(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 169 043 B9**

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

(15) Correction information:
Corrected version no 1 (W1 B1)
Corrections, see
Claims EN 4

(48) Corrigendum issued on:
22.01.2025 Bulletin 2025/04

(45) Date of publication and mention of the grant of the patent:
30.10.2024 Bulletin 2024/44

(21) Application number: **16305322.6**

(22) Date of filing: **22.03.2016**

(51) International Patent Classification (IPC):
H04W 12/06 *(2021.01)* ***H04W 8/08*** *(2009.01)*
H04W 12/062 *(2021.01)* ***H04L 9/40*** *(2022.01)*
H04W 84/12 *(2009.01)*

(52) Cooperative Patent Classification (CPC):
H04L 63/0876; H04W 12/062; H04W 8/082; H04W 84/12

(54) **SUPPORT OF IMEI CHECKING FOR WLAN ACCESS TO A PACKET CORE OF A MOBILE NETWORK**

UNTERSTÜTZUNG VON IMEI-PRÜFUNG FÜR WLAN-ZUGRIFF AUF EINEN PAKETKERN EINES MOBILEN NETZWERKS

SUPPORT DE VÉRIFICATION D'IMEI POUR UN ACCÈS WLAN À UN NOYAU DE PAQUETS D'UN RÉSEAU MOBILE

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **11.11.2015 EP 15306791**

(43) Date of publication of application:
17.05.2017 Bulletin 2017/20

(73) Proprietor: **Alcatel Lucent**
91620 Nozay (FR)

(72) Inventors:
- **DREVON, Nicolas**
  91620 NOZAY (FR)
- **THIEBAUT, Laurent**
  91620 NOZAY (FR)
- **LANDAIS, Bruno**
  22304 LANNION (FR)

(74) Representative: **Page White Farrer**
Bedford House
21a John Street
London WC1N 2BF (GB)

(56) References cited:
WO-A1-2014/117811 WO-A2-2010/013914
US-A1- 2014 165 149

- **"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses (Release 13)", 17 September 2015 (2015-09-17), XP051071779, Retrieved from the Internet <URL:http://www.3gpp.org/ftp/tsg_sa/WG2_Arch/Latest_SA2_Specs/DRAFT_INTERIM/Archive/> [retrieved on 20150917]**

EP 3 169 043 B9

Description

[0001] The present invention generally relates to mobile communication networks and systems.

[0002] Descriptions of mobile networks and systems can be found in the literature, such as in particular in Technical Specifications published by standardization bodies such as for example 3GPP (3rd Generation Partnership Project).

[0003] An example of 3GPP mobile system is EPS (Evolved Packet System). An EPS network comprises a Core Network called EPC (Evolved Packet Core) that can be accessed not only by 3GPP access, but also by non-3GPP access, such as in particular WLAN access will be considered more particularly in the following. WLAN access to EPC is specified in particular in 3GPP TS 23.402, and includes Trusted WLAN access and Untrusted WLAN access. An example of non-roaming architecture for 3GPP and Non 3GPP (Trusted or Untrusted) access to EPC is recalled in figure 1 taken from 3GPP TS 23.402. An example of roaming architecture for 3GPP and Non 3GPP (Trusted or Untrusted) access to EPC is recalled in figure 2 taken from 3GPP TS 23.402.

[0004] In a system such as EPS for example, a UE may connect to various external networks (referred to as Packet Data Network PDN, an example being an operator's IMS network), via EPC providing connectivity (referred to as PDN connectivity) services. User authentication and authorization procedures are generally performed before granting access and providing connectivity services at establishment of a PDN connection or EPC session.

[0005] Untrusted WLAN access to EPC involves entities such as ePDG (evolved Packet Data Gateway) and 3GPP AAA Server (and 3GPP AAA Proxy in case of rooming), and interfaces such as SWa interface between WLAN AN (WLAN Access Network) and 3GPP AAA Server(or between WLAN AN and 3GPP AAA Proxy in case of roaming), and SWm interface between ePDG and 3GPP AAA Server (or between ePDG and 3GPP AAA Proxy in case of roaming), as specified in particular by 3GPP TS 23.402. Authentication and authorization procedures and protocols for these procedures are specified in particular in 3GPP TS 33.402 and 3GPP TS 29.273.

[0006] Trusted WLAN access to EPC involves entities such as TWAN (Trusted WLAN Access Network) and 3GPP AAA Server (and 3GPP AAA Proxy in case of rooming), and interfaces such as STa interface between TWAN and 3GPP AAA Server (or between TWAN and 3GPP AAA Proxy in case of roaming), as specified in particular by 3GPP TS 23.402 and 3GPP TS 29.273. Authentication and authorization procedures and protocols for these procedures are specified in particular in 3GPP TS 33.402 and 3GPP TS 29.273.

[0007] In such systems, an IMEI (International Mobile Equipment Identity) has been defined for mobile equipment identification purpose. As specified in particular by 3GPP TS 23.002, an equipment may be classified as white-listed, grey-listed or black-listed or may be unclassified. Such lists are specified in particular in 3GPP TS 22.016. The white list is composed of all number series of equipment identities that are permitted for use. The black list contains all equipment identities that belong to equipment that need to be barred. Besides the black and white list, administrations have the possibility to use a grey list. Equipments on the grey list are not barred (unless on the black list or not on the white list), but are tracked by the network (for evaluation or other purposes).

[0008] IMEI checking procedures may be performed, whereby a mobile equipment (or UE) may provide its IMEI upon request, and the network may check the status of this IMEI with the EIR (Equipment Identity register).

[0009] As recognized by the inventors, and as will be explained with more details later, there is a need to enhance IMEI checking in such systems, in particular for WLAN access (Trusted or Untrusted) to EPC.

[0010] Embodiments of the present invention in particular address such needs.

[0011] WO2010013914 describes a technique for permitting a UE to conditionally access an EPC network, when the UE is requesting the access to the EPC network using a non-3GPP access network.

- There is hereby provided a 3GPP AAA server according to claim 1, a 3GPP AAA proxy according to claim 4, and methods according to claims 5 and 8.

[0012] Some embodiments of apparatus and/or methods in accordance with embodiments of the present invention are now described, by way of example only, and with reference to the accompanying drawings, in which:

- Figure 1 is intended to recall an example of non-roaming architecture for 3GPP and Non 3GPP (Trusted or Untrusted) access to EPC,
- Figure 2 is intended to recall an example of roaming architecture for 3GPP and Non 3GPP (Trusted or Untrusted) access to EPC,
- Figure 3 is intended to illustrate an example of signaling flow for authentication and authorization procedure, for untrusted WLAN access to EPC,
- Figure 4 is intended to illustrate signaling flow for authentication and authorization procedure including IMEI checking, for untrusted WLAN access to EPC,
- Figure 5 is intended to illustrate signaling flow for authentication and authorization procedure including IMEI checking, for trusted WLAN access to EPC,
- Figure 6 is intended to illustrate signaling flow for authentication and authorization procedure including IMEI checking, for trusted WLAN access to EPC,
- Figure 7 is intended to illustrate signaling flow for authentication and authorization procedure includ-

ing IMEI checking, for untrusted WLAN access to EPC,

- Figure 8 is intended to illustrate an example of signaling flow for authentication and authorization procedure including IMEI checking, for trusted WLAN access to EPC, according to embodiments of the invention,
- Figure 9 is intended to illustrate signaling flow for authentication and authorization procedure including IMEI checking, for untrusted WLAN access to EPC,
- Figure 10 is intended to illustrate an example of signaling flow for authentication and authorization procedure including IMEI checking, for trusted WLAN access to EPC, according to embodiments of the invention.

Abbreviations

[0013]

AAA	Authentication Authorization Accounting
AKA	Authentication and Key Agreement
DEA	Diameter EAP Answer
DER	Diameter EAP Request
EAP	Extensible Authentication Protocol
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
HPLMN	Home Public Land Mobile Network
HSS	Home Subscriber Server
IMSI	International Mobile Subscriber Identity
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
LTE	Long Term Evolution
PDN	Packet Data Network
PDN GW	PDN Gateway
PLMN	Public Land Mobile Network
TWAN	Trusted WLAN Access Network
UWAN	Untrusted WLAN Access Network
UE	User Equipment
HPLMN	Visited Public Land Mobile Network
WLAN	Wireless Local Area Network

[0014] Description of various aspects and/or embodiments of the invention

[0015] IMEI(SV) checking is specified for 3GPP accesses for CS and PS domains in TS 23.002, TS 23.018, TS 23.060 and TS 23.401, as well as in appropriate stage 3 specifications. In order to check the IMEI(SV), the network needs to trigger the retrieval of the IMEI(SV) from the UE. NAS messages are specified for that. IMEI(SV) retrieval for non-3GPP accesses such as trusted and untrusted WLAN is specified but for such non-3GPP accesses IMEI(SV) checking in the EIR is not specified yet and a study is currently under progress in SA2 to define whether EIR should be interfaced to the TWAN (for trusted WLAN access) and to ePDG (for untrusted WLAN) or to the AAA server. All contributions up to now push for interfacing the EIR with the AAA server for various reasons, one reason being that the architecture would be common to both trusted and untrusted WLAN, another reason being that it reduces the number of interfaces to the EIR .

