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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
03 May 2018 (03.05.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/077438 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/EP2016/076203

(22) International Filing Date:
31 October 2016 (31.10.2016)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **NOKIA TECHNOLOGIES OY** [FI/FI]; Karaportti 3, 02610 Espoo (FI).

(72) Inventor: **HORN, Guenther**; Prälat-Zistl-Str. 12, 80331 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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

(54) Title: ENHANCEMENTS IN AKA-BASED AUTHENTICATION

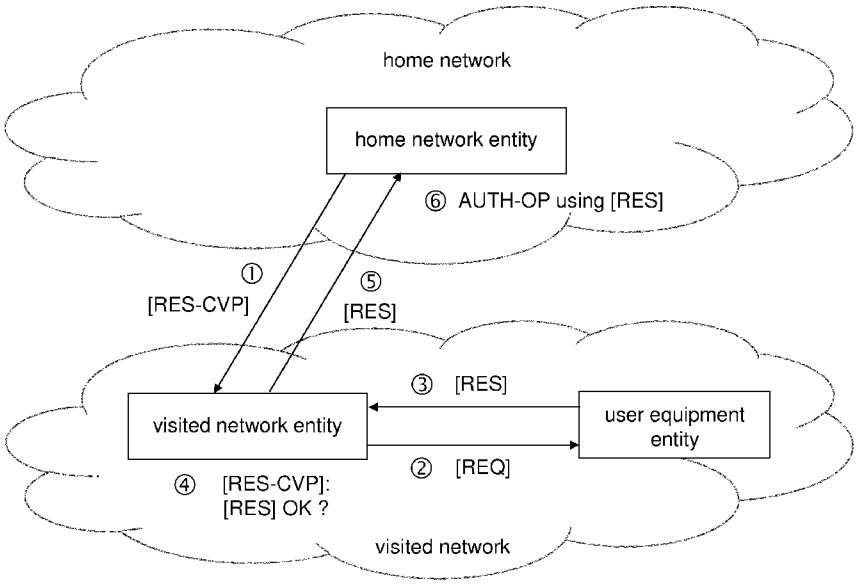

Figure 1

(57) Abstract: There are provided measures for enhancements in AKA-based authentication, especially for roaming situations. Such measures exemplarily comprise provision of a parameter enabling verification of correctness of an authentication response of a user equipment from a home network to a visited network of the user equipment, said parameter being derivable from an expected authentication response, verification of correctness of the authentication response of the user equipment entity using said parameter in the visited network, provision of the authentication response of the user equipment from the visited network to the home network as an indication of completion of authentication of the user equipment when correctness of the authentication response of the user equipment is positively verified, and confirmation of completion of authentication of the user equipment by the visited network in the home network when the provided authentication response corresponds to the expected authentication response.

WO 2018/077438 A1

[Continued on next page]

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

Published:

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

Description

Title

Enhancements in AKA-based authentication

Field

The present invention relates to enhancements in AKA-based authentication. More specifically, the present invention relates to measures (including methods, apparatuses and computer program products) for enabling/realizing enhancements in AKA-based authentication, especially for roaming situations.

Background

Generally, security is a vital issue in all kinds of communication networks, thus paying a key role in the development of modern and future communication systems, including 3GPP systems like LTE/LTE-A as well as NG/5G systems.

In the present specification, authentication is addressed as one aspect of security in communication systems. Specifically, the present specification is directed to subscriber authentication, i.e. authentication of a user equipment subscriber (the subscription on the USIM in the user equipment) or, stated in other words, between a user equipment and a network. For such subscriber authentication, various authentication mechanisms come into consideration, particularly including EAP-AKA' and EPS AKA. Even more specifically, the present specification is directed to subscriber authentication in roaming situations, i.e. when a user equipment user equipment to be authenticated is roaming in a visited network rather than in its home network.

In such roaming situations, the following considerations can be made in view of inter-network and, hence, inter-operator security issues.

Roaming relations between operators are currently based on trust. However, some home network operators may want to reduce the degree of trust they have to place in operators of visited networks of their subscribers. This is because the home network operators' trust

may be abused by visited network operators, e.g. for claiming false charges. The choice of an appropriate authentication technique may help here.

The security threat can be described as follows: A fraudulent visited network that has a valid roaming relationship with the home network operator may request authentication vectors for user equipment subscriber authentication from the home network and subsequently send a request affecting the state (status) of the user equipment user equipment (e.g. an update location request) for subscribers that are not actually present in the visited network. For example, the visited network operator may thereby hope to be able to obtain additional revenue by claiming charges for the allegedly visiting subscriber.

This security threat may exist even when the origin of the update location request can be verified by the home network through appropriate security measures in the interconnection network (e.g. through network domain security). This is because the visited network is an authorized participant in the interconnection network that, however, abuses the roaming relationship.

Another variant of this type of security threat consists in the visited network authenticating a visiting subscriber correctly, but then claiming charges for traffic allegedly incurred by this subscriber even when the subscriber has already left, or was never attached to, the visited network. For example, a visited network could properly authenticate the subscriber, but then not even bother sending the attach accept message.

In order to cope with such security threats in roaming situations, increased home control in roaming situations is desired. This means that, for example, the home network shall have means to ascertain that a subscriber whose location is updated to a new visited network has actually been authenticated involving this visited network. Additionally, this may also mean that the home network shall have means to ascertain a minimum authentication frequency for his roaming subscribers.

Stated in other words, it could be said that security mechanisms are needed to fight inter-operator fraud and misuse of international signaling networks, or that the home network is enabled to verify that his roaming subscriber is really attached to a visited network that claims it is.

Accordingly, there is a demand for enabling/realizing enhancements in authentication, especially for roaming situations, which can address the aforementioned security issues. Since AKA-based authentication is widely used in conventional communication system, it is preferable that such enhancements are enabled/realized in AKA-based authentication.

Summary

Various exemplifying embodiments of the present invention aim at addressing at least part of the above issues and/or problems and drawbacks.

Various aspects of exemplifying embodiments of the present invention are set out in the appended claims.

According to an example aspect of the present invention, there is provided a method (of a home network entity of a home network of a user equipment entity), the method comprising: providing, for a visited network entity of a visited network of the user equipment entity, a parameter enabling verification of correctness of an authentication response from the user equipment entity, said parameter being derivable from an expected authentication response from the user equipment entity, obtaining, from the visited network entity, the authentication response from the user equipment entity as an indication of completion of authentication of the user equipment entity, and confirming completion of authentication of the user equipment entity by the visited network entity when the obtained authentication response corresponds to the expected authentication response.

According to an example aspect of the present invention, there is provided a method (of a home network entity of a home network of a user equipment entity), the method comprising: recording, upon confirmation of completion of authentication of the user equipment entity by a visited network of the user equipment entity, a time of authentication of the user equipment entity and an identifier of the visited network, obtaining a request for a procedure affecting a state of the user equipment entity, said request including an identifier of an originating visited network of the user equipment entity, and rejecting the requested procedure, if the request is not received within a predefined time period since the recorded time of authentication of the user equipment, or if the identifier of the

originating visited network in the request does not correspond to the recorded identifier of the visited network.

According to an example aspect of the present invention, there is provided a method (of a visited network entity of a visited network of a user equipment entity), the method comprising: obtaining, from a home network entity of a home network of the user equipment entity, a parameter enabling verification of correctness of an authentication response from the user equipment entity, said parameter being related to an expected authentication response from the user equipment entity, obtaining, from the user equipment entity, the authentication response as a result of an authentication procedure between the visited network entity and the user equipment entity, verifying correctness of the authentication response from the user equipment entity using said parameter, and providing, to the home network entity, the authentication response from the user equipment entity as an indication of completion of authentication of the user equipment entity when correctness of the authentication response from the user equipment entity is positively verified.

According to an example aspect of the present invention, there is provided an apparatus (of a home network entity of a home network of a user equipment entity), comprising at least one processor and at least one memory including a computer program code, wherein the at least one memory and the computer program code are configured, with the at least one processor, to cause the apparatus to perform at least the following: providing, for a visited network entity of a visited network of the user equipment entity, a parameter enabling verification of correctness of an authentication response from the user equipment entity, said parameter being derivable from an expected authentication response from the user equipment entity, obtaining, from the visited network entity, the authentication response from the user equipment entity as an indication of completion of authentication of the user equipment entity, and confirming completion of authentication of the user equipment entity by the visited network entity when the obtained authentication response corresponds to the expected authentication response.

According to an example aspect of the present invention, there is provided an apparatus (of a home network entity of a home network of a user equipment entity), comprising at least one processor and at least one memory including a computer program code, wherein the at least one memory and the computer program code are configured, with the

at least one processor, to cause the apparatus to perform at least the following: recording, upon confirmation of completion of authentication of the user equipment entity by a visited network of the user equipment entity, a time of authentication of the user equipment entity and an identifier of the visited network, obtaining a request for a procedure affecting a state of the user equipment entity, said request including an identifier of an originating visited network of the user equipment entity, and rejecting the requested procedure, if the request is not received within a predefined time period since the recorded time of authentication of the user equipment, or if the identifier of the originating visited network in the request does not correspond to the recorded identifier of the visited network.

According to an example aspect of the present invention, there is provided an apparatus (of a visited network entity of a visited network of a user equipment entity), comprising at least one processor and at least one memory including a computer program code, wherein the at least one memory and the computer program code are configured, with the at least one processor, to cause the apparatus to perform at least the following: obtaining, from a home network entity of a home network of the user equipment entity, a parameter enabling verification of correctness of an authentication response from the user equipment entity, said parameter being related to an expected authentication response from the user equipment entity, obtaining, from the user equipment entity, the authentication response as a result of an authentication procedure between the visited network entity and the user equipment entity, verifying correctness of the authentication response from the user equipment entity using said parameter, and providing, to the home network entity, the authentication response from the user equipment entity as an indication of completion of authentication of the user equipment entity when correctness of the authentication response from the user equipment entity is positively verified.

According to an example aspect of the present invention, there is provided a computer program product comprising (computer-executable) computer program code which, when the program code is executed (or run) on a computer or the program is run on a computer (e.g. a computer of an apparatus according to any one of the aforementioned apparatus-related example aspects of the present invention), is configured to cause the computer to carry out the method according to any one of the aforementioned method-related example aspects of the present invention.

The computer program product may comprise or may be embodied as a (tangible/non-transitory) computer-readable (storage) medium or the like, on which the computer-executable computer program code is stored, and/or the program is directly loadable into an internal memory of the computer or a processor thereof.

Further developments and/or modifications of the aforementioned exemplary aspects of the present invention are set out in the following.

By way of exemplifying embodiments of the present invention, enhancements in AKA-based authentication, especially for roaming situations, which can address the aforementioned security issues, can be enabled/realized. In a nutshell, increased home control in roaming situations can be facilitated thereby.

Brief description of the drawings

In the following, the present invention will be described in greater detail by way of non-limiting examples with reference to the accompanying drawings, in which

Figure 1 shows a schematic diagram illustrating scheme of an enhanced authentication technique according to exemplifying embodiments of the present invention,

Figure 2 shows a flowchart illustrating an example of a method, operable at a home network entity, according to exemplifying embodiments of the present invention,

Figure 3 shows a flowchart illustrating an example of a method, operable at a visited network entity, according to exemplifying embodiments of the present invention,

Figure 4 shows a flowchart illustrating an example of a method, operable at a home network entity, according to exemplifying embodiments of the present invention,

Figure 5 shows a flow diagram illustrating an example of a procedure according to exemplifying embodiments of the present invention,

Figure 6 shows a flow diagram illustrating an example of another procedure according to exemplifying embodiments of the present invention,

Figure 7 shows a schematic diagram illustrating an example of a structure of apparatuses according to exemplifying embodiments of the present invention, and

Figure 8 shows a schematic diagram illustrating another example of a functional structure of apparatuses according to exemplifying embodiments of the present invention.

Detailed description

The present invention is described herein with reference to particular non-limiting examples and to what are presently considered to be conceivable embodiments of the present invention. A person skilled in the art will appreciate that the present invention is by no means limited to these examples and embodiments, and may be more broadly applied.

