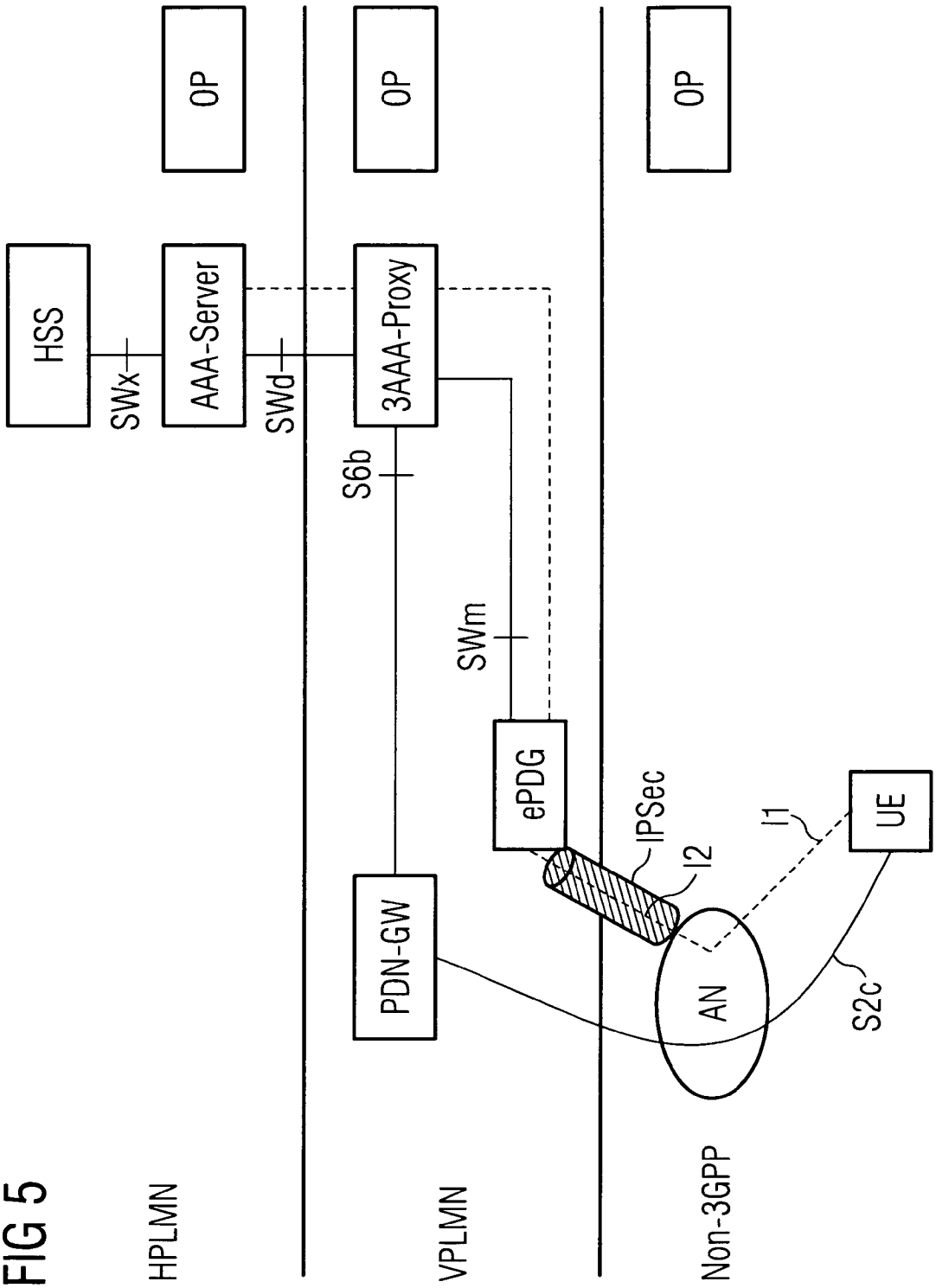

OP
OP
OP
HSS
AAA-Server
3AAA-Proxy
SWx
SWd
S6b
SWm
ePDG
IPSec
I1
I2
UE
PDN-GW
AN
S2c
HPLMN
VPLMN
Non-3GPP