[0016] CT1 has recently agreed in CT1 two CRs that allow the network to retrieve the ME's IMEI(SV): 24.302 CR0460 for trusted WLAN and 24.302 CR0461 for untrusted WLAN. For the trusted WLAN case, the IMEI(SV) is retrieved from the UE by the AAA server (via EAP-AKA' new attribute AT_DEVICE_IDENTITY), while for the untrusted WLAN case the IMEI(SV) is retrieved from the UE by the ePDG (via a new IKEv2 attribute DEVICE_IDENTITY).

[0017] However, which entity should trigger the IMEI(SV) checking, and which entity should decide whether to continue the authorization process in case of black-listed, grey-listed or white-listed ME is not specified.

[0018] For non roaming PS sessions, the AAA server (in HPLMN) could be this entity. But for roaming sessions like emergency sessions, this might be in the VPLMN. The main reason is local regulatory policies which force the emergency sessions/calls to be handled by the VPLMN (or by the TWAN operator in the trusted WLAN access case) and thus to take decision on whether to accept emergency sessions issued by e.g. potentially stolen devices.

[0019] This would be in line with the mechanisms specified for the 3GPP accesses where the IMEI checking is fully performed in the VPLMN (by the MSC, SGSN, MME). See e.g. TS 23.401 clause 5.3.2.1, which specifies in step 5b:

"In order to minimise signalling delays, the retrieval of the ME Identity may be combined with NAS security setup in step 5a. The MME may send the ME Identity Check Request (ME Identity, IMSI) to the EIR. The EIR shall respond with ME Identity Check Ack (Result). Dependent upon the Result, the MME decides whether to continue with this Attach procedure or to reject the UE.

[0020] For an Emergency Attach, the IMEI check to the EIR may be performed. If the IMEI is blocked, operator policies determine whether the Emergency Attach procedure continues or is stopped."

[0021] In case of WLAN access to EPC, no solution is specified for triggering the IMEI(SV) checking and deciding whether to continue the Access authorization in case of in case of black-listed or grey-listed ME (Mobile Equipment) especially in case of roaming.

[0022] Only a partial solution for the HPLMN is disclosed:

- For untrusted WLAN case, the ePDG retrieves the IMEI(SV) from the UE per TS 29.273 CR0422. This can be done at step 6 of the authentication procedure described in TS 33.402 clause 8.2.2. The ePDG sends the IKE_AUTH
- Response message to the UE together with the EAP

Payload for AKA-Challenge, and the UE responds with its IMEI(SV) together with the EAP payload for AKA-Challenge in step 8 as specified by TS 24.302 CR0461. The IMEI(SV) is provided in step 8 to the AAA Server, which can then complete authentication and check IMEI in step 8a. No additional exchange with the AAA server is required.

Figure 8.2.2-1 in clause 8.2.2 of TS 33.402 (Tunnel full authentication and authorization - untrusted access) has been updated (figure 3) for enabling IMEI checking by the AAA server.

[0023] The signaling flows of Figures 4, 5 and 6 allow in roaming scenarios the ePDG orTWAN operator to request IMEI checking using an EIR (Equipment Identity Register) via the AAA server in the Home PLMN.

[0024] Unfortunately, the signaling flows of Figures 4, 5 and 6 are not applicable to all operators because, although some operators use a centralized EIR (e.g. the GSMA EIR), some other operators are willing to check the IMEI using an EIR that is local to their PLMN or to the country.

[0025] The signaling flows of Figures 7 to 10, in addition to allowing in roaming scenarios the ePDG orTWAN operator to request IMEI checking using an EIR (Equipment Identity Register) via the AAA server in the Home PLMN, allow the ePDG or the TWAN operator to request IMEI checking using an EIR located in the VPLMN country and connected to the 3GPP AAA proxy.

1) Figures 4, 5 and 6

[0026] The signaling flows of Figures 4, 5 and 6 enhance the above mechanism for IMEI(SV) checking, which only allows the ePDG to decide whether to retrieve the IMEI(SV) from the UE, to allow the 3GPP AAA server to instruct the ePDG to retrieve the IMEI(SV) from the UE.

[0027] The signaling flows also include enhancing the above mechanism for IMEI(SV) checking, which only allows full IMEI checking procedure by the HPLMN, to allow the VPLMN or the TWAN operator to

- request to have IMEI checking performed

  - - decide on whether to continue or stop the authorization process depending on the result of IMEI checking e.g. in case of black-listed, grey-listed or white-listed ME

although the IMEI checking is performed via the 3GPP AAA server in the HPLMN.

[0028] If it is required that the operator granting the access (VPLMN or TWAN operator) must decide whether to continue the Access authorization process in case of black-listed, grey-listed or white-listed ME (at least for emergency session with Local Break Out). The signaling flows, allowing in particular to minimize the number of AAA server exchanges and the number of interfaces to the EIR include one or more of:

- In untrusted WLAN case, after it receives the IKE_AUTH Request from the UE, the ePDG may add an **"IMEI check request"** indication in the subsequent Authentication & Authorization Request (Diameter DER) message to the AAA server.

- As the AAA server in HPLMN may want to carry out an IMEI check, it needs to ensure that the IMEI is requested from the UE. In TWAN case it is the AAA server that requests the IMEI from the UE. In the untrusted WLAN case, it is the ePDG that requests the IMEI from the UE. Thus the AAA server needs to be able to instruct the ePDG to retrieve the IMEI from the UE: in the untrusted WLAN case, the AAA server may add an **"IMEI-request"** indicator in the signaling to the ePDG.

- In trusted WLAN case, after it receives the first EAP-RSP/Identity message from the UE, the TWAN may add an **"IMEI check request"** indication in the subsequent Authentication & Authorization Request (Diameter DER) message to the AAA server.

- Then in both trusted and untrusted WLAN cases, the AAA server would request the EIR to check the IMEI.

- To allow the ePDG/TWAN to decide whether the call setup should continue or should be stopped, it is proposed to add another indication **"action on IMEI check result"** in the DER message. The Authentication & Authorization Answer (Diameter DEA) message would also contain a indication "IMEI check result" in order to inform the ePDG/TWAN whether the authorization for the emergency call was given to a user that uses a black-listed, grey-listed or white-listed ME. The ePDG/TWAN may then decide e.g. to inform the local authorities. This is depicted in the following two call flows.

- **"action on IMEI check result"** provides the AAA server with instructions on whether to continue or to stop the authorization process to the UE for each of the IMEI check result values provided by the EIR i.e. black-listed ME, grey-listed ME and white-listed ME. In the case of a trusted WLAN access, the instructions may also only allow to continue the authorization process for an emergency session (the UE indicates this is an emergency session in EAP signalling to the 3GPP AAA server, and the TWAN is not aware whether the authentication and authorization procedure initiated by the UE is to setup an emergency session till much later in the call flow).

Untrusted WLAN

[0029] An example of call flow in case of Untrusted

WLAN is depicted in figure 4. The IMEI retrieval has been recently agreed at 3GPP (i.e. IMEI Request parameter in step 6, IMEI parameter and the steps 8b and 8c in the figure). Figure 4 includes the addition of IMEI Request in step 5, IMEI Check Request and Action on IMEI Check Result

[0030] (black-listed, grey-listed or white-listed ME).

Notes

[0031]

- The parameter **"Action on IMEI check result"** contains the action (Stop, Continue) for the case of regular attach/session requests and the action for the case of emergency attach/session requests. Or it may contain a single action (Stop, Continue, Continue Only for an emergency session)

- the call flow (AA-answer in step 9 contains EAP-Success) depicts the case where the terminal was detected by the EIR check as not black/grey listed or where the "Action on IMEI Check Result" was "Continue"

- In case where the terminal would be detected by the EIR check as black/grey listed and where the corresponding "Action on IMEI Check Result" would not be "Continue", the AA-answer in step 9 would contain an EAP-rejection.

- In both cases, if the "IMEI Check Result" indicates that the terminal was detected by the EIR check as black/grey listed, the ePDG may log information and inform the local authorities.

Trusted WLAN

[0032] An example of signaling flow related to a possible solution in case of Trusted WLAN is depicted in figure 5.

[0033] The IMEI retrieval has been recently agreed at 3GPP (i.e. IMEI Request parameter, IMEI parameter and the steps 22c and 22d in the figure).

[0034] Figure 5 includes the addition of IMEI Request in steps 4 and 5, IMEI Check Request and Action on IMEI Check Result (black-listed, grey-listed or white-listed ME).