It is to be noted that the following description of the present invention and its embodiments mainly refers to specifications being used as non-limiting examples for certain exemplifying network configurations and system deployments. Namely, the present invention and its embodiments are mainly described in relation to 3GPP specifications being used as non-limiting examples. As such, the description of exemplifying embodiments given herein specifically refers to terminology which is directly related thereto. Such terminology is only used in the context of the presented non-limiting examples and embodiments, and does naturally not limit the invention in any way. Rather, any other system configuration or deployment may equally be utilized as long as complying with what is described herein and/or exemplifying embodiments described herein are applicable to it.

Hereinafter, various exemplifying embodiments and implementations of the present invention and its aspects are described using several variants and/or alternatives. It is generally to be noted that, according to certain needs and constraints, all of the described variants and/or alternatives may be provided alone or in any conceivable combination (also including combinations of individual features of the various variants and/or alternatives). In this description, the words “comprising” and “including” should be understood as not limiting the described exemplifying embodiments and implementations to consist of only those features that have been mentioned, and such exemplifying

embodiments and implementations may also contain features, structures, units, modules etc. that have not been specifically mentioned.

In the drawings, it is to be noted that lines/arrows interconnecting individual blocks or entities are generally meant to illustrate an operational coupling there-between, which may be a physical and/or logical coupling, which on the one hand is implementation-independent (e.g. wired or wireless) and on the other hand may also comprise an arbitrary number of intermediary functional blocks or entities not shown.

According to exemplifying embodiments of the present invention, in general terms, there are provided measures and mechanisms for enabling/realizing enhancements in AKA-based authentication, especially for roaming situations.

Figure 1 shows a schematic diagram illustrating scheme of an enhanced authentication technique according to exemplifying embodiments of the present invention.

As shown in Figure 1, the basic underlying system configuration is assumed to comprise a home network including at least one (involved/concerned) home network entity, e.g. AUSF/ARPF in case of a NG/5G system or HSS in case of a LTE/LTE-A system, and a visited network including at least one (involved/concerned) visited network entity, e.g. SEAF in case of a NG/5G system or MME in case of a LTE/LTE-A system. Further, it is assumed that a user equipment entity, e.g. a UE with a USIM, is not roaming in its home network but in the visited network.

As a starting point for the enhanced authentication technique described below, it is assumed that a subscriber authentication of the user equipment entity by the visited network (entity) is to be performed.

Based on such assumptions, the enhanced authentication technique can work as follows.

In a first phase, the home network (entity) provides a parameter enabling verification of correctness of an authentication response of/from the user equipment entity (hereinafter referred to as correctness verification parameter RES-CVP) to the visited network (entity). It is noted that the RES-CVP is derivable from or related to the expected authentication response XRES for the authentication of the user equipment entity by the

visited network (entity), while the expected authentication response XRES is known at the home network (entity) but is not provided to the visited network (entity).

In a second phase, the visited network (entity) issues an authentication request REQ to the user equipment entity. The authentication request includes authentication information dedicated for the authentication of the user equipment entity.

In a third phase, the user equipment entity issues an authentication response RES in response to the authentication request REQ to the visited network (entity).

In a fourth phase, the visited network (entity) verifies correctness of the authentication response RES of/from the user equipment entity using the RES-CVP. That is, the RES-CVP is constructed such that the visited network (entity) is enabled to verify correctness of the authentication response RES of/from the user equipment entity, but is not able to guess the (expected) authentication response RES without having been received (with a reasonable probability).

In a fifth phase, if correctness of the authentication response RES of/from the user equipment entity is positively verified in the fourth phase (i.e. when authentication of the user equipment entity by the visited network (entity) is successfully completed), the visited network (entity) provides the authentication response RES of/from the user equipment entity to the home network (entity), as an indication of completion of authentication of the user equipment entity. That is, the visited network (entity) proves to the home network (entity) that is has indeed authenticated the user equipment entity by sending back the full authentication response RES received from the user equipment entity. Insofar, the provision of the authentication response RES of/from the user equipment entity from the visited network (entity) to the home network (entity) can be regarded as an authentication confirmation or an authentication success indication.

Otherwise, if correctness of the authentication response RES of/from the user equipment entity is not positively verified in the fourth phase (i.e. when authentication of the user equipment entity by the visited network (entity) is not successful), the visited network (entity) aborts the authentication procedure, e.g. by sending an authentication rejection message to the user equipment entity.

In a sixth phase, the home network (entity) performs one or more authentication operations using the authentication response RES of/from the user equipment entity, as obtained from the visited network (entity) in the fifth phase. In particular, by comparing the obtained authentication response RES with the expected authentication response XRES, the home network (entity) can confirm completion of authentication of the user equipment entity by the visited network (entity) when the obtained authentication response RES

corresponds to the expected authentication response XRES. Also, the home network (entity) can link the recent authentication procedure with any subsequent procedure, preferably with any subsequent procedure affecting the state (status) of the user equipment entity.

According to exemplifying embodiments of the present invention, the correctness verification parameter RES-CVP is derivable from or related to the expected authentication response XRES for the authentication of the user equipment entity. More specifically, the correctness verification parameter RES-CVP is (constructed) such that the parameter is derivable from the expected authentication response, but the expected authentication response is not derivable from the parameter (so, there is an asymmetric/irreversible property in terms of producibility/derivability). That is, the correctness verification parameter RES-CVP is (constructed) such that the visited network (entity) is enabled to verify correctness of the authentication response RES of/from the user equipment entity, but is not able to guess the (expected) authentication response RES without having been received (with a reasonable probability). Accordingly, any parameter exhibiting these properties can be used.

As one example, the correctness verification parameter RES-CVP can be generated by decomposing the expected authentication response XRES, i.e. the correctness verification parameter RES-CVP can be a decomposed part of the expected authentication response XRES. If so, the correctness verification using the correctness verification parameter RES-CVP can comprise decomposing the authentication response RES of/from the user equipment entity in an equivalent manner as the decomposition of the expected authentication response XRES, and comparing a decomposed part of the authentication response RES of/from the user equipment entity with the correctness verification parameter RES-CVP, i.e. the decomposed part of the expected authentication response XRES. It is noted that the visited network (entity) can gather information of the decomposition of the expected authentication response XRES by/at the home network (entity) either implicitly, e.g. by analyzing the RES-CVP (in consideration of knowledge on the usual/specified form of XRES), or explicitly, e.g. by corresponding information being provided by the home network (entity).

This variant is described in further detail in an exemplary use case or implementation below.

As another example, the correctness verification parameter RES-CVP can be generated by calculating a hash value from the expected authentication response XRES and a random challenge RAND dedicated for authentication of the user equipment entity, i.e. the correctness verification parameter RES-CVP can be a calculated hash value. If so, the correctness verification using the correctness verification parameter RES-CVP can comprise calculating a hash value from the authentication response RES of/from the user equipment entity and the random challenge RAND (which is provided by the home network (entity), and comparing the calculated hash value with the hash value serving as the correctness verification parameter RES-CVP.

This variant assumes that the home and visited networks have a hash function h in common. The home network then sends only the hash value h(XRES, RAND) to the visited network, as the correctness verification parameter RES-CVP, where RAND is the random challenge contained in an authentication vector. Due to the one-way property of the hash function, the visited network cannot deduce XRES from h(XRES, RAND) and RAND. Hence, the visited network can send an authentication confirmation or an authentication success indication in the form of or containing RES to the home network only when it has actually received RES from the user equipment entity. Hence, the visited network can properly prove to the home network that is has indeed authenticated the user equipment entity. However, as compared with the above variant, this variant could be less preferable, since the hash function needs to be standardized and updating mechanisms need to be specified, and increased lengths for RES and XRES are required in order to ensure a sufficient security level (because with current/smaller lengths, like 32 or perhaps even 64 bits, the visited network could perform an exhaustive search of all possible XRES values, then compute h(XRES, RAND) until finding a match with the value received from the home network, thereby circumventing the security concept of the enhanced authentication technique according to exemplifying embodiments of the present invention).

The above-described enhanced authentication technique can generally be based on any AKA-based authentication mechanism, but can be most usefully applied to EPS AKA.

According to exemplifying embodiments of the present invention, the above-described enhanced authentication technique is based on an EPS AKA mechanism, which is

(mainly) modified (or enhanced) in that RES-CVP is provided instead of XRES and an authentication confirmation or authentication success indication in the form of RES is introduced. Insofar, if being based on an EPS AKA mechanism, the enhanced authentication technique according to exemplifying embodiments of the present invention is hereinafter referred to as EPS AKA*. It is noted that the thus effected modification or enhancement of EPS AKA* as compared with conventional EPS AKA is such that it does not affect the authentication exchange between the visited network (entity) and the user equipment entity; in particular, the user equipment entity does not see any difference between EPS AKA and EPS AKA*.

Figure 2 shows a flowchart illustrating an example of a method, operable at a home network entity, according to exemplifying embodiments of the present invention. The method of Figure 2 can be executed in a home network or by/at a home network entity, as illustrated in Figure 1.

As shown in Figure 2, a method according to exemplifying embodiments of the present invention, which is operable in the domain of the home network, comprises an operation (S210) of providing, for a visited network entity of a visited network of the user equipment entity, a parameter enabling verification of correctness of an authentication response from the user equipment entity, said parameter being derivable from an expected authentication response from the user equipment entity, an operation (S220) of obtaining, from the visited network entity, the authentication response from the user equipment entity as an indication of completion of authentication of the user equipment entity, and an operation (S230) of confirming completion of authentication of the user equipment entity by the visited network entity when the obtained authentication response corresponds to the expected authentication response.

With reference to the scheme of Figure 1, operation S210 corresponds to the first phase, operation S220 corresponds to the fifth phase, and operation S230 corresponds to the sixth phase.

Figure 3 shows a flowchart illustrating an example of a method, operable at a visited network entity, according to exemplifying embodiments of the present invention. The method of Figure 2 can be executed in a visited network or by/at a visited network entity, as illustrated in Figure 1.

As shown in Figure 3, a method according to exemplifying embodiments of the present invention, which is operable in the domain of the visited network, comprises an operation (S310) of obtaining, from a home network entity of a home network of the user equipment entity, a parameter enabling verification of correctness of an authentication response from the user equipment entity, said parameter being related to an expected authentication response from the user equipment entity, an operation (S320) of obtaining, from the user equipment entity, the authentication response as a result of an authentication procedure between the visited network entity and the user equipment entity, an operation (S330) of verifying correctness of the authentication response from the user equipment entity using said parameter, and an operation (S340) of providing, to the home network entity, the authentication response from the user equipment entity as an indication of completion of authentication of the user equipment entity when correctness of the authentication response from the user equipment entity is positively verified.

With reference to the scheme of Figure 1, operation S310 corresponds to the first phase, operation S320 corresponds to the third phase, operation S330 corresponds to the fourth phase, and operation S340 corresponds to the fifth phase.

Figure 4 shows a flowchart illustrating an example of a method, operable at a home network entity, according to exemplifying embodiments of the present invention. The method of Figure 4 can be executed in a home network or by/at a home network entity, as illustrated in Figure 1.

As shown in Figure 4, a method according to exemplifying embodiments of the present invention, which is operable in the domain of the home network, comprises an operation (S410) of recording, upon confirmation of completion of authentication of the user equipment entity by a visited network of the user equipment entity, a time of authentication of the user equipment entity and an identifier of the visited network, operation (S420) of obtaining a request for a procedure affecting a state (status) of the user equipment entity, said request including an identifier of an originating visited network of the user equipment entity, and operation (S430) of rejecting the requested procedure, if the request is not received within a predefined time period since the recorded time of authentication of the user equipment, or if the identifier of the originating visited network in the request does not correspond to the recorded identifier of the visited network.

With reference to the scheme of Figure 1, operations S410 to S430 can be regarded to correspond to the sixth phase. Stated in other words, operations S410 to S430 can be regarded as a linking functionality of linking the recent authentication procedure with any subsequent procedure, preferably with any subsequent procedure affecting the state (status) of the user equipment entity, as described in connection with the sixth phase.