FIG 5

FIG 6

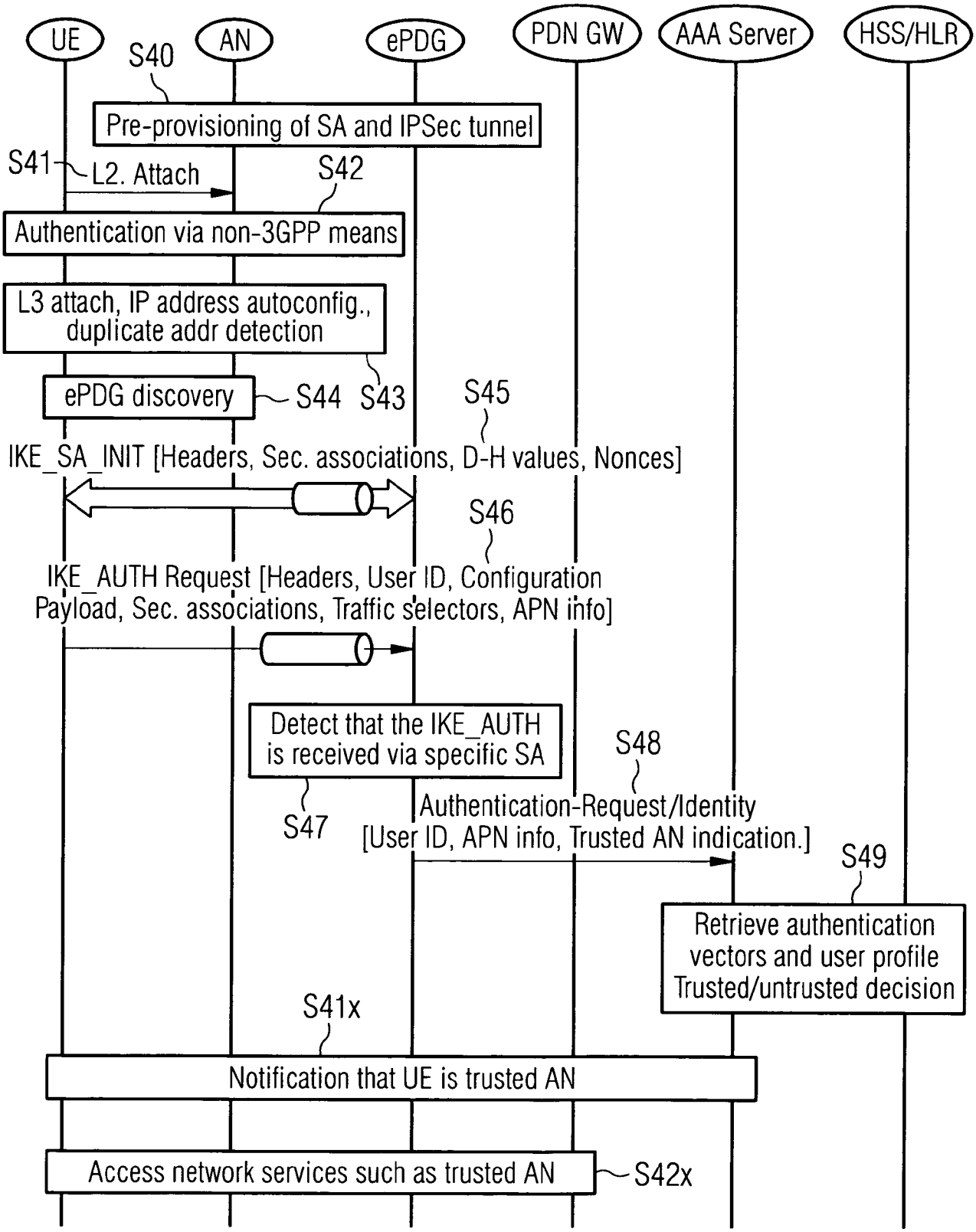
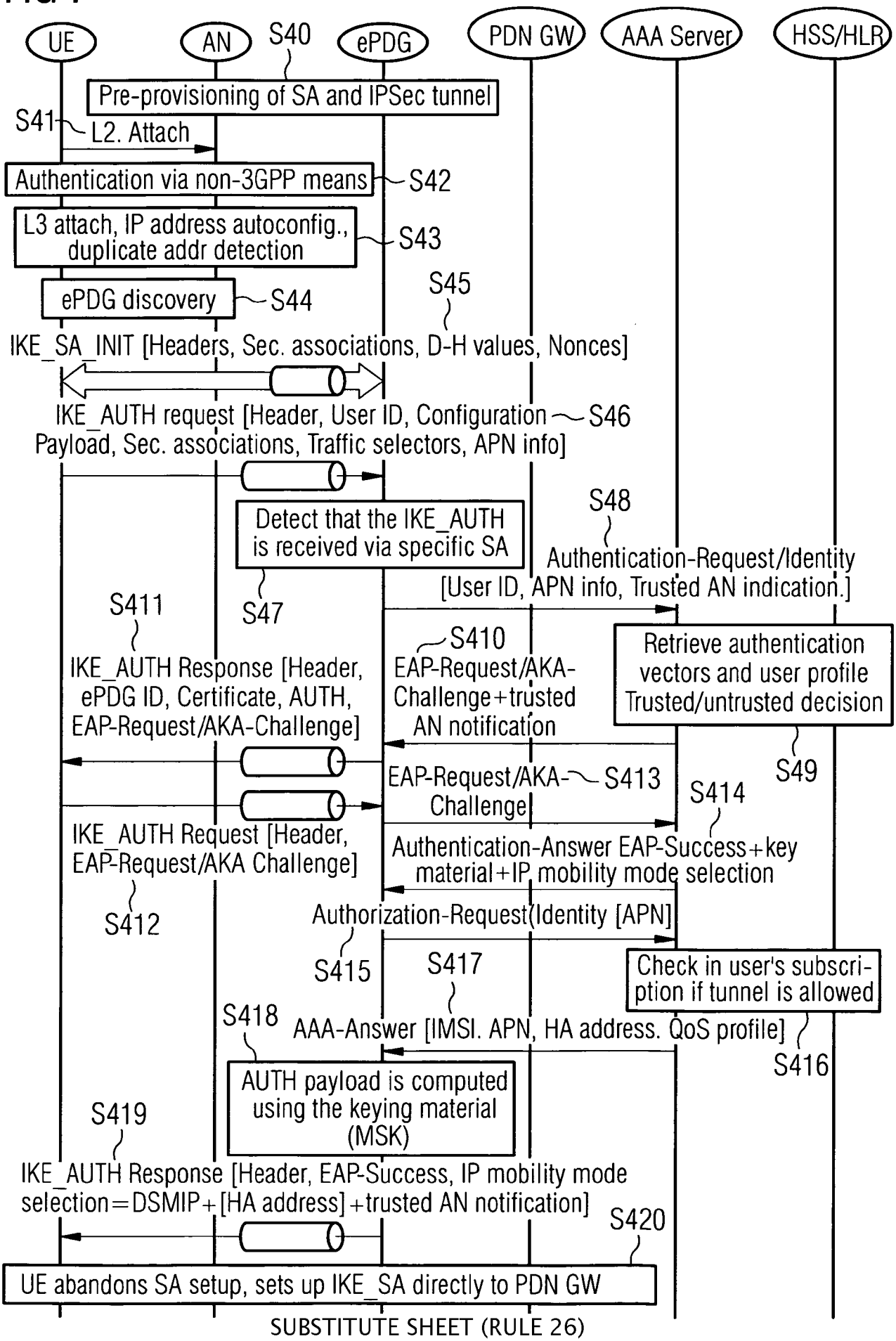