Notes:

[0035]

- The parameter **"Action on IMEI check result"** may contain the action (Stop, Continue) for the case of regular attach/session requests and the action for the case of emergency attach/session requests. Or it may contain a single action (Stop, Continue, Continue Only for an emergency session).

- IMEI Request parameter in steps 4 and 5 is intended to request the AAA server to retrieve the IMEI(SV) from the UE and to return it to the TWAN. The absence of this parameter does not preclude the AAA server to decide the retrieval of the IMEI(SV) from the UE and to provide it to the TWAN.

[0036] An alternative solution includes requesting IMEI Check as soon as possible i.e. in the EAP-RSP/Identity in step 4. An example of a corresponding call flow is depicted in figure 6.

[0037] Figure 6 includes the addition of IMEI Check Request and Action on IMEI Check Result (black-listed, grey-listed or white-listed ME).

Notes

[0038]

- The parameter **"Action on IMEI check result"** may contain the action (Stop, Continue) for the case of regular attach/session requests and the action for the case of emergency attach/session requests. Or it may contain a single action (Stop, Continue, Continue Only for an emergency session).

- the **"IMEI Request"** in steps 4 and 5 of the other alternative (intended to request the AAA server to retrieve the IMEI(SV) from the UE and to return it to the TWAN) could also be used in this alternative in case the TWAN wants to trigger the acquisition of the IMEI for other purposes than EIR check .

- the call flow (AA-answer in step 23 contains EAP-Success) depicts the case where the terminal was detected by the EIR check as not e.g. black or grey listed or where the "Action on IMEI Check Result" was "Continue".

- In case the terminal would be detected by the EIR check as e.g. black or grey listed and where the corresponding "Action on IMEI Check Result" would not be "Continue", the AA-answer in step 23 would contain an EAP-rejection.

- In both cases, if the "IMEI Check Result" indicates that the terminal was detected by the EIR check as black/grey listed, the TWAN may log information and inform the local authorities.

2) Figures 7 to 10

[0039] The signaling flows of Figures 7 to 10 allow the handling of IMEI checking assuming two cases i.e. where the EIR is in the visited country and where the EIR is in the home country. It is also assumed that the AAA server/-

proxy is interfaced with the EIR.

[0040] It is assumed that the EIR (specified in particular in TS 23.002) is interfaced with the AAA server (or proxy) and not directly to the ePDG/TWAN to minimize the number of interfaces and to avoid the duplication of the procedures in ePDG and TWAN.

[0041] As already indicated, the non-roaming case mechanism is straight forward, but the roaming case requires more analysis.

[0042] For 3GPP access, TS 23.401 clause 5.3.2.1 specifies in step 5b: *"In order to minimise signalling delays, the retrieval of the ME Identity may be combined with NAS security setup in step 5a.* The MME may send *the ME Identity Check Request (ME Identity, IMSI) to the EIR. The EIR shall respond with ME Identity Check Ack (Result).* Dependent upon the Result, the MME decides whether to continue with this Attach procedure or to reject the UE." Therefore, for 3GPP access, the decision for triggering the IMEI check procedure, as well as the decision for continuing the procedure is performed in the VPLMN.

[0043] Moreover, depending on local regulations, the EIR may be located in the visited country (local EIR, not always synchronized with an EIR outside the country) or centralized (e.g. GSMA EIR). The solution should work with both alternatives.

[0044] In embodiments of the invention, the operator who is granting the access (i.e. the VPLMN or the TWAN operator) takes the responsibility of the action plan i.e.

- determining whether to trigger IMEI checking,
- determining (via e.g. operator configuration) whether the EIR to be used is in the local country or in the home country, and
- deciding whether to continue the authorization process in case of black-listed, grey-listed or white-listed UE (at least for emergency session with Local Break Out).

[0045] In the untrusted WLAN case, the ePDG can retrieve the IMEI from the UE on its own. It is not the case for trusted WLAN case, in which only the 3GPP AAA server can do that. Hence, the solutions for untrusted WLAN and for trusted WLAN will necessarily be different.

[0046] Examples of signaling flows allowing in particular to minimize the number of AAA exchanges are illustrated in figures 7 to 10.

[0047] Examples of signaling flows illustrated in figures 7 (untrusted WLAN) and 8 (trusted WLAN) are first described.

Untrusted WLAN

[0048] For untrusted WLAN, an example of signaling allowing to keep the same number of 3GPP AAA exchanges is illustrated in figure 7:

- After it receives the IKE_AUTH Request from the UE, the ePDG first decides to retrieve the IMEI from the UE (step 6 of figure 7). In order to allow the 3GPP AAA proxy or server to check the IMEI via the EIR, the ePDG just has to add the following parameters in the subsequent Authentication & Authorization Request DER Diameter message to the 3GPP AAA server (step 8 of figure 7):

  ◦ the **IMEI** retrieved from the UE (part of Terminal Information IE in Authentication and Authorization Request message) ,

  ◦ an **"IMEI check request"** parameter that indicates whether the IMEI shall be checked by the visited country EIR, or by the home country EIR. The absence of this parameter indicates that IMEI check should not be performed.

- The ePDG also has to decide whether the authorization process should continue or should be stopped depending on the IMEI check result. Hence it is proposed to add another parameter **"Action upon IMEI check"** indicating whether the 3GPP AAA server shall continue or stop the authentication and authorization procedure for each of the potential IMEI check results from the EIR (e.g. unknown, black listed, grey listed, white listed).

- The 3GPP AAA Proxy always forwards the **"Action upon IMEI check"** and **"IMEI check request"** parameters to the 3GPP AAAA server. In addition, if the **"IMEI check request"** parameter indicates the visited country EIR, the 3GPP AAA proxy will then request the EIR to check the IMEI and to provide the **"IMEI check result"** returned by the EIR to the 3GPP AAA server (step 8c in figure 7).

- If the **"IMEI check request"** parameter indicates the home country EIR, the 3GPP AAA server requests the EIR to check the IMEI.

- Based on **"Action upon IMEI check"** and **"IMEI check result"** returned by the visited or home EIR, the AAA server determines whether the authentication and authorization procedure shall continue or shall be stopped.

Trusted WLAN

[0049] For trusted WLAN, an example of signaling flow which may require one more 3GPP AAA exchange is illustrated in figure 8. When the EIR is in the visited country, the TWAN cannot immediately provide the IMEI to the 3GPP AAA proxy. Hence, it may be necessary to have a preliminary step where the TWAN asks the 3GPP AAA server to retrieve the IMEI and to return it to the TWAN, before the 3GPP AAA proxy can check the IMEI via the local country EIR:

- After it receives the first EAP-RSP/Identity message from the UE, the TWAN adds to the subsequent Authentication & Authorization Request DER Diameter message to the 3GPP AAA server (via the 3GPP AAA Proxy in roaming cases) (steps 4 and 5 in figure 8):

    ◦ The **"IMEI check request"** parameter indicates whether the IMEI shall be checked by the visited country EIR, or by the home country EIR. The absence of this parameter indicates that IMEI check should not be performed;

    ◦ The **"Action upon IMEI check"** parameter indicates whether the 3GPP AAA server shall continue or stop the authentication and authorization procedure for each of the potential IMEI check results from the EIR (e.g. unknown, black listed, grey listed, white listed);

- If the 3GPP AAA server receives the **"IMEI check request"** parameter from a TWAN, it shall perform the IMEI retrieval (step 13 to 17 in figure 8).

- After the 3GPP AAA server has retrieved the IMEI,

    ◦ If the **"IMEI check request"** parameter indicates the visited country EIR, the 3GPP AAA server shall return the IMEI to the TWAN in **a new AAA-TWAN DEA Diameter message with EAP-Payload AVP absent,** with the result code set to DIAMETER_MULTI_ROUND_AUTH and with **a new "IMEI-in-VPLMN-Check" flag** set to 1 in the DEA-Flags AVP (same mechanism as specified in TS 29.273 for TWAN SCM mode) (steps 19a and 19b in figure 8);

    ◦ If the **"IMEI check request"** parameter indicates the home country EIR, the 3GPP AAA server requests the EIR to check the IMEI (steps 19c and 19d in figure 8);

    ◦ If no IMEI check was required, the 3GPP AAA server should/may still provide the IMEI to the TWAN if available. This may be done via any message other than step 19a/19b, e.g. in step 23a/23b or any other intermediate message not shown in figure 8.

- If the TWAN receives the above **AAA-TWAN DEA Diameter message** with the **"IMEI-in-VPLMN-Check" flag** set to 1,

    ◦ The TWAN re-issues a new DER command via the 3GPP AAA Proxy including the last EAP-Payload sent in the previous request, together with the **"IMEI-in-VPLMN-Check" flag** set to 1 in the DER-Flags AVP and the IMEI (step 20a in figure 8);

    ◦ The 3GPP AAA Proxy requests the EIR to check the IMEI and forwards the **"IMEI check result"** returned by the EIR to the AAA server (steps 20b to 20d in figure 8).