Yet, it is noted that the method of Figure 4 is inherently independent of the operations in the first to sixth phases, and could be performed without or could be combined with (performed subsequent to) the operations in the first to sixth phases of Figure 1. That is, the method of Figure 4 is applicable in a standalone fashion or as a continuation of the method of Figure 2.

As mentioned above, the above-described enhanced authentication technique, as well as the individual methods related thereto, can be implemented in any LTE/LTE-A as well as NG/5G communication system. For implementation in a LTE/LTE-A communication system, the only prerequisite would be that the home network (entity) knows which visited networks implement this enhanced authentication technique. Then, the home network (entity) can operate accordingly in order to ensure security, i.e. any visited networks that do not implement this enhanced authentication technique would then undergo enhanced scrutiny by the home network (entity).

In the following, an exemplary use case or implementation of the enhanced authentication technique according to exemplifying embodiments of the present invention is described.

For the description of the exemplary use case or implementation, implementation in a NG/5G communication system, with AUSF/ARPF acting as home network (entity), SEAF acting as visited network (entity) and UE (with USIM) acting as user equipment entity, and with adopting EPS AKA as underlying authentication mechanism, is assumed for explanatory/illustrative purpose.

Firstly, focus is directed to the concept of EPS AKA with success confirmation (EPS AKA*).

As described above, the EPS AKA* solution enhances EPS AKA with providing an authentication confirmation/success indication/message from the visited network to the home network such that the indication/message cannot be spoofed by the visited network with a reasonable probability, besides using a correctness verification parameter instead of a full expected authentication result for authenticating the UE in the visited network. The EPS AKA* solution leaves the authentication exchange between the UE and the visited network unchanged (as far as the security parameters are concerned). In particular, the EPS AKA*solution does not affect the authentication behavior of the UE, compared to EPS AKA.

Figure 5 shows a flow diagram illustrating an example of a procedure (for enabling/realizing the concept of EPS AKA with success confirmation (EPS AKA*)) according to exemplifying embodiments of the present invention.

As shown in Figure 5, the operational sequence of EPS AKA* can be as follows.

1. The SEAF in the visited network requests a new authentication vector by sending a Next Gen Authentication Information Request (NG-AIR) to the AUSF in the home network. The NG-AIR contains an identifier of the UE to be authenticated, i.e. for the authentication for which authentication information is requested.

Upon receipt of the NG-AIR, the AUSF/ARPF, particularly the AUSF, may initiate the authentication procedure for the identified UE, i.e. the further procedure as described hereinafter.

2. The AUSF/ARPF, particularly the AUSF, generates the correctness verification parameter RES-CVP. In this regard, the AUSF may translate the NG-AIR into a request to the ARPF, and the ARPF may generate the authentication vector (in the same way as for EPS AKA) and return it to the AUSF. Preferably, only one authentication vector, including RAND, AUTN and XRES, shall be returned in response to an NG-AIR. Then, the AUSF can use XRES for generation of the correctness verification parameter RES-CVP.

For generation of the correctness verification parameter RES-CVP, the AUSF may split (decompose) the parameter XRES, for example, into two equal parts XRES1 and XRES2. This may be accomplished, for example, by choosing XRES1 to be the n least significant

bits of XRES, where 2n is the length of XRES. The assumption is made here that the knowledge of XRES1 does help in guessing XRES2 (with reasonable probability/effort). This assumption is believed to be fulfilled when the expected authentication response XRES is pseudo-randomly generated, e.g. as in MILENAGE or TUAK. As long as this assumption is fulfilled, the manner of splitting (decomposing) XRES into XRES1 and XRES2 is not restricted.

The AUSF may then store XRES, at least temporarily until a protocol timer (with a predefined time period) expires.

3. The AUSF/ARPF, particularly the AUSF, then returns (i.e. provides) an authentication vector AV* (including XRESa (as RES-CVP), RAND and AUTN) in a Next Gen Authentication Information Answer (NG-AIA). The only difference between AV* and an authentication vector AV, as defined for EPS AKA, is that AV* contains only XRES1 (as RES-CVP) while AV contains the full XRES.

4. The SEAF understands from the NG-AIA that it includes AV*, not AV. This can be readily recognized by analyzing the contents of the NG-AIA, by analyzing an appropriate message header of the NG-AIA, or the like. Then, the SEAF sends (the thus obtained) RAND and AUTN (in an Authentication Request) to the UE. Thereby, the SEAF initiates the authentication procedure between the SEAF and the UE using (the thus obtained) RAND and AUTN.

5. The UE generates the authentication response RES using RAND and AUTN (from the Authentication Request).

6. The UE returns the authentication response RES (in Authentication Response), as defined for EPS AKA. Accordingly, the SEAF obtains the authentication response RES.

7. The SEAF verifies correctness of authentication of the UE using the RES. That is, the SEAF determines whether or not the UE is successfully authenticated.

For the correctness verification, the SEAF uses its knowledge about the type and/or form of the correctness verification parameter RES-CVP, as received in step 3 before. In the present case, the SEAF splits (decomposes) RES into RES1 and RES2 in the same way

as the AUSF did for generating RES-CVP from XRES, and compares RES1 with XRES1 (i.e. the RES-CVP). If they coincide, the SEAF considers the authentication successful. If not, the SEAF rejects the authentication.

8. If the authentication was completed/successful, the SEAF sends (i.e. provides) the RES, as received from the UE, in a new Next Gen Authentication Confirmation (NG-AC) message (containing an identification of the subscriber (UE)) to the AUSF, particularly the AUSF. Accordingly, the AUSF/ARPF, particularly the AUSF, obtains the authentication response RES.

Otherwise, if the authentication was not completed/successful, the SEAF aborts the authentication procedure. This may, but does not need to, be reported to the AUSF/ARPF, particularly the AUSF

9. Upon receipt thereof, the AUSF/ARPF, particularly the AUSF, may optionally process the RES. In regard, the RES or the NG-AC may be refused by the AUSF/ARPF, particularly the AUSF, when the NG-AC message was not received in response to an NG-AIA or was not received in time, i.e. within the predefined time period of the aforementioned protocol timer (e.g. within a predefined time period since the RES-CVP has been provided or the NG-AIA has been transmitted).

10. Otherwise, when the NG-AC message was received in response to an NG-AIA and was received in time, the AUSF/ARPF, particularly the AUSF, confirms completion of authentication of the UE by the SEAF. In this regard, the AUSF/ARPF, particularly the AUSF, compares the received RES with the stored XRES. If they coincide, the AUSF/ARPF, particularly the AUSF, considers the authentication successful and records the event, e.g. together with the time and the subscriber (UE) identity, e.g. in a database of successful authentications. If not, the AUSF/ARPF, particularly the AUSF, rejects the authentication.

As a result of the above-described procedure, all further operations of the home network (entity) and the visited network (entity) can be performed in view of the authentication result, i.e. whether or not authentication of the UE is confirmed (successful) or nor.

Secondly, focus is directed to the concept of linking a state/status-affecting procedure, like a location update, with an authentication result.

As described above, the linking solution basically consists in using an authentication protocol with success indication/confirmation, e.g. EAP-AKA' or EPS AKA*, and link an authentication result (from usage of that authentication protocol) to a subsequent procedure affecting a state (status) of the UE, or a request for such procedure. For example, such procedure may be an update location procedure, and the corresponding request may be a Next Generation Update Location Request (NG-ULR).

Figure 6 shows a flow diagram illustrating an example of another procedure (for enabling/realizing the concept of linking a state/status-affecting procedure with an authentication result) according to exemplifying embodiments of the present invention. In Figure 6,

As shown in Figure 6, the operational sequence of authentication linking can be as follows.

1.-3. The actual linking procedure starts upon/with confirmation of completion of authentication of the UE by a visited network (entity) thereof, i.e. the SEAF. Stated in other words, the actual linking procedure starts when a most recent successful authentication of the UE has taken place. This is illustrated in steps 1 to 3, which may be implemented as described for steps 7 to 10 (particularly steps 7, 8 and 10) of Figure 5.

The actual linking procedure is carried out in/by steps 4 to 6, as is indicated by way of a dashed box.

4. The AUSF/ARPF, particularly the AUSF, records the most recent successful authentication event, namely time of the most recent successful authentication of the UE (subscriber), e.g. time of the confirmation in step 3 or the completion verification in step 1, together with the identity of the visited network (or the visited network entity) that was involved in the authentication of the UE (subscriber).

5. The AUSF/ARPF, particularly the AUSF, receives (i.e. obtains) an update location request as an example of a request for a procedure affecting a state (status) of the UE,

e.g. in the form of a NG-ULR. This request contains an identifier of the UE (subscriber) subject to the requested update location procedure and an identifier of an originating visited network (or visited network entity) of the UE (subscriber) subject to the requested update location procedure.

6. The AUSF/ARPF, particularly the AUSF, checks how the requested update location procedure is to be processed, and processes it accordingly. Specifically, upon arrival of e.g. a new NG-ULR, the AUSF/ARPF, particularly the AUSF, checks whether there is a sufficiently recent authentication of the UE (subscriber) by the visited network (or visited network entity) originating e.g. the NG-ULR.

Such check considers time and identity aspects. Namely, it is checked whether the request is received within a predefined time period since the recorded time of the most recent authentication of the UE (subscriber), and whether the identifier of the originating visited network (or visited network entity) in the request corresponds to the recorded identifier of the visited network (or visited network entity) having conducted the most recent authentication of the UE (subscriber). The predefined time period applied in this regard may be arbitrarily set, e.g. by the AUSF/ARPF, particularly the AUSF, or any other instance of the home network.

If at least one of these conditions is not fulfilled, the AUSF/ARPF, particularly the AUSF, rejects the request, e.g. the NG-ULR, or more specifically the thus requested procedure. Otherwise, if both conditions are fulfilled, the AUSF/ARPF, particularly the AUSF, accepts the request, e.g. the NG-ULR, and initiates the thus requested procedure.

It is noted that, with this approach, the authentication procedure and the update location (e.g. NG-ULR) procedure are performed independently, but are linked or coupled through linking information in the home network (entity). In the above example, the linking information comprise time and identity of involved visited network (entity) of a most recent authentication of a (the same) UE (subscriber).

The procedure of Figure 6 is operable in a standalone fashion. Yet, it is particularly beneficial to combine the procedure of Figure 6 with the procedure of Figure 5. Namely, by obtaining an authentication result using an enhanced authentication mechanism, such as the EPS AKA* procedure of Figure 5, and linking the thus obtained authentication

result with a subsequent state/status-affecting procedure, such as with the procedure of Figure 6, advanced technical effects in the context of increasing home control in roaming situations can be achieved.

As indicated above, in case of the state-affecting procedure being an update location procedure (e.g. the corresponding request being a Next Generation Update Location Request (NG-ULR)), the concept of authentication linking may be more specifically referred to as a concept of linking location update with authentication result.

By virtue of exemplifying embodiments of the present invention, as evident from the above, enhancements in AKA-based authentication, especially for roaming situations, which can address the initially described security issues, can be enabled/realized. In a nutshell, increased home control in roaming situations can be facilitated thereby.

According to exemplifying embodiments of the present invention, increased home control in roaming situations can be achieved. This means that, for example, the home network is enabled to ascertain that a subscriber whose location is updated to a new visited network has actually been authenticated involving this visited network. Additionally, the home network may be further enabled to ascertain a minimum authentication frequency for his roaming subscribers. Stated in other words, it could be said that security mechanisms are provided which are effective to fight inter-operator fraud and misuse of international signaling networks, or that the home network is enabled to verify that his roaming subscriber is really attached to a visited network that claims it is.

In the following, an evaluation is outlined for the enhanced authentication mechanism according to exemplifying embodiments of the present invention, especially the enhanced authentication mechanism, such as the EPS AKA* procedure.