UE
AN
ePDG
PDN GW
AAA Server
HSS/HLR
S40
Pre-provisioning of SA and IPSec tunnel
S41
L2. Attach
S42
Authentication via non-3GPP means
L3 attach, IP address autoconfig., duplicate addr detection
ePDG discovery
S44
S43
S45
IKE_SA_INIT [Headers, Sec. associations, D-H values, Nonces]
S46
IKE_AUTH Request [Headers, User ID, Configuration Payload, Sec. associations, Traffic selectors, APN info]
Detect that the IKE_AUTH is received via specific SA
S47
S48
Authentication-Request/Identity [User ID, APN info, Trusted AN indication.]
S49
Retrieve authentication vectors and user profile Trusted/untrusted decision
S41x
Notification that UE is trusted AN
Access network services such as trusted AN
S42x

FIG 7


UE
AN
S40
ePDG
PDN GW
AAA Server
HSS/HLR
Pre-provisioning of SA and IPSec tunnel
S41
L2. Attach
Authentication via non-3GPP means
S42
L3 attach, IP address autoconfig., duplicate addr detection
S43
ePDG discovery
S44
S45
IKE_SA_INIT [Headers, Sec. associations, D-H values, Nonces]
IKE_AUTH request [Header, User ID, Configuration Payload, Sec. associations, Traffic selectors, APN info]
S46
Detect that the IKE_AUTH is received via specific SA
S47
S48
Authentication-Request/Identity [User ID, APN info, Trusted AN indication.]
S411
IKE_AUTH Response [Header, ePDG ID, Certificate, AUTH, EAP-Request/AKA-Challenge]
S410
EAP-Request/AKA-Challenge+trusted AN notification
Retrieve authentication vectors and user profile Trusted/untrusted decision
S49
EAP-Request/AKA-Challenge
S413
S414
IKE_AUTH Request [Header, EAP-Request/AKA Challenge]
Authentication-Answer EAP-Success+key material+IP mobility mode selection
S412
Authorization-Request(Identity [APN]
S415
S417
Check in user's subscription if tunnel is allowed
S418
AAA-Answer [IMSI. APN, HA address. QoS profile]
S416
AUTH payload is computed using the keying material (MSK)
S419
IKE_AUTH Response [Header, EAP-Success, IP mobility mode selection=DSMIP+[HA address]+trusted AN notification]
S420
UE abandons SA setup, sets up IKE_SA directly to PDN GW

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/051161

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/02 H04L29/06

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)
H04L H04W

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2008/155066 A2 (PANASONIC CORP [JP]; BACHMANN JENS [DE]; WENIGER KILIAN [DE]; ARAMAKI) 24 December 2008 (2008-12-24) page 2, line 24 - page 5, line 3 page 16, line 6 - page 21, line 14 page 29, line 1 - page 32, line 13	1-23
A	SHEFFER Y; NIR Y: "Secure Beacon: Securely Detecting a Trusted Network; draft-sheffer-ipsec-secure-beacon-03.txt" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, 21 January 2008 (2008-01-21), XP015054614 section 2 section 3 section 4	1-23

☐ 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 document 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	Date of mailing of the international search report
3 November 2009	10/11/2009

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Ruiz Sanchez, J

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2009/051161

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2008155066 A2	24-12-2008	NONE	