[0050] The AAA server applies the IMEI check instructions received in the **"Action upon IMEI check"** i.e., based on the **"Action upon IMEI check"** and on the **"IMEI check result"** from the visited or home EIR, determines whether the authentication and authorization procedure shall continue or shall be stopped (step 21 in figure 8).

[0051] Examples of signaling flows illustrated in figures 9 (untrusted WLAN access) and 10 (trusted WLAN access) are now described.

Untrusted WLAN

[0052] For untrusted WLAN, an example of signaling flow allowing to keep the same number of 3GPP AAA exchanges is illustrated in figure 9:

- After it receives the IKE_AUTH Request from the UE, the ePDG first decides to retrieve the IMEI from the UE (step 6 of figure 9). In order to allow the 3GPP AAA proxy or server to check the IMEI via the EIR, the ePDG just has to add the following parameters in the subsequent Authentication & Authorization Request DER Diameter message to the 3GPP AAA server (step 8 of figure 9):

    ◦ the **IMEI** retrieved from the UE (already existing and part of Terminal Information IE in Authentication and Authorization Request message),

    ◦ an **"IMEI check request"** parameter that indicates whether the IMEI shall be checked by the visited country EIR, or by the home country EIR. The absence of this parameter indicates that IMEI check should not be performed.

- The ePDG also has to decide whether the authorization process should continue or should be stopped depending on the IMEI check result. Hence it is proposed to add another parameter **"Action upon IMEI check"** indicating whether the 3GPP AAA server or AAA proxy shall continue or stop the authentication and authorization procedure for each of the potential IMEI check results from the EIR (e.g. unknown, black listed, grey listed, white listed).

- If the **"IMEI check request"** parameter indicates the visited country EIR, the 3GPP AAA proxy will then have to request the EIR to check the IMEI and, based on the **"Action upon IMEI check"** provided by the

ePDG, will determine whether the authentication and authorization procedure shall continue or shall be stopped. This indication will be provided to the 3GPP AAA server via the **"Decision to Proceed"** parameter.
NOTE: An alternative could be that, instead of computing and sending the "Decision to Proceed" parameter, the 3GPP AAA Proxy signals to the 3GPP AAA server the result of the IMEI check (e.g. black, white ..) together with the "action upon IMEI check" parameter, leaving the 3GPP AAA server in the HPLMN behaving in a similar manner than if it did the IMEI check itself towards an EIR in the HPLMN.

- If the **"IMEI check request"** parameter indicates the home country EIR, the 3GPP AAA proxy forwards the ePDG request unchanged to the 3GPP AAA server.

Trusted WLAN

[0053] For trusted WLAN, an example of signaling flow which may require one more 3GPP AAA exchange is illustrated in figure 10. When the EIR is in the visited country, the TWAN cannot immediately provide the IMEI to the 3GPP AAA proxy. Hence, it may be necessary to have a preliminary step where the TWAN asks the 3GPP AAA server to retrieve the IMEI and to return it to the TWAN, before the 3GPP AAA proxy can check the IMEI via the local country EIR:

- After it receives the first EAP-RSP/Identity message from the UE, the TWAN just have to add the **"IMEI check request"** parameter in the subsequent Authentication & Authorization Request DER Diameter message to the 3GPP AAA server (step 4 of figure 10). If the "IMEI check request" parameter indicates the home country EIR, the parameter **"Action upon IMEI check"** is also added.

    ◦ If the 3GPP AAA server receives the "IMEI check request" parameter from a TWAN, it shall perform the IMEI retrieval.

    ◦ After IMEI retrieval:

        ▪ If the "IMEI check request" parameter indicates the visited country EIR, the 3GPP AAA server returns the IMEI to the TWAN and postpones the final decision on Authentication and Authorization until explicit indication from the TWAN or the 3GPP AAA proxy (see further steps).

        ▪ If the "IMEI check request" parameter indicates the home country EIR, the 3GPP AAA server requests the EIR to check the IMEI (steps 19c and 19d in figure 10);

- After the 3GPP AAA server has retrieved the IMEI and if the "IMEI check request" parameter indicates the visited country EIR, it shall return it to the TWAN in **a new AAA-TWAN DEA Diameter message with EAP-Payload AVP absent,** with the result code set to DIAMETER MULTI ROUND AUTH and with **a new "IMEI-in-VPLMN-Check" flag** set to 1 in the DEA-Flags AVP (same mechanism as specified in TS 29.273 for TWAN SCM mode).

- The TWAN then re-issues a new DER command including the last EAP-Payload sent in the previous request, together with the **"IMEI-in-VPLMN-Check" flag** set to 1 in the DER-Flags AVP, the IMEI, the **"IMEI check request"** parameter and the **"Action upon IMEI check"** parameter.

    ◦ The **"IMEI check request"** parameter indicates that the IMEI shall be checked by the visited country EIR

    ◦ The **"Action upon IMEI check"** parameter indicates whether the 3GPP AAA server or AAA proxy shall continue or stop the authentication and authorization procedure for each of the potential IMEI check results from the EIR (e.g. unknown, black listed, grey listed, white listed).

    ◦ The **"IMEI-in-VPLMN-Check" flag** set to 1 in the DER-Flags AVP indicates to the AAA server that the EAP-Payload can be discarded since already sent in previous DER (same principle as for TS 29.273 for TWAN SCM mode).

- When the TWAN receives the IMEI from the 3GPP AAA server, the process continues in the same way as in the ePDG case:
  If the **"IMEI check request"** parameter indicates the visited country EIR, the 3GPP AAA proxy requests the EIR to check the IMEI and, based on the **"Action upon IMEI check",** determines whether the authentication and authorization procedure shall continue or shall be stopped. This indication is provided to the 3GPP AAA server via the **"Decision to proceed"** parameter.

[0054] A person of skill in the art would readily recognize that steps of various above-described methods can be performed by programmed computers. Herein, some embodiments are also intended to cover program storage devices, e.g., digital data storage media, which are machine or computer readable and encode machine-executable or computer-executable programs of instructions, wherein said instructions perform some or all of the steps of said above-described methods. The program storage devices may be, e.g., digital memories, magnetic storage media such as a magnetic disks and magnetic tapes, hard drives, or optically readable digital data sto-

rage media. The embodiments are also intended to cover computers programmed to perform said steps of the above-described methods.

Claims

1. An Authentication Authorization Accounting server in a Home Public Land Mobile Network of a Third Generation Partnership Project packet core for a user equipment, wherein the Authentication Authorisation Accounting server is configured to:

   receive from a Trusted WLAN access network a request for checking of an International Mobile Equipment Identity of the user equipment by an Equipment Identity Register in a Visited Public Land Mobile Network for the user equipment;
   send an Authentication Authorization Accounting message to the Trusted WLAN access network, wherein the Authentication Authorization Accounting message comprises an International Mobile Equipment Identity retrieved from the user equipment via the Trusted WLAN access network, and an indication that the International Mobile Equipment Identity is to be checked by the Equipment Identity Register in said Visited Public Land Mobile Network.

2. An Authentication Authorization Accounting server according to claim 1, wherein receiving the request comprises receiving an Authentication Authorization Accounting Diameter Extensible Authentication Protocol message comprising an indication that the International Mobile Equipment Identity is to be checked by the Equipment Identity Register in said Visited Public Land Mobile Network, and wherein the Authentication Authorization Accounting message comprises an Authentication Authorization Accounting Diameter Extensible Authentication Protocol message.

3. An Authentication Authorization Accounting server according to claim 1 or 2, configured to:
   receive an indication of a determination whether to continue or stop an authentication and authorization procedure for the user equipment based on a result of checking the International Mobile Equipment Identity by said Equipment Identity Register in said Visited Public Land Mobile Network.

4. An Authentication Authorization Accounting proxy of a Third Generation Partnership Project packet core, configured to:

   receive a first Authentication Authorization Accounting message from a Trusted WLAN access network, wherein the first Authentication Authorization Accounting message comprises an International Mobile Equipment Identity retrieved from the user equipment via an Authentication Authorisation Accounting server for the user equipment in a Home Public Land Mobile Network of a Third Generation Partnership Project packet core, and an indication that the International Mobile Equipment Identity is to be checked by an Equipment Identity Register in a Visited Public Land Mobile Network for the user equipment; and
   send a second Authentication Authorization Accounting message to the Authentication Authorization Accounting server for the user equipment, wherein the second Authentication Authorization Accounting message comprises an indication of a determination at the Authentication Authorization Accounting proxy whether to continue or stop an authentication and authorization procedure at the Authentication Authorization Accounting server for the user equipment based on a result of checking the International Mobile Equipment Identity by the Equipment Identity Register in the Visited Public Land Mobile Network for the user equipment.