I. From a security point of view, the following aspects may for example be evaluated as follows.

I.1 The probability of spoofing the response, i.e. the authentication response RES

Assume that an SEAF wants to spoof RES in the absence of the subscriber. In the above-described exemplary use case or implementation, the SEAF has obtained XRES1 (as RES-CVP) from the AUSF, but needs to guess RES2. In EPS AKA, RES has a minimum length of 32 bits. (For the commonly used authentication algorithm set

MILENAGE, the length of RES is 64 bits.) So, RES2 has a minimum length of 16 bits. This means that the SEAF has a chance of at most 1 in 2^16 =65.000 to guess RES2 correctly.

The success probability for a fraudulent visited network is considered sufficiently low for the following reasons:

- A chance of at most 1 in 65.000 (=2^16) (1 in 4 billion = 2^32 for MILENAGE) is considered commercially unattractive.
- It would be highly suspicious to the home network if very many instances of RES2 were incorrect, while RES1 was always correct, as this would be extremely unlikely.

I.2 The case of RES1 being correct, but RES2 being incorrect

This case is deemed to be not practically relevant. Namely, the probability of this happening is determined by the length of RES1 and is considered sufficiently low for any practical purposes.

I.3 Impersonating an MME towards the home network or the UE

This scenario is deemed to be not an effective strategy for the visited network.

I.4 Key issued to SEAF before AUSF knows about authentication success

The fact that the visited network obtains the intermediate key from the home network before the home network receives the authentication success confirmation cannot be meaningfully exploited by the visited network.

II. From an efficiency point of view, the following aspects may for example be evaluated as follows.

II.1 Authentication delay

The efficiency advantage of EPS AKA over EAP-AKA' is inherited by EPS AKA* as far as authentication delay over the air interface is concerned: This is because EPS AKA*, like EPS AKA, requires only one roundtrip between the visited network and the home network. Thus, the visited network can go ahead with the Security Mode procedure etc. without having to wait for a second roundtrip of authentication with the home network. So, the efficiency over the radio interface is as good as for EPS AKA. This is particularly useful in full authentications that do not entail an Update Location procedure or any further interaction with the home network.

II.2 Computation overhead

Computation overhead of EPS AKA* is also the same as for EPS AKA and lower than for EAP-AKA'. Namely, EPS AKA*, like EPS AKA, has lower computational

complexity than EAP-AKA'. This is an advantage, in particular, to UEs (or other involved devices and entities) with restricted capabilities.

II.3 Statelessness

The AUSF is no longer stateless as in EPS AKA. It becomes stateful as in EAP-AKA'. This is a disadvantage compared to EPS AKA.

In summary, it can be said that EPS AKA* strikes a balance between improved security, compared to EPS AKA, and still better efficiency over the radio interface, compared to EAP-AKA'.

The above-described methods, procedures and functions may be implemented by respective functional elements, entities, modules, units, processors, or the like, as described below.

While in the foregoing exemplifying embodiments of the present invention are described mainly with reference to methods, procedures and functions, corresponding exemplifying embodiments of the present invention also cover respective apparatuses, entities, modules, units, network nodes and/or systems, including both software and/or hardware thereof.

Respective exemplifying embodiments of the present invention are described below referring to Figures 7 and 8, while for the sake of brevity reference is made to the detailed description of respective corresponding configurations/setups, schemes, methods and functionality, principles and operations according to Figures 1 to 6.

In Figures 7 and 8, the blocks are basically configured to perform respective methods, procedures and/or functions as described above. The entirety of blocks are basically configured to perform the methods, procedures and/or functions as described above, respectively. With respect to Figures 7 and 8, it is to be noted that the individual blocks are meant to illustrate respective functional blocks implementing a respective function, process or procedure, respectively. Such functional blocks are implementation-independent, i.e. may be implemented by means of any kind of hardware or software or combination thereof, respectively.

Further, in Figures 7 and 8, only those functional blocks are illustrated, which relate to any one of the above-described methods, procedures and/or functions. A skilled person will acknowledge the presence of any other conventional functional blocks required for an operation of respective structural arrangements, such as e.g. a power supply, a central processing unit, respective memories or the like. Among others, one or more memories are provided for storing programs or program instructions for controlling or enabling the individual functional entities or any combination thereof to operate as described herein in relation to exemplifying embodiments.

Figure 7 shows a schematic diagram illustrating an example of a structure of apparatuses according to exemplifying embodiments of the present invention.

As indicated in Figure 7, according to exemplifying embodiments of the present invention, an apparatus 700 may comprise at least one processor 710 and at least one memory 720 (and possibly also at least one interface 730), which may be operationally connected or coupled, for example by a bus 740 or the like, respectively.

The processor 710 of the apparatus 700 can be any suitable computing means, including hardware circuitry and/or software code (e.g. stored in or read from the memory 720). The processor 710 and/or the interface 730 of the apparatus 700 may also include a modem or the like to facilitate communication over a (hardwire or wireless) link, respectively. The interface 730 of the apparatus 700 may include a suitable transmitter, receiver or transceiver connected or coupled to one or more antennas, antenna units, such as antenna arrays or communication facilities or means for (hardwire or wireless) communications with the linked, coupled or connected device(s), respectively. The interface 730 of the apparatus 700 is generally configured to communicate with at least one other apparatus, device, node or entity (in particular, the interface thereof).

The memory 720 of the apparatus 700 may represent a (non-transitory/tangible) storage medium and store respective software, programs, program products, macros or applets, etc. or parts of them, which may be assumed to comprise program instructions or computer program code that, when executed by the respective processor, enables the respective electronic device or apparatus to operate in accordance with the exemplifying embodiments of the present invention. Further, the memory 720 of the apparatus 700 may

(comprise a database to) store any data, information, or the like, which is used in the operation of the apparatus.

In general terms, respective apparatuses (and/or parts thereof) may represent means for performing respective operations and/or exhibiting respective functionalities, and/or the respective devices (and/or parts thereof) may have functions for performing respective operations and/or exhibiting respective functionalities.

In view of the above, the thus illustrated apparatus 700 is suitable for use in practicing one or more of the exemplifying embodiments of the present invention, as described herein.

When in the subsequent description it is stated that the processor (or some other means) is configured to perform some function, this is to be construed to be equivalent to a description stating that a (i.e. at least one) processor or corresponding circuitry, potentially in cooperation with a computer program code stored in the memory of the respective apparatus or otherwise available (it should be appreciated that the memory may also be an external memory or provided/realized by a cloud service or the like), is configured to cause the apparatus to perform at least the thus mentioned function.

According to exemplifying embodiments of the present invention, the thus illustrated apparatus 700 may represent or realize/embody a (part of a) a home network or home network entity. Specifically, the thus illustrated apparatus 700 may be configured to perform a procedure and/or exhibit a functionality and/or implement a mechanism, as described for the home network (entity), in any one of Figures 1, 2 and 4 to 6.

Accordingly, the apparatus 700 may be caused or the apparatus 700 or its at least one processor 710 (possibly together with computer program code stored in its at least one memory 720), in a basic form, is configured to provide, for a visited network entity of a visited network of the user equipment entity, a parameter enabling verification of correctness of an authentication response from the user equipment entity, said parameter being derivable from an expected authentication response from the user equipment entity, to obtain, from the visited network entity, the authentication response from the user equipment entity as an indication of completion of authentication of the user equipment entity, and to confirm completion of authentication of the user equipment entity by the

visited network entity when the obtained authentication response corresponds to the expected authentication response.

Also, the apparatus 700 may be caused or the apparatus 700 or its at least one processor 710 (possibly together with computer program code stored in its at least one memory 720), in a basic form, is configured to record, upon confirmation of completion of authentication of the user equipment entity by a visited network of the user equipment entity, a time of authentication of the user equipment entity and an identifier of the visited network, to obtain a request for a procedure affecting a state of the user equipment entity, said request including an identifier of an originating visited network of the user equipment entity, and to reject the requested procedure, if the request is not received within a predefined time period since the recorded time of authentication of the user equipment, or if the identifier of the originating visited network in the request does not correspond to the recorded identifier of the visited network.

According to exemplifying embodiments of the present invention, the thus illustrated apparatus 700 may represent or realize/embody a (part of a) a visited network or visited network entity. Specifically, the thus illustrated apparatus 700 may be configured to perform a procedure and/or exhibit a functionality and/or implement a mechanism, as described for the visited network (entity), in any one of Figures 1, 3, 5 and 6.

Accordingly, the apparatus 700 may be caused or the apparatus 700 or its at least one processor 710 (possibly together with computer program code stored in its at least one memory 720), in a basic form, is configured to obtain, from a home network entity of a home network of the user equipment entity, a parameter enabling verification of correctness of an authentication response from the user equipment entity, said parameter being related to an expected authentication response from the user equipment entity, to obtain, from the user equipment entity, the authentication response as a result of an authentication procedure between the visited network entity and the user equipment entity, to verify correctness of the authentication response from the user equipment entity using said parameter, and to provide, to the home network entity, the authentication response from the user equipment entity as an indication of completion of authentication of the user equipment entity when correctness of the authentication response from the user equipment entity is positively verified.

As mentioned above, any apparatus according to exemplifying embodiments of the present invention may be structured by comprising respective units or means for performing corresponding operations, procedures and/or functions. For example, such units or means may be implemented/realized on the basis of an apparatus structure, as exemplified in Figure 7, i.e. by one or more processors 710, one or more memories 720, one or more interfaces 730, or any combination thereof.

Figure 8 shows a schematic diagram illustrating another example of a functional structure of apparatuses according to exemplifying embodiments of the present invention. Generally, it is noted that any such apparatus may be realized in a physical form, i.e. as or in any specified network node or entity, or in logical form, i.e. as or in any specified network function.

It is to be noted that the individual apparatuses shown in Figure 8 are inherently independent from each other but could be operable to interwork, i.e. exemplifying embodiments of the present invention cover any one of these apparatuses alone or any combination of such apparatuses (including one or more of any one of these apparatuses).

As shown in Figure 8, an apparatus 810 according to exemplifying embodiments of the present invention may comprise (at least) a unit or means 811 for providing a parameter enabling verification of correctness of an authentication response from a user equipment entity, a unit or means 812 for obtaining the authentication response from the user equipment entity as an indication of completion of authentication of the user equipment entity, and a unit or means 813 for confirming completion of authentication of the user equipment entity by the visited network entity when the obtained authentication response corresponds to an expected authentication response.

As evident from the above, the apparatus 810 may optionally also comprise a unit or means 814 for generating the parameter using the expected authentication response, and/or a unit or means 815 for refusing the authentication response, and/or a unit or means 816 for recording a time of authentication of the user equipment entity and an identifier of the visited network upon confirmation of completion of authentication of the user equipment entity, obtaining a request for a procedure affecting a state of the user equipment entity, said request including an identifier of an originating visited network of

the user equipment entity, and rejecting the requested procedure, if the request is not received within a predefined time period since the recorded time of authentication of the user equipment, or if the identifier of the originating visited network in the request does not correspond to the recorded identifier of the visited network.

As shown in Figure 8, an apparatus 820 according to exemplifying embodiments of the present invention may comprise (at least) a unit or means 821 for recording a time of authentication of a user equipment entity and an identifier of a visited network, a unit or means 822 for obtaining a request for a procedure affecting a state of the user equipment entity, said request including an identifier of an originating visited network of the user equipment entity, and a unit or means 823 for rejecting the requested procedure, if the request is not received within a predefined time period since the recorded time of authentication of the user equipment, or if the identifier of the originating visited network in the request does not correspond to the recorded identifier of the visited network.

As evident from the above, the apparatus 820 may optionally also comprise a unit or means 824 for providing a parameter enabling verification of correctness of an authentication response from the user equipment entity, obtaining the authentication response from the user equipment entity as an indication of completion of authentication of the user equipment entity, and confirming completion of authentication of the user equipment entity by the visited network entity when the obtained authentication response corresponds to the expected authentication response.

As shown in Figure 8, an apparatus 830 according to exemplifying embodiments of the present invention may comprise (at least) a unit or means 831 for obtaining a parameter enabling verification of correctness of an authentication response from a user equipment entity, a unit or means 832 for obtaining the authentication response as a result of an authentication procedure between the visited network entity and the user equipment entity, a unit or means 833 for verifying correctness of the authentication response from the user equipment entity using said parameter, and a unit or means 834 for providing the authentication response from the user equipment entity as an indication of completion of authentication of the user equipment entity when correctness of the authentication response from the user equipment entity is positively verified.

As evident from the above, the apparatus 830 may optionally also comprise a unit or means 834 for obtaining a random challenge and an authentication token dedicated for authentication of the user equipment entity, and initiating the authentication procedure using the obtained random challenge and authentication token.

For further details regarding the operability/functionality of the individual apparatuses (or units/means thereof) according to exemplifying embodiments of the present invention, reference is made to the above description in connection with any one of Figures 1 to 6, respectively.

According to exemplifying embodiments of the present invention, any one of the (at least one) processor, the (at least one) memory and the (at least one) interface, as well as any one of the illustrated units/means, may be implemented as individual modules, chips, chipsets, circuitries or the like, or one or more of them can be implemented as a common module, chip, chipset, circuitry or the like, respectively.

According to exemplifying embodiments of the present invention, a system may comprise any conceivable combination of the thus depicted apparatuses and other network elements or functional entities, which are configured to cooperate as described above.

In general, it is to be noted that respective functional blocks or elements according to above-described aspects can be implemented by any known means, either in hardware and/or software, respectively, if it is only adapted to perform the described functions of the respective parts. The mentioned method steps can be realized in individual functional blocks or by individual devices, or one or more of the method steps can be realized in a single functional block or by a single device.

Generally, any method step is suitable to be implemented as software or by hardware without changing the idea of the present invention. Such software may be software code independent and can be specified using any known or future developed programming language, such as e.g. Java, C++, C, and Assembler, as long as the functionality defined by the method steps is preserved. Such hardware may be hardware type independent and can be implemented using any known or future developed hardware technology or any hybrids of these, such as MOS (Metal Oxide Semiconductor), CMOS (Complementary MOS), BiMOS (Bipolar MOS), BiCMOS (Bipolar CMOS), ECL (Emitter Coupled Logic),

TTL (Transistor-Transistor Logic), etc., using for example ASIC (Application Specific IC (Integrated Circuit)) components, FPGA (Field-programmable Gate Arrays) components, CPLD (Complex Programmable Logic Device) components or DSP (Digital Signal Processor) components. A device/apparatus may be represented by a semiconductor chip, a chipset, or a (hardware) module comprising such chip or chipset; this, however, does not exclude the possibility that a functionality of a device/apparatus or module, instead of being hardware implemented, be implemented as software in a (software) module such as a computer program or a computer program product comprising executable software code portions for execution/being run on a processor. A device may be regarded as a device/apparatus or as an assembly of more than one device/apparatus, whether functionally in cooperation with each other or functionally independently of each other but in a same device housing, for example.

Apparatuses and/or units/means or parts thereof can be implemented as individual devices, but this does not exclude that they may be implemented in a distributed fashion throughout the system, as long as the functionality of the device is preserved. Such and similar principles are to be considered as known to a skilled person.

Software in the sense of the present description comprises software code as such comprising code means or portions or a computer program or a computer program product for performing the respective functions, as well as software (or a computer program or a computer program product) embodied on a tangible medium such as a computer-readable (storage) medium having stored thereon a respective data structure or code means/portions or embodied in a signal or in a chip, potentially during processing thereof.

The present invention also covers any conceivable combination of method steps and operations described above, and any conceivable combination of nodes, apparatuses, modules or elements described above, as long as the above-described concepts of methodology and structural arrangement are applicable.

In view of the above, there are provided measures for enhancements in AKA-based authentication, especially for roaming situations. Such measures exemplarily comprise provision of a parameter enabling verification of correctness of an authentication response of a user equipment from a home network to a visited network of the user equipment, said

parameter being derivable from an expected authentication response, verification of correctness of the authentication response of the user equipment entity using said parameter in the visited network, provision of the authentication response of the user equipment from the visited network to the home network as an indication of completion of authentication of the user equipment when correctness of the authentication response of the user equipment is positively verified, and confirmation of completion of authentication of the user equipment by the visited network in the home network when the provided authentication response corresponds to the expected authentication response.

Even though the invention is described above with reference to the examples according to the accompanying drawings, it is to be understood that the invention is not restricted thereto. Rather, it is apparent to those skilled in the art that the present invention can be modified in many ways without departing from the scope of the inventive idea as disclosed herein.

List of acronyms and abbreviations

3GPP	3rd Generation Partnership Project
AKA	Authentication and Key Agreement
ARPF	Authentication Credential Repository and Processing Function
AUSF	Authentication Server Function
AUTN	Authentication Token
AV	Authentication Vector
EAP	Extensible Authentication Protocol
EPS	Evolved Packet System
HSS	Home Subscriber Server
LTE	Long Term Evolution
LTE-A	Long Term Evolution Advanced
MME	Mobility Management Entity
NG	Next Generation
NG-AC	Next Generation Authentication Confirmation
NG-AIA	Next Generation Authentication Information Answer
NG-AIR	Next Generation Authentication Information Request
NG-ULR	Next Generation Update Location Request
RAND	Random Challenge

RES	Authentication Response
RES-CVP	Authentication Response Correctness Verification Parameter
REQ	Authentication Request
SEAF	Security Anchor Function
UE	User Equipment
USIM	Universal Subscriber Identity Module
XRES	Expected Authentication Response

Claims

1. A method of a home network entity of a home network of a user equipment entity, the method comprising:

providing, for a visited network entity of a visited network of the user equipment entity, a parameter enabling verification of correctness of an authentication response from the user equipment entity, said parameter being derivable from an expected authentication response from the user equipment entity,

obtaining, from the visited network entity, the authentication response from the user equipment entity as an indication of completion of authentication of the user equipment entity, and

confirming completion of authentication of the user equipment entity by the visited network entity when the obtained authentication response corresponds to the expected authentication response.

2. The method according to claim 1, wherein

said parameter is generated using the expected authentication response, and/or

said parameter is constructed such that the expected authentication response is not derivable from said parameter.

3. The method according to claim 1 or 2, wherein said parameter is generated by one of

decomposing the expected authentication response, and adopting a decomposed part of the expected authentication response as said parameter, and

calculating a hash value from the expected authentication response and a random challenge dedicated for authentication of the user equipment entity, and adopting the calculated hash value as said parameter.

4. The method according to any one of claims 1 to 3, wherein

said parameter is provided by or in an authentication vector.

5. The method according to any one of claims 1 to 4, further comprising:

transmitting said parameter in an authentication information answer in response to an authentication information request from the visited network entity, and

receiving the authentication response in an authentication confirmation in response to the authentication information answer.

6. The method according to claim 5, further comprising:

refusing the authentication response, if the authentication response is not in response to the authentication information answer, or if the authentication response is not received within a predefined time period since providing said parameter or transmitting the authentication information answer.

7. The method according to any one of claims 1 to 6, further comprising:

initiating the method in response to an authentication information request for the user equipment entity from the visited network entity.

8. The method according to any one of claims 1 to 7, further comprising:

recording a time of authentication of the user equipment entity and an identifier of the visited network upon confirmation of completion of authentication of the user equipment entity,

obtaining a request for a procedure affecting a state of the user equipment entity, said request including an identifier of an originating visited network of the user equipment entity, and

rejecting the requested procedure, if the request is not received within a predefined time period since the recorded time of authentication of the user equipment, or if the identifier of the originating visited network in the request does not correspond to the recorded identifier of the visited network.

9. The method according to claim 8, wherein

the requested procedure comprises an update location procedure for the user equipment entity, and/or

the request comprises an update location request for the user equipment entity.

10. A method of a home network entity of a home network of a user equipment entity, the method comprising:

recording, upon confirmation of completion of authentication of the user equipment entity by a visited network of the user equipment entity, a time of authentication of the user equipment entity and an identifier of the visited network,

obtaining a request for a procedure affecting a state of the user equipment entity, said request including an identifier of an originating visited network of the user equipment entity, and

rejecting the requested procedure, if the request is not received within a predefined time period since the recorded time of authentication of the user equipment, or if the identifier of the originating visited network in the request does not correspond to the recorded identifier of the visited network.

11. The method according to claim 10, wherein

the requested procedure comprises an update location procedure for the user equipment entity, and/or

the request comprises an update location request for the user equipment entity.

12. The method according to claim 10 or 11, further comprising:

providing, for a visited network entity of the visited network of the user equipment entity, a parameter enabling verification of correctness of an authentication response from the user equipment entity, said parameter being derivable from an expected authentication response from the user equipment entity,

obtaining, from the visited network entity, the authentication response from the user equipment entity as an indication of completion of authentication of the user equipment entity, and

confirming completion of authentication of the user equipment entity by the visited network entity when the obtained authentication response corresponds to the expected authentication response.

13. The method according to any one of claims 1 to 12, wherein

authentication of the user equipment entity is performed using an EPS AKA or EAP AKA' mechanism.

14. The method according to any one of claims 1 to 13, wherein

the home network and the visited network belong to a NG or 5G communication system, and/or

the home network entity comprises or is comprised by at least one of an Authentication Server Function, AUSF, and an Authentication Credential Repository and Processing Function, APRF, and/or

the visited network entity comprises or is comprised by a Security Anchor Function, SEAF.

15. The method according to any one of claims 1 to 13, wherein

the home network and the visited network belong to a LTE or LTE-A communication system, and/or

the home network entity comprises or is comprised by a Home Subscriber Server, HSS, and/or

the visited network entity comprises or is comprised by a Mobility Management Entity, MME.

16. A method of a visited network entity of a visited network of a user equipment entity, the method comprising:

obtaining, from a home network entity of a home network of the user equipment entity, a parameter enabling verification of correctness of an authentication response from the user equipment entity, said parameter being related to an expected authentication response from the user equipment entity,

obtaining, from the user equipment entity, the authentication response as a result of an authentication procedure between the visited network entity and the user equipment entity,

verifying correctness of the authentication response from the user equipment entity using said parameter, and

providing, to the home network entity, the authentication response from the user equipment entity as an indication of completion of authentication of the user equipment entity when correctness of the authentication response from the user equipment entity is positively verified.

17. The method according to claim 16, wherein

said parameter is constructed such that said parameter is derivable from the expected authentication response, but the expected authentication response is not derivable from said parameter, and/or

said parameter is one of

a decomposed part of the expected authentication response, and

a hash value of the expected authentication response and a random challenge dedicated for authentication of the user equipment entity.

18. The method according to claim 16 or 17, wherein, when said parameter is a decomposed part of the expected authentication response, said verifying comprising:

decomposing the obtained authentication response from the user equipment entity in an equivalent manner as the decomposition of the expected authentication response, and

comparing a decomposed part of the obtained authentication response from the user equipment entity with the decomposed part of the expected authentication response serving as said parameter.

19. The method according to claim 16 or 17, wherein, when said parameter is a hash value of the expected authentication response and a random challenge dedicated for authentication of the user equipment entity, said verifying comprising:

calculating a hash value from the obtained authentication response from the user equipment entity and the random challenge, and

comparing the calculated hash value with the hash value serving as said parameter.

20. The method according to any one of claims 16 to 19, further comprising:

obtaining, from the home network entity, a random challenge and an authentication token dedicated for authentication of the user equipment entity, and

initiating the authentication procedure using the obtained random challenge and authentication token.

21. The method according to any one of claims 16 to 20, wherein

said parameter is obtained by or in an authentication vector.

22. The method according to any one of claims 16 to 21, further comprising:

transmitting an authentication information request for the user equipment entity to the home network entity,

receiving said parameter in an authentication information answer in response to the authentication information request to the home network entity, and

transmitting the authentication response in an authentication confirmation in response to the authentication information answer.

23. The method according to any one of claims 16 to 22, wherein

authentication of the user equipment entity is performed using an EPS AKA or EAP AKA' mechanism.

24. The method according to any one of claims 16 to 23, wherein

the home network and the visited network belong to a NG or 5G communication system, and/or

the home network entity comprises or is comprised by at least one of an Authentication Server Function, AUSF, and an Authentication Credential Repository and Processing Function, APRF, and/or

the visited network entity comprises or is comprised by a Security Anchor Function, SEAF.