5. An Authentication Authorization Accounting proxy according to claim 4, wherein the first Authentication Authorization Accounting message comprises an Authentication Authorization Accounting Diameter Extensible Authentication Protocol message, and wherein the second Authentication Authorization Accounting message comprises an Authentication Authorization Accounting Diameter Extensible Authentication Protocol message

6. A method, comprising:

   receiving at an Authentication Authorization Accounting server in a Home Public Land Mobile Network of a Third Generation Partnership Project packet core for a user equipment from a Trusted WLAN access network a request for checking of an International Mobile Equipment Identity of the user equipment by an Equipment Identity Register in a Visited Public Land Mobile Network for the user equipment, and
   sending an Authentication Authorization Accounting message from the Authentication Authorization Accounting server to the Trusted WLAN access network, wherein the Authentication Authorization Accounting message comprises an International Mobile Equipment Identity retrieved from the user equipment via the Trusted WLAN access network, and an indication that the International Mobile Equipment Identity is to be checked by the Equipment Identity Register in said Visited Public Land Mobile

Network.

7. The method according to claim 6, wherein receiving the request comprises receiving an Authentication Authorization Accounting Diameter Extensible Authentication Protocol message comprising an indication that the International Mobile Equipment Identity is to be checked by the Equipment Identity Register in said Visited Public Land Mobile Network; and wherein the Authentication Authorization Accounting message comprises an Authentication Authorization Accounting Diameter Extensible Authentication Protocol message.

8. The method according to claim 6 or claim 7, comprising:
receiving at the Authentication Authorization Accounting server an indication of a determination whether to continue or stop an authentication and authorization procedure for the user equipment based on a result of checking the International Mobile Equipment Identity by said Equipment Identity Register in said Visited Public Land Mobile Network.

9. A method comprising:

receiving at an Authentication Authorization Accounting proxy of a Third Generation Partnership Project packet core a first Authentication Authorization Accounting message from a Trusted WLAN access network entity, wherein the first Authentication Authorization Accounting message comprises an International Mobile Equipment Identity retrieved from the user equipment via an Authentication Authorisation Accounting server for the user equipment in a Home Public Land Mobile Network of a Third Generation Partnership Project packet core, and an indication that the International Mobile Equipment Identity is to be checked by an Equipment Identity Register in a Visited Public Land Mobile Network for the user equipment; and
sending a second Authentication Authorization Accounting message from the Authentication Authorization Accounting proxy to the Authentication Authorization Accounting server for the user equipment in the Home Public Land Mobile Network, wherein the second Authentication Authorization Accounting message comprises an indication of a result of a determination at the Authentication Authorization Accounting proxy whether to continue or stop an authentication and authorization procedure at the Authentication Authorisation Accounting server for the user equipment based on a result of checking the International Mobile Equipment Identity by the Equipment Identity Register in a Visited Public Land Mobile Network for the user equipment.

10. The method according to claim 9, wherein the first Authentication Authorization Accounting message comprises an Authentication Authorization Accounting Diameter Extensible Authentication Protocol message, and wherein the second Authentication Authorization Accounting message comprises an Authentication Authorization Accounting Diameter Extensible Authentication Protocol message.

Patentansprüche

1. Authentication Authorization Accounting Server in einem Home Public Land Mobile Network eines Third Generation Partnership Project Paketkerns für ein Benutzergerät, wobei der Authentication Authorization Accounting Server ausgestaltet ist zum:

Empfangen, von einem Trusted WLAN Zugangsnetz, einer Anforderung zur Prüfung einer International Mobile Equipment Identity des Benutzergeräts durch ein Equipment Identity Register in einem Visited Public Land Mobile Network für das Benutzergerät;
Senden einer Authentication Authorization Accounting Nachricht an das Trusted WLAN Zugangsnetz, wobei die Authentication Authorization Accounting Nachricht eine International Mobile Equipment Identity, die von dem Benutzergerät über das Trusted WLAN Zugangsnetz abgerufen wird, und eine Angabe umfasst, dass die International Mobile Equipment Identity durch das Equipment Identity Register in dem Visited Public Land Mobile Network zu prüfen ist.

2. Authentication Authorization Accounting Server nach Anspruch 1, wobei das Empfangen der Anforderung das Empfangen einer Authentication Authorization Accounting Diameter Extensible Authentication Protocol Nachricht umfasst, die eine Angabe umfasst, dass die International Mobile Equipment Identity durch das Equipment Identity Register in dem Public Land Mobile Network zu prüfen ist, und wobei die Authentication Authorization Accounting Nachricht eine Authentication Authorization Accounting Diameter Extensible Authentication Protocol Nachricht umfasst.

3. Authentication Authorization Accounting Server nach Anspruch 1 oder 2, der ausgestaltet ist zum:
Empfangen einer Angabe einer Bestimmung, ob die Authentifizierungs- und Autorisierungsprozedur für das Benutzergerät fortzusetzen oder anzuhalten ist, basierend auf einem Ergebnis der Prüfung der International Mobile Equipment Identity durch das Equipment Identity Register in dem Visited Public Land Mobile Network.

4. Authentication Authorization Accounting Proxy eines Third Generation Partnership Project Paketkerns, der ausgestaltet ist zum:

Empfangen einer ersten Authentication Authorization Accounting Nachricht von einem Trusted WLAN Zugangsnetz, wobei die erste Authentication Authorization Accounting Nachricht eine International Mobile Equipment Identity, die von dem Benutzergerät über einen Authentication Authorization Accounting Server für das Benutzergerät in einem Home Public Land Mobile Network eines Third Generation Partnership Project Paketkerns abgerufen wurde, und eine Angabe umfasst, dass die International Mobile Equipment Identity durch ein Equipment Identity Register in einem Visited Public Land Mobile Network für das Benutzergerät zu prüfen ist; und
Senden einer zweiten Authentication Authorization Accounting Nachricht an den Authentication Authorization Accounting Server für das Benutzergerät, wobei die zweite Authentication Authorization Accounting Nachricht eine Angabe einer Bestimmung an dem Authentication Authorization Accounting Proxy umfasst, ob eine Authentifizierungs- und Autorisierungsprozedur an dem Authentication Authorization Accounting Server für Benutzergerät fortzusetzen oder anzuhalten ist, basierend auf einem Ergebnis der Prüfung der International Mobile Equipment Identity durch das Equipment Identity Register in dem Visited Public Land Mobile Network für das Benutzergerät.

5. Authentication Authorization Accounting Proxy nach Anspruch 4, wobei die erste Authentication Authorization Accounting Nachricht eine Authentication Authorization Accounting Diameter Extensible Authentication Protocol Nachricht umfasst, und wobei die zweite Authentication Authorization Accounting Nachricht eine Authentication Authorization Accounting Diameter Extensible Authentication Protocol Nachricht umfasst.

6. Verfahren, umfassend:

Empfangen, an einem Authentication Authorization Accounting Server in einem Home Public Land Mobile Network eines Third Generation Partnership Project Paketkerns für ein Benutzergerät von einem Trusted WLAN Zugangsnetz, einer Anforderung zur Prüfung einer International Mobile Equipment Identity des Benutzergeräts durch ein Equipment Identity Register in einem Visited Public Land Mobile Network für das Benutzergerät, und
Senden einer Authentication Authorization Accounting Nachricht von dem Authentication Authorization Accounting Server an das Trusted WLAN Zugangsnetz, wobei die Authentication Authorization Accounting Nachricht eine International Mobile Equipment Identity, die von dem Benutzergerät über das Trusted WLAN Zugangsnetz abgerufen wird, und eine Angabe umfasst, dass die International Mobile Equipment Identity durch das Equipment Identity Register in dem Visited Public Land Mobile Network zu prüfen ist.

7. Verfahren nach Anspruch 6, wobei das Empfangen der Anforderung das Empfangen einer Authentication Authorization Accounting Diameter Extensible Authentication Protocol Nachricht umfasst, die eine Angabe umfasst, dass die International Mobile Equipment Identity durch das Equipment Identity Register in dem Visited Public Land Mobile Network zu prüfen ist; und wobei die Authentication Authorization Accounting Nachricht eine Authentication Authorization Accounting Diameter Extensible Authentication Protocol Nachricht umfasst.

8. Verfahren nach Anspruch 6 oder Anspruch 7, umfassend:
Empfangen, an dem Authentication Authorization Accounting Server, einer Angabe einer Bestimmung, ob eine Authentifizierungs- und Autorisierungsprozedur für das Benutzergerät fortzusetzen oder anzuhalten ist, basierend auf einem Ergebnis der Prüfung der International Mobile Equipment Identity durch das Equipment Identity Register in dem Visited Public Land Mobile Network.

9. Verfahren, umfassend:

Empfangen, an einem Authentication Authorization Accounting Proxy eines Third Generation Partnership Project Paketkerns, einer ersten Authentication Authorization Accounting Nachricht von einer Trusted WLAN Zugangsnetzentität, wobei die erste Authentication Authorization Accounting Nachricht eine International Mobile Equipment Identity, die von dem Benutzergerät über einen Authentication Authorization Accounting Server für das Benutzergerät in einem Home Public Land Mobile Network eines Third Generation Partnership Project Paketkerns abgerufen wird, und eine Angabe umfasst, dass die International Mobile Equipment Identity durch ein Equipment Identity Register in einem Visited Public Land Mobile Network für das Benutzergerät zu prüfen ist; und
Senden einer zweiten Authentication Authorization Accounting Nachricht von dem Authentication Authorization Accounting Proxy an den Authentication Authorization Accounting Server für das Benutzergerät in dem Home Public Land

Mobile Network, wobei die zweite Authentication Authorization Accounting Nachricht eine Angabe eines Ergebnisses einer Bestimmung an dem Authentication Authorization Accounting Proxy umfasst, ob eine Authentifizierungs- und Autorisierungsprozedur an dem Authentication Authorization Accounting Server für das Benutzergerät fortzusetzen oder anzuhalten ist, basierend auf einem Ergebnis des Prüfens der International Mobile Equipment Identity durch das Equipment Identity Register in einem Visited Public Land Mobile Network für das Benutzergerät.

10. Verfahren nach Anspruch 9, wobei die erste Authentication Authorization Accounting Nachricht eine Authentication Authorization Accounting Diameter Extensible Authentication Protocol Nachricht umfasst, und wobei die zweite Authentication Authorization Accounting Nachricht eine Authentication Authorization Accounting Diameter Extensible Authentication Protocol Nachricht umfasst.

Revendications

1. Serveur d'authentification, d'autorisation et de comptabilité dans un réseau mobile terrestre public domestique d'un coeur de paquet de projet de partenariat de troisième génération pour un équipement utilisateur, dans lequel le serveur d'authentification, d'autorisation et de comptabilité est configuré pour :

recevoir d'un réseau d'accès WLAN de confiance une demande de vérification d'une identité internationale d'équipement mobile de l'équipement utilisateur par un registre d'identités d'équipements dans un réseau mobile terrestre public visité pour l'équipement utilisateur ;
envoyer un message d'authentification, d'autorisation et de comptabilité au réseau d'accès WLAN de confiance, dans lequel le message d'authentification, d'autorisation et de comptabilité comprend une identité internationale d'équipement mobile récupérée auprès de l'équipement utilisateur via le réseau d'accès WLAN de confiance, et une indication selon laquelle l'identité internationale d'équipement mobile doit être vérifiée par le registre d'identités d'équipements dans ledit réseau mobile terrestre public visité.

2. Serveur d'authentification, d'autorisation et de comptabilité selon la revendication 1, dans lequel la réception de la demande comprend la réception d'un message de protocole d'authentification extensible de diamètre d'authentification, d'autorisation et de comptabilité comprenant une indication selon laquelle l'identité internationale d'équipement mobile doit être vérifiée par le registre d'identités d'équipements dans ledit réseau mobile terrestre public visité, et dans lequel le message d'authentification, d'autorisation et de comptabilité comprend un message de protocole d'authentification extensible de diamètre d'authentification, d'autorisation et de comptabilité.

3. Serveur d'authentification, d'autorisation et de comptabilité selon la revendication 1 ou 2, configuré pour :
recevoir une indication d'une détermination quant à s'il faut poursuivre ou arrêter une procédure d'authentification et d'autorisation pour l'équipement utilisateur sur la base du résultat de la vérification de l'identité internationale d'équipement mobile par ledit registre d'identités d'équipements dans ledit réseau mobile terrestre public visité.

4. Mandataire d'authentification, d'autorisation et de comptabilité d'un coeur de paquet de projet de partenariat de troisième génération, configuré pour :

recevoir un premier message d'authentification, d'autorisation et de comptabilité d'un réseau d'accès WLAN de confiance, dans lequel le premier message d'authentification, d'autorisation et de comptabilité comprend une identité internationale d'équipement mobile récupérée auprès de l'équipement utilisateur via un serveur d'authentification, d'autorisation et de comptabilité pour l'équipement utilisateur dans un réseau mobile terrestre public domestique d'un coeur de paquet de projet de partenariat de troisième génération, et une indication selon laquelle l'identité internationale d'équipement mobile doit être vérifiée par un registre d'identités d'équipements dans un réseau mobile terrestre public visité pour l'équipement utilisateur ; et
envoyer un deuxième message d'authentification, d'autorisation et de comptabilité au serveur d'authentification, d'autorisation et de comptabilité pour l'équipement utilisateur, dans lequel le deuxième message d'authentification, d'autorisation et de comptabilité comprend une indication d'une détermination au niveau du mandataire d'authentification, d'autorisation et de comptabilité quant à s'il faut poursuivre ou arrêter une procédure d'authentification et d'autorisation au niveau du serveur d'authentification, d'autorisation et de comptabilité pour l'équipement utilisateur sur la base du résultat de la vérification de l'identité internationale d'équipement mobile par le registre d'identités d'équipements dans le réseau mobile terrestre public visité pour l'équipement utilisateur.

5. Mandataire d'authentification, d'autorisation et de comptabilité selon la revendication 4, dans lequel le premier message d'authentification, d'autorisation et de comptabilité comprend un message de protocole d'authentification extensible de diamètre d'authentification, d'autorisation et de comptabilité, et dans lequel le deuxième message d'authentification, d'autorisation et de comptabilité comprend un message de protocole d'authentification extensible de diamètre d'authentification, d'autorisation et de comptabilité

6. Procédé, comprenant :

au niveau d'un serveur d'authentification, d'autorisation et de comptabilité dans un réseau mobile terrestre public domestique d'un coeur de paquet de projet de partenariat de troisième génération pour un équipement utilisateur d'un réseau d'accès WLAN de confiance, la réception d'une demande de vérification d'une identité internationale d'équipement mobile de l'équipement utilisateur par un registre d'identités d'équipements dans un réseau mobile terrestre public visité pour l'équipement utilisateur, et
l'envoi d'un message d'authentification, d'autorisation et de comptabilité du serveur d'authentification, d'autorisation et de comptabilité au réseau d'accès WLAN de confiance, dans lequel le message d'authentification, d'autorisation et de comptabilité comprend une identité internationale d'équipement mobile récupérée auprès de l'équipement utilisateur via le réseau d'accès WLAN de confiance, et une indication selon laquelle l'identité internationale d'équipement mobile doit être vérifiée par le registre d'identités d'équipements dans ledit réseau mobile terrestre public visité.

7. Procédé selon la revendication 6, dans lequel la réception de la demande comprend la réception d'un message de protocole d'authentification extensible de diamètre d'authentification, d'autorisation et de comptabilité comprenant une indication selon laquelle l'identité internationale d'équipement mobile doit être vérifiée par le registre d'identités d'équipements dans ledit réseau mobile terrestre public visité ; et dans lequel le message d'authentification, d'autorisation et de comptabilité comprend un message de protocole d'authentification extensible de diamètre d'authentification, d'autorisation et de comptabilité.

8. Procédé selon la revendication 6 ou la revendication 7, comprenant :
au niveau du serveur d'authentification, d'autorisation et de comptabilité, la réception d'une indication d'une détermination quant à s'il faut poursuivre ou arrêter une procédure d'authentification et d'autorisation pour l'équipement utilisateur sur la base du résultat de la vérification de l'identité internationale d'équipement mobile par ledit registre d'identités d'équipements dans ledit réseau mobile terrestre public visité.

9. Procédé comprenant :

au niveau d'un mandataire d'authentification, d'autorisation et de comptabilité d'un coeur de paquet de projet de partenariat de troisième génération, la réception d'un premier message d'authentification, d'autorisation et de comptabilité d'une entité de réseau d'accès WLAN de confiance, dans lequel le premier message d'authentification, d'autorisation et de comptabilité comprend une identité internationale d'équipement mobile récupérée auprès de l'équipement utilisateur via un serveur d'authentification, d'autorisation et de comptabilité pour l'équipement utilisateur dans un réseau mobile terrestre public domestique d'un coeur de paquet de projet de partenariat de troisième génération, et une indication selon laquelle l'identité internationale d'équipement mobile doit être vérifiée par un registre d'identités d'équipements dans un réseau mobile terrestre public visité pour l'équipement utilisateur ; et
l'envoi d'un deuxième message d'authentification, d'autorisation et de comptabilité du mandataire d'authentification, d'autorisation et de comptabilité au serveur d'authentification, d'autorisation et de comptabilité pour l'équipement utilisateur dans le réseau mobile terrestre public domestique,
dans lequel le deuxième message d'authentification, d'autorisation et de comptabilité comprend une indication du résultat d'une détermination au niveau du mandataire d'authentification, d'autorisation et de comptabilité quant à s'il faut poursuivre ou arrêter une procédure d'authentification et d'autorisation au niveau du serveur d'authentification, d'autorisation et de comptabilité pour l'équipement utilisateur sur la base du résultat de la vérification de l'identité internationale d'équipement mobile par le registre d'identités d'équipements dans un réseau mobile terrestre public visité pour l'équipement utilisateur.