25. The method according to any one of claims 16 to 23, wherein

the home network and the visited network belong to a LTE or LTE-A communication system, and/or

the home network entity comprises or is comprised by a Home Subscriber Server, HSS, and/or

the visited network entity comprises or is comprised by a Mobility Management Entity, MME.

26. An apparatus of a home network entity of a home network of a user equipment entity, comprising

at least one processor and at least one memory including a computer program code, wherein the at least one memory and the computer program code are configured, with the at least one processor, to cause the apparatus to perform at least

the following:

providing, for a visited network entity of a visited network of the user equipment entity, a parameter enabling verification of correctness of an authentication response from the user equipment entity, said parameter being derivable from an expected authentication response from the user equipment entity,

obtaining, from the visited network entity, the authentication response from the user equipment entity as an indication of completion of authentication of the user equipment entity, and

confirming completion of authentication of the user equipment entity by the visited network entity when the obtained authentication response corresponds to the expected authentication response.

27. The apparatus according to claim 26, wherein

said parameter is generated using the expected authentication response, and/or

said parameter is constructed such that the expected authentication response is not derivable from said parameter.

28. The apparatus according to claim 26 or 27, wherein said parameter is generated by one of

decomposing the expected authentication response, and adopting a decomposed part of the expected authentication response as said parameter, and

calculating a hash value from the expected authentication response and a random challenge dedicated for authentication of the user equipment entity, and adopting the calculated hash value as said parameter.

29. The apparatus according to any one of claims 26 to 29, wherein

said parameter is provided by or in an authentication vector.

30. The apparatus according to any one of claims 26 to 29, wherein the at least one memory and the computer program code are configured, with the at least one processor, to cause the apparatus to perform:

transmitting said parameter in an authentication information answer in response to an authentication information request from the visited network entity, and

receiving the authentication response in an authentication confirmation in response to the authentication information answer.

31. The apparatus according to claim 30, wherein the at least one memory and the computer program code are configured, with the at least one processor, to cause the apparatus to perform:

refusing the authentication response, if the authentication response is not in response to the authentication information answer, or if the authentication response is not received within a predefined time period since providing said parameter or transmitting the authentication information answer.

32. The apparatus according to any one of claims 26 to 31, wherein the at least one memory and the computer program code are configured, with the at least one processor, to cause the apparatus to perform:

initiating the operation of the apparatus in response to an authentication information request for the user equipment entity from the visited network entity.

33. The apparatus according to any one of claims 26 to 32, wherein the at least one memory and the computer program code are configured, with the at least one processor, to cause the apparatus to perform:

recording a time of authentication of the user equipment entity and an identifier of the visited network upon confirmation of completion of authentication of the user equipment entity,

obtaining a request for a procedure affecting a state of the user equipment entity, said request including an identifier of an originating visited network of the user equipment entity, and

rejecting the requested procedure, if the request is not received within a predefined time period since the recorded time of authentication of the user equipment, or if the identifier of the originating visited network in the request does not correspond to the recorded identifier of the visited network.

34. The apparatus according to claim 33, wherein

the requested procedure comprises an update location procedure for the user equipment entity, and/or

the request comprises an update location request for the user equipment entity.

35. An apparatus of a home network entity of a home network of a user equipment entity, comprising

at least one processor and at least one memory including a computer program code, wherein the at least one memory and the computer program code are configured, with the at least one processor, to cause the apparatus to perform at least the following:

recording, upon confirmation of completion of authentication of the user equipment entity by a visited network of the user equipment entity, a time of authentication of the user equipment entity and an identifier of the visited network,

obtaining a request for a procedure affecting a state of the user equipment entity, said request including an identifier of an originating visited network of the user equipment entity, and

rejecting the requested procedure, if the request is not received within a predefined time period since the recorded time of authentication of the user equipment, or if the identifier of the originating visited network in the request does not correspond to the recorded identifier of the visited network.

36. The apparatus according to claim 35, wherein

the requested procedure comprises an update location procedure for the user equipment entity, and/or

the request comprises an update location request for the user equipment entity.

37. The apparatus according to claim 35 or 36, wherein the at least one memory and the computer program code are configured, with the at least one processor, to cause the apparatus to perform:

providing, for a visited network entity of the visited network of the user equipment entity, a parameter enabling verification of correctness of an authentication response from the user equipment entity, said parameter being derivable from an expected authentication response from the user equipment entity,

obtaining, from the visited network entity, the authentication response from the user equipment entity as an indication of completion of authentication of the user equipment entity, and

confirming completion of authentication of the user equipment entity by the visited network entity when the obtained authentication response corresponds to the expected authentication response.

38. The apparatus according to any one of claims 26 to 37, wherein

authentication of the user equipment entity is performed using an EPS AKA or EAP AKA' mechanism.

39. The apparatus according to any one of claims 26 to 38, wherein

the home network and the visited network belong to a NG or 5G communication system, and/or

the home network entity comprises or is comprised by at least one of an Authentication Server Function, AUSF, and an Authentication Credential Repository and Processing Function, APRF, and/or

the visited network entity comprises or is comprised by a Security Anchor Function, SEAF.

40. The apparatus according to any one of claims 26 to 38, wherein

the home network and the visited network belong to a LTE or LTE-A communication system, and/or

the home network entity comprises or is comprised by a Home Subscriber Server, HSS, and/or

the visited network entity comprises or is comprised by a Mobility Management Entity, MME.

41. An apparatus of a visited network entity of a visited network of a user equipment entity, comprising

at least one processor and at least one memory including a computer program code, wherein the at least one memory and the computer program code are configured, with the at least one processor, to cause the apparatus to perform at least the following:

obtaining, from a home network entity of a home network of the user equipment entity, a parameter enabling verification of correctness of an authentication response

from the user equipment entity, said parameter being related to an expected authentication response from the user equipment entity,

obtaining, from the user equipment entity, the authentication response as a result of an authentication procedure between the visited network entity and the user equipment entity,

verifying correctness of the authentication response from the user equipment entity using said parameter, and

providing, to the home network entity, the authentication response from the user equipment entity as an indication of completion of authentication of the user equipment entity when correctness of the authentication response from the user equipment entity is positively verified.

42. The apparatus according to claim 41, wherein

said parameter is constructed such that said parameter is derivable from the expected authentication response, but the expected authentication response is not derivable from said parameter, and/or

said parameter is one of

a decomposed part of the expected authentication response, and

a hash value of the expected authentication response and a random challenge dedicated for authentication of the user equipment entity.

43. The apparatus according to claim 41 or 42, wherein, when said parameter is a decomposed part of the expected authentication response, said verifying comprising:

decomposing the obtained authentication response from the user equipment entity in an equivalent manner as the decomposition of the expected authentication response, and

comparing a decomposed part of the obtained authentication response from the user equipment entity with the decomposed part of the expected authentication response serving as said parameter.

44. The apparatus according to claim 41 or 42, wherein, when said parameter is a hash value of the expected authentication response and a random challenge dedicated for authentication of the user equipment entity, said verifying comprising:

calculating a hash value from the obtained authentication response from the user equipment entity and the random challenge, and

comparing the calculated hash value with the hash value serving as said parameter.

45. The apparatus according to any one of claims 41 to 44, wherein the at least one memory and the computer program code are configured, with the at least one processor, to cause the apparatus to perform:

obtaining, from the home network entity, a random challenge and an authentication token dedicated for authentication of the user equipment entity, and

initiating the authentication procedure using the obtained random challenge and authentication token.

46. The apparatus according to any one of claims 41 to 45, wherein

said parameter is obtained by or in an authentication vector.

47. The apparatus according to any one of claims 41 to 46, wherein the at least one memory and the computer program code are configured, with the at least one processor, to cause the apparatus to perform:

transmitting an authentication information request for the user equipment entity to the home network entity,

receiving said parameter in an authentication information answer in response to the authentication information request to the home network entity, and

transmitting the authentication response in an authentication confirmation in response to the authentication information answer.

48. The apparatus according to any one of claims 41 to 47, wherein

authentication of the user equipment entity is performed using an EPS AKA or EAP AKA' mechanism.

49. The apparatus according to any one of claims 41 to 48, wherein

the home network and the visited network belong to a NG or 5G communication system, and/or

the home network entity comprises or is comprised by at least one of an Authentication Server Function, AUSF, and an Authentication Credential Repository and Processing Function, APRF, and/or

the visited network entity comprises or is comprised by a Security Anchor Function, SEAF.

50. The apparatus according to any one of claims 41 to 48, wherein

the home network and the visited network belong to a LTE or LTE-A communication system, and/or

the home network entity comprises or is comprised by a Home Subscriber Server, HSS, and/or

the visited network entity comprises or is comprised by a Mobility Management Entity, MME.

51. A computer program product comprising computer program code which, when the computer program code is executed on a computer, is configured to cause the computer to carry out the method according to any one of claims 1 to 15 or any one of claims 16 to 25.

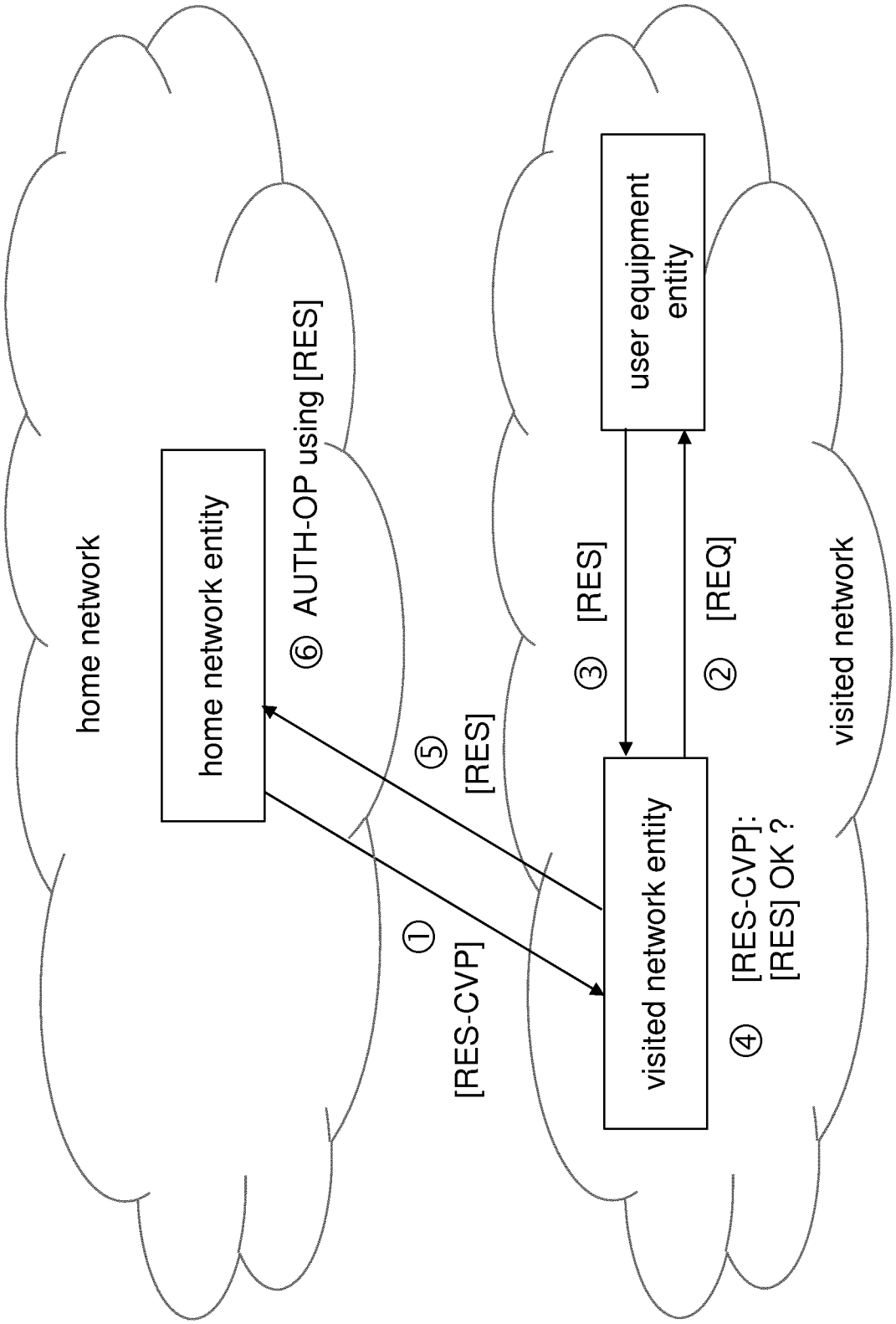
home network
home network entity
⑥ AUTH-OP using [RES]
⑤ [RES]
① [RES-CVP]
visited network
user equipment entity
③ [RES]
② [REQ]
visited network entity
④ [RES-CVP]: [RES] OK ?