10. Procédé selon la revendication 9, dans lequel le premier message d'authentification, d'autorisation et de comptabilité comprend un message de protocole d'authentification extensible de diamètre d'authentification, d'autorisation et de comptabilité, et dans lequel le deuxième message d'authentification, d'autorisation et de comptabilité comprend un

message de protocole d'authentification extensible de diamètre d'authentification, d'autorisation et de comptabilité.

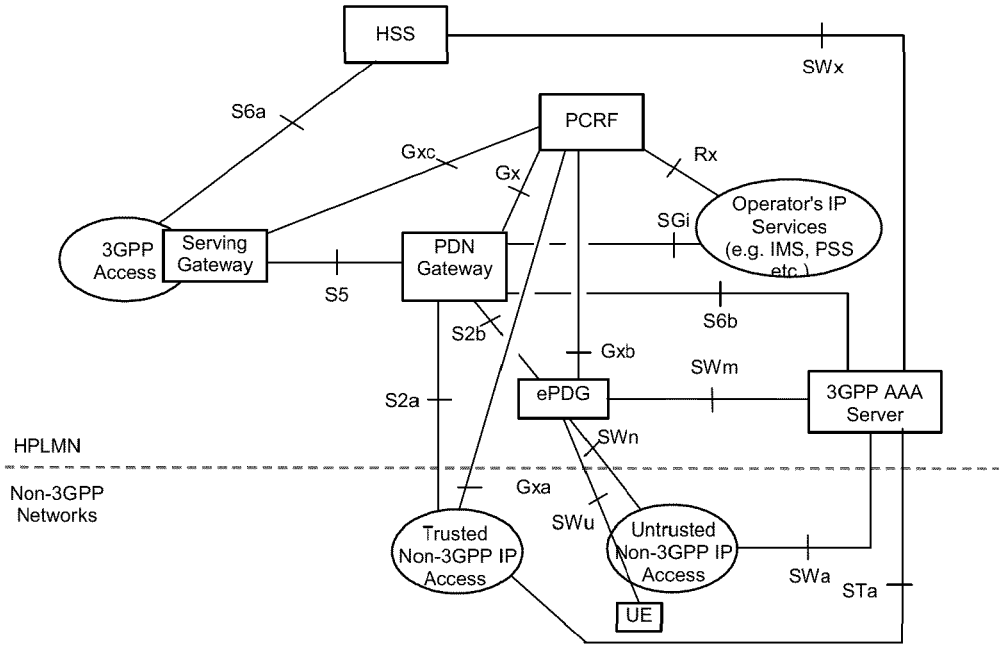
HSS
SWx
S6a
PCRF
Gxc
Rx
Gx
SGi
Operator's IP Services (e.g. IMS, PSS etc.)
3GPP Access
Serving Gateway
PDN Gateway
S5
S6b
S2b
Gxb
SWm
S2a
ePDG
3GPP AAA Server
SWn
HPLMN
Non-3GPP Networks
Gxa
SWu
Trusted Non-3GPP IP Access
Untrusted Non-3GPP IP Access
SWa
STa
UE

FIG. 1

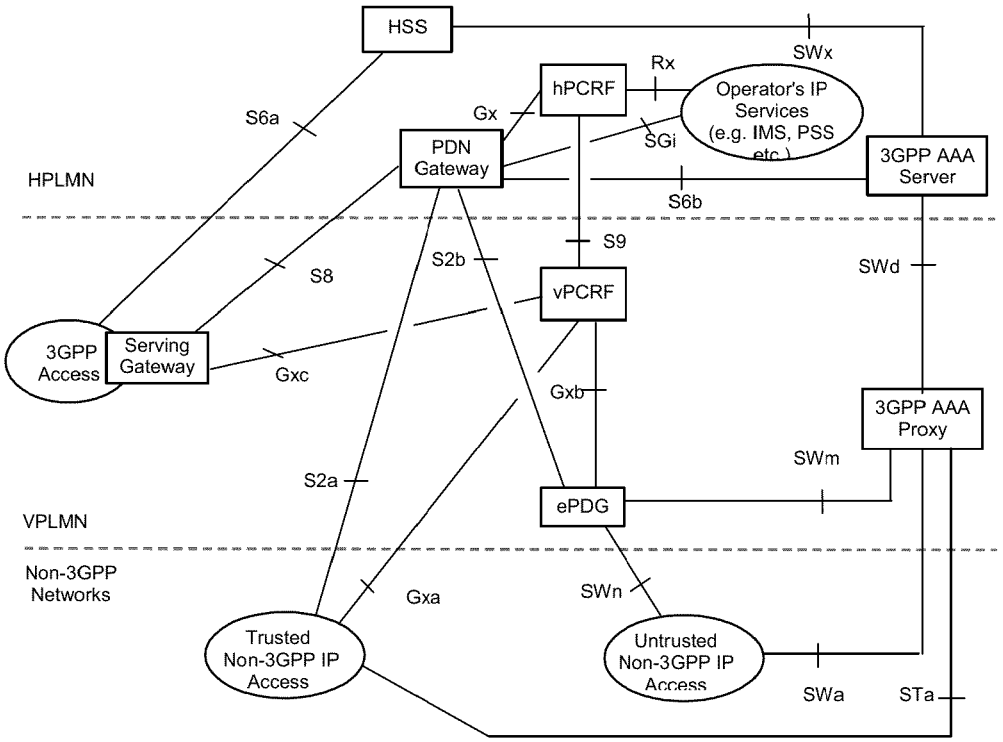
HSS
SWx
Rx
hPCRF
Operator's IP Services (e.g. IMS, PSS etc.)
S6a
Gx
SGi
PDN Gateway
3GPP AAA Server
HPLMN
S6b
S9
S2b
SWd
S8
vPCRF
3GPP Access
Serving Gateway
Gxc
Gxb
3GPP AAA Proxy
SWm
S2a
ePDG
VPLMN
Non-3GPP Networks
Gxa
SWn
Trusted Non-3GPP IP Access
Untrusted Non-3GPP IP Access
SWa
STa