Figure 1

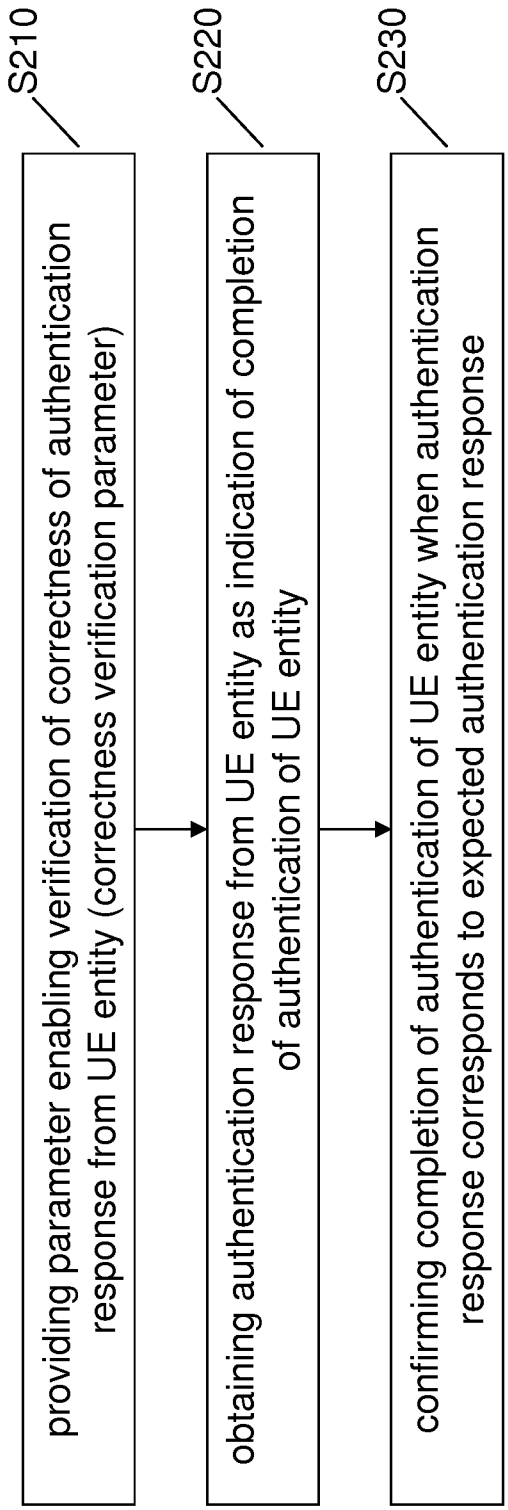
S210
providing parameter enabling verification of correctness of authentication response from UE entity (correctness verification parameter)
S220
obtaining authentication response from UE entity as indication of completion of authentication of UE entity
S230
confirming completion of authentication of UE entity when authentication response corresponds to expected authentication response

Figure 2

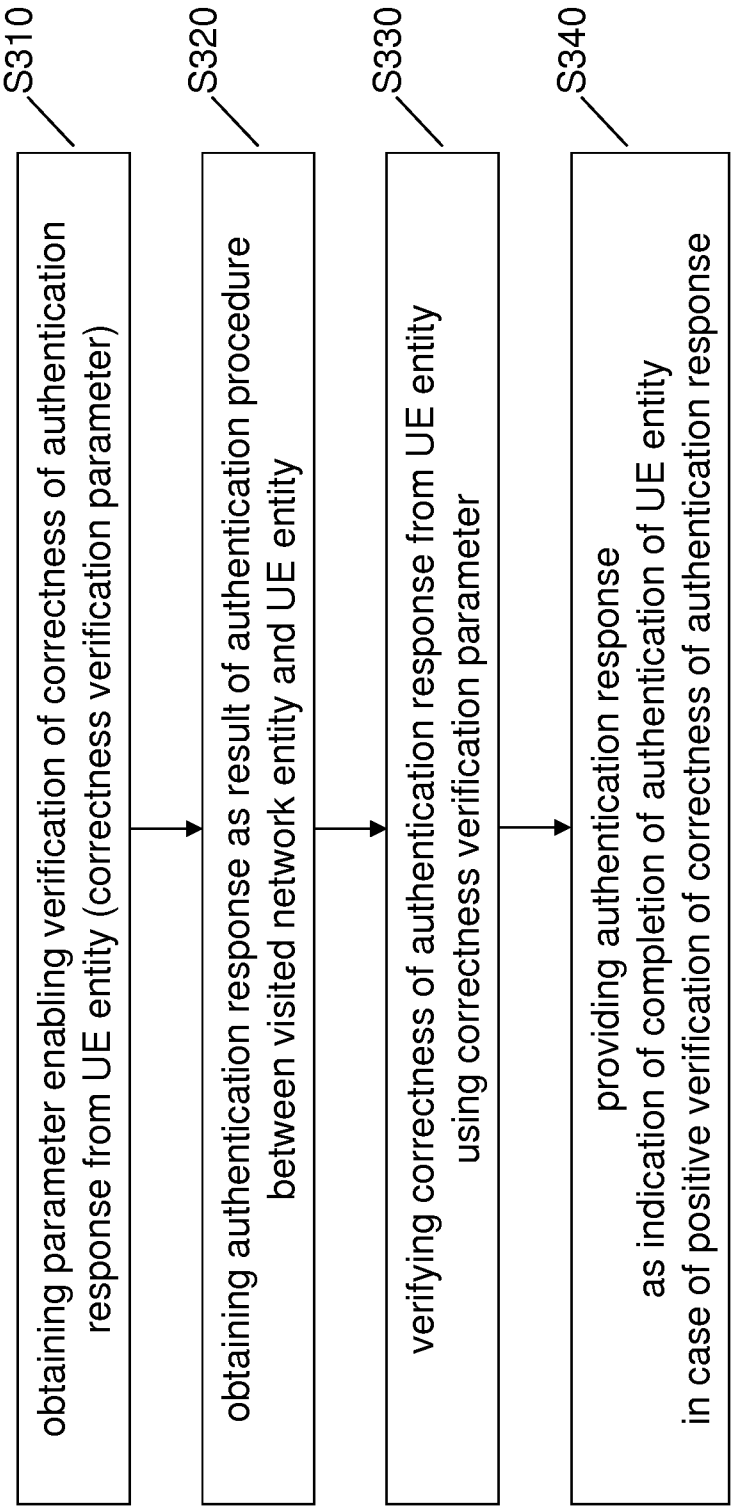
S310
obtaining parameter enabling verification of correctness of authentication response from UE entity (correctness verification parameter)
S320
obtaining authentication response as result of authentication procedure between visited network entity and UE entity
S330
verifying correctness of authentication response from UE entity using correctness verification parameter
S340
providing authentication response as indication of completion of authentication of UE entity in case of positive verification of correctness of authentication response

Figure 3

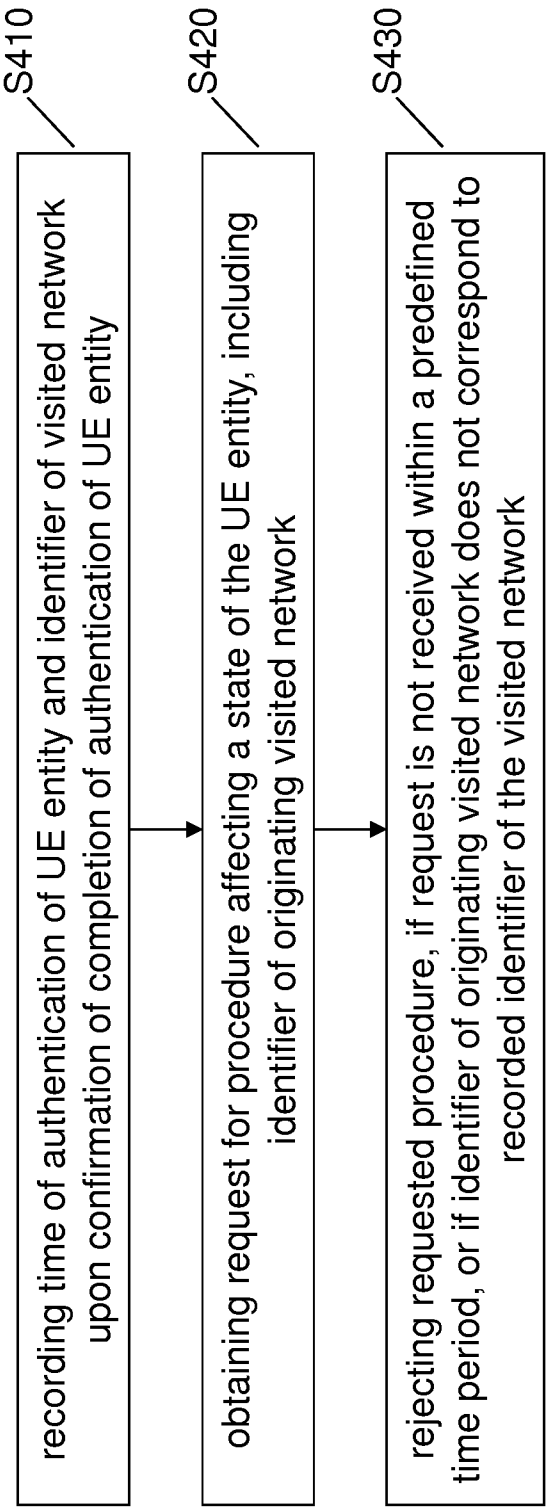
S410
recording time of authentication of UE entity and identifier of visited network upon confirmation of completion of authentication of UE entity
S420
obtaining request for procedure affecting a state of the UE entity, including identifier of originating visited network
S430
rejecting requested procedure, if request is not received within a predefined time period, or if identifier of originating visited network does not correspond to recorded identifier of the visited network

Figure 4

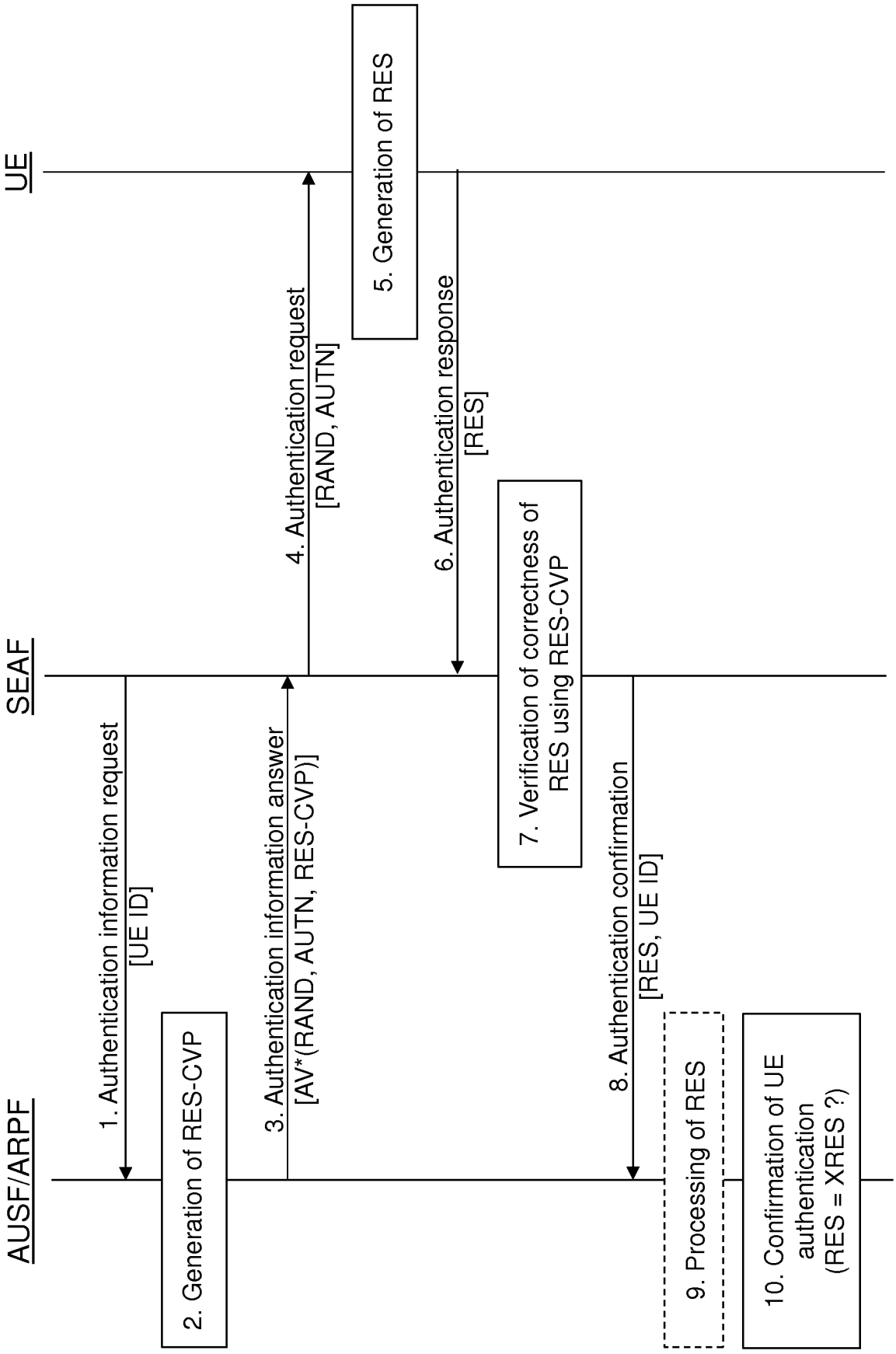
UE
SEAF
AUSF/ARPF
1. Authentication information request
[UE ID]
2. Generation of RES-CVP
3. Authentication information answer
[AV*(RAND, AUTN, RES-CVP)]
4. Authentication request
[RAND, AUTN]
5. Generation of RES
6. Authentication response
[RES]
7. Verification of correctness of RES using RES-CVP
8. Authentication confirmation
[RES, UE ID]
9. Processing of RES
10. Confirmation of UE authentication
(RES = XRES ?)

Figure 5

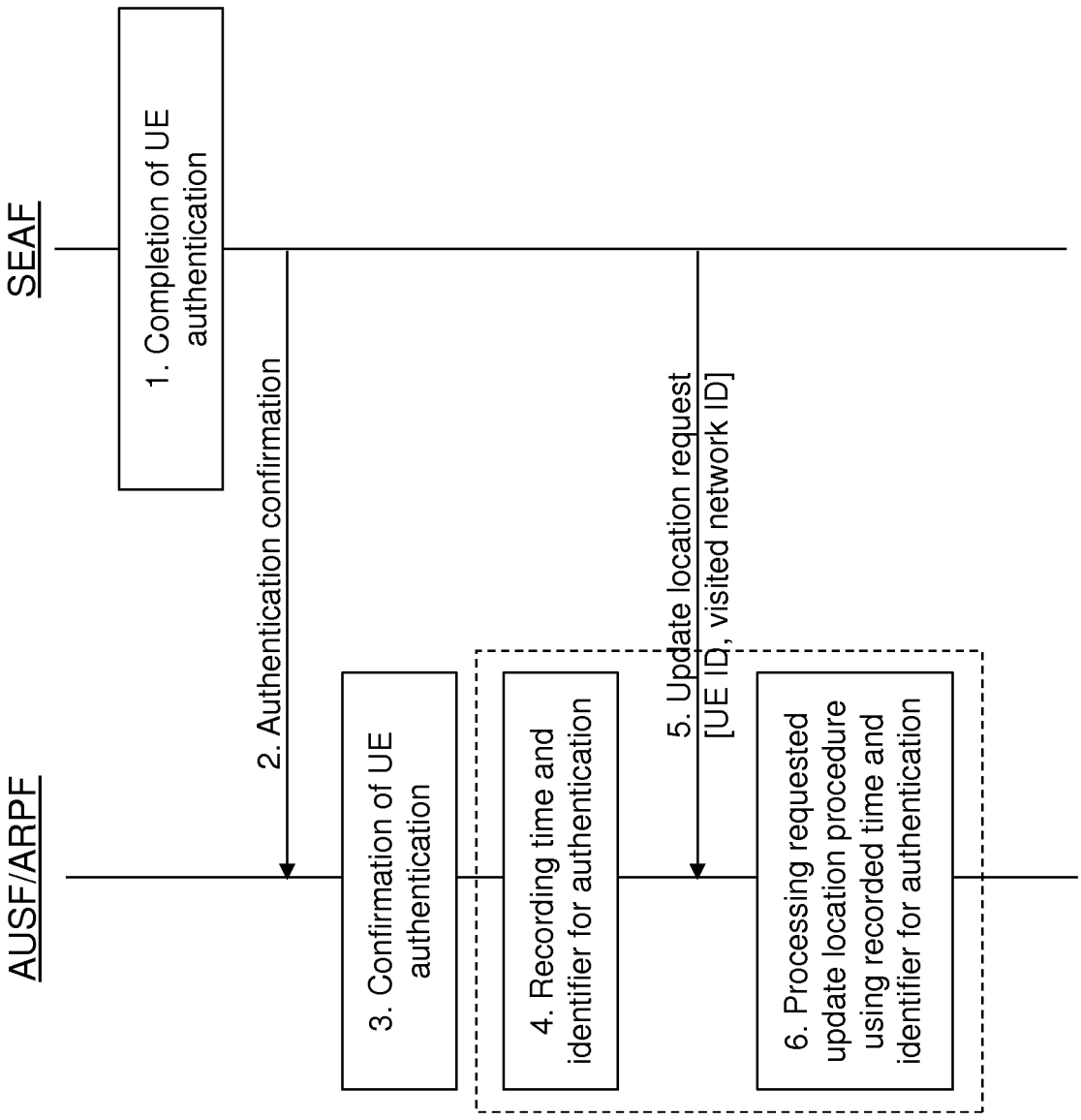
SEAF
AUSF/ARPF
1. Completion of UE authentication
2. Authentication confirmation
3. Confirmation of UE authentication
4. Recording time and identifier for authentication
5. Update location request [UE ID, visited network ID]
6. Processing requested update location procedure using recorded time and identifier for authentication

Figure 6

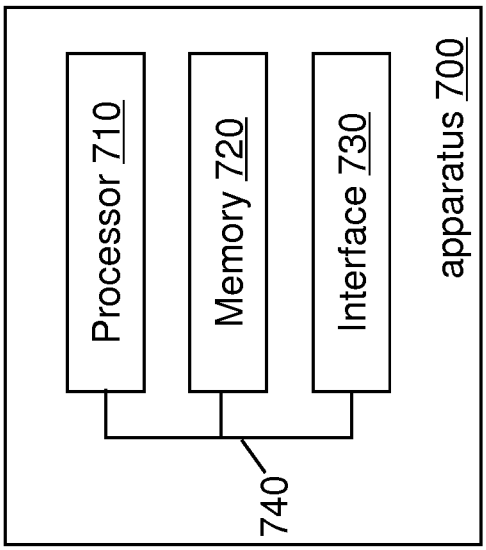

Figure 7

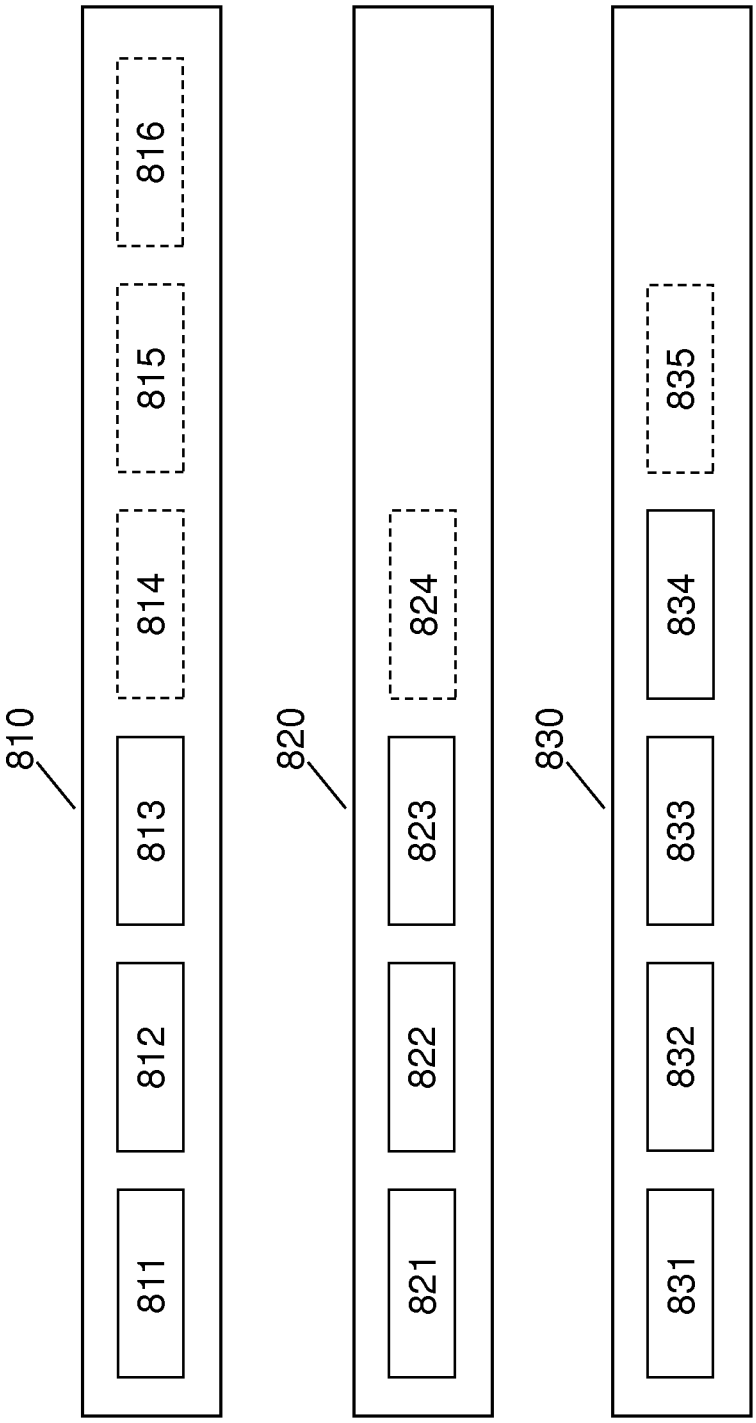
810
811
812
813
814
815
816
820
821
822
823
824
830
831
832
833
834
835

Figure 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/076203

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

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

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 practicable, search terms used)

EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 512 307 A1 (ERICSSON TELEFON AB L M [SE]) 9 March 2005 (2005-03-09) paragraph [0047] - paragraph [0063]; figures 4,5	1-51

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 June 2017	29/06/2017

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	Raposo Pires, João

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2016/076203

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1512307 A1	09-03-2005	AT 491315 T	15-12-2010
		AU 2003230490 A1	31-12-2003
		CN 1659922 A	24-08-2005
		EP 1512307 A1	09-03-2005
		HK 1080246 A1	30-04-2009
		JP 4546240 B2	15-09-2010
		JP 2005530429 A	06-10-2005
		US 2003233546 A1	18-12-2003
		WO 03107712 A1	24-12-2003