FIG. 2

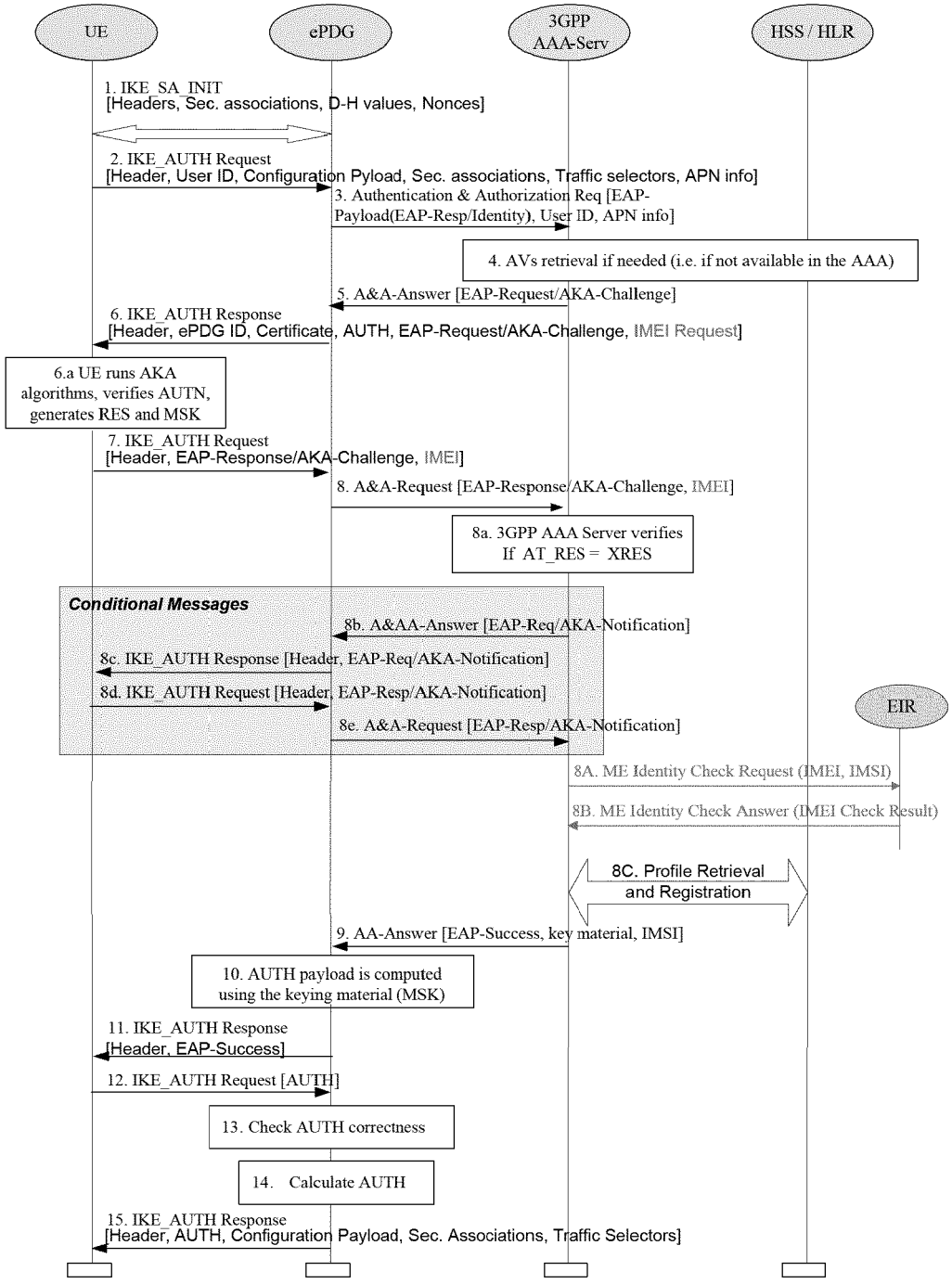
UE
ePDG
3GPP AAA-Serv
HSS / HLR
1. IKE_SA_INIT [Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request [Header, User ID, Configuration Pyload, Sec. associations, Traffic selectors, APN info]
3. Authentication & Authorization Req [EAP-Payload(EAP-Resp/Identity), User ID, APN info]
4. AVs retrieval if needed (i.e. if not available in the AAA)
5. A&A-Answer [EAP-Request/AKA-Challenge]
6. IKE_AUTH Response [Header, ePDG ID, Certificate, AUTH, EAP-Request/AKA-Challenge, IMEI Request]
6.a UE runs AKA algorithms, verifies AUTN, generates RES and MSK
7. IKE_AUTH Request [Header, EAP-Response/AKA-Challenge, IMEI]
8. A&A-Request [EAP-Response/AKA-Challenge, IMEI]
8a. 3GPP AAA Server verifies If AT_RES = XRES
Conditional Messages
8b. A&AA-Answer [EAP-Req/AKA-Notification]
8c. IKE_AUTH Response [Header, EAP-Req/AKA-Notification]
8d. IKE_AUTH Request [Header, EAP-Resp/AKA-Notification]
8e. A&A-Request [EAP-Resp/AKA-Notification]
EIR
8A. ME Identity Check Request (IMEI, IMSI)
8B. ME Identity Check Answer (IMEI Check Result)
8C. Profile Retrieval and Registration
9. AA-Answer [EAP-Success, key material, IMSI]
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response [Header, EAP-Success]
12. IKE_AUTH Request [AUTH]
13. Check AUTH correctness
14. Calculate AUTH
15. IKE_AUTH Response [Header, AUTH, Configuration Payload, Sec. Associations, Traffic Selectors]

FIG. 3

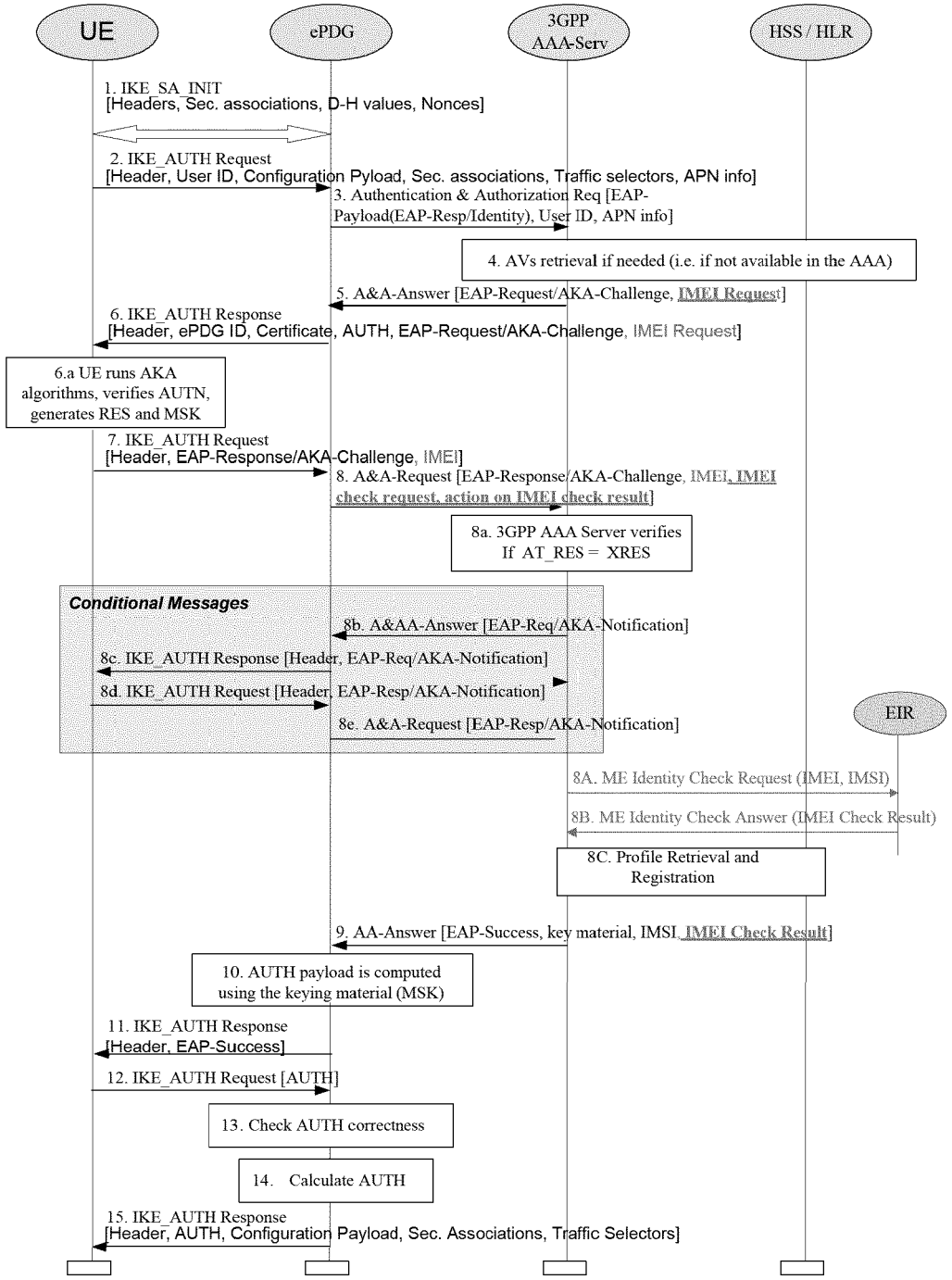
UE
ePDG
3GPP AAA-Serv
HSS / HLR
1. IKE_SA_INIT [Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request [Header, User ID, Configuration Pyload, Sec. associations, Traffic selectors, APN info]
3. Authentication & Authorization Req [EAP-Payload(EAP-Resp/Identity), User ID, APN info]
4. AVs retrieval if needed (i.e. if not available in the AAA)
5. A&A-Answer [EAP-Request/AKA-Challenge, IMEI Request]
6. IKE_AUTH Response [Header, ePDG ID, Certificate, AUTH, EAP-Request/AKA-Challenge, IMEI Request]
6.a UE runs AKA algorithms, verifies AUTN, generates RES and MSK
7. IKE_AUTH Request [Header, EAP-Response/AKA-Challenge, IMEI]
8. A&A-Request [EAP-Response/AKA-Challenge, IMEI, IMEI check request, action on IMEI check result]
8a. 3GPP AAA Server verifies If AT_RES = XRES
Conditional Messages
8b. A&AA-Answer [EAP-Req/AKA-Notification]
8c. IKE_AUTH Response [Header, EAP-Req/AKA-Notification]
8d. IKE_AUTH Request [Header, EAP-Resp/AKA-Notification]
8e. A&A-Request [EAP-Resp/AKA-Notification]
EIR
8A. ME Identity Check Request (IMEI, IMSI)
8B. ME Identity Check Answer (IMEI Check Result)
8C. Profile Retrieval and Registration
9. AA-Answer [EAP-Success, key material, IMSI, IMEI Check Result]
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response [Header, EAP-Success]
12. IKE_AUTH Request [AUTH]
13. Check AUTH correctness
14. Calculate AUTH
15. IKE_AUTH Response [Header, AUTH, Configuration Payload, Sec. Associations, Traffic Selectors]

FIG. 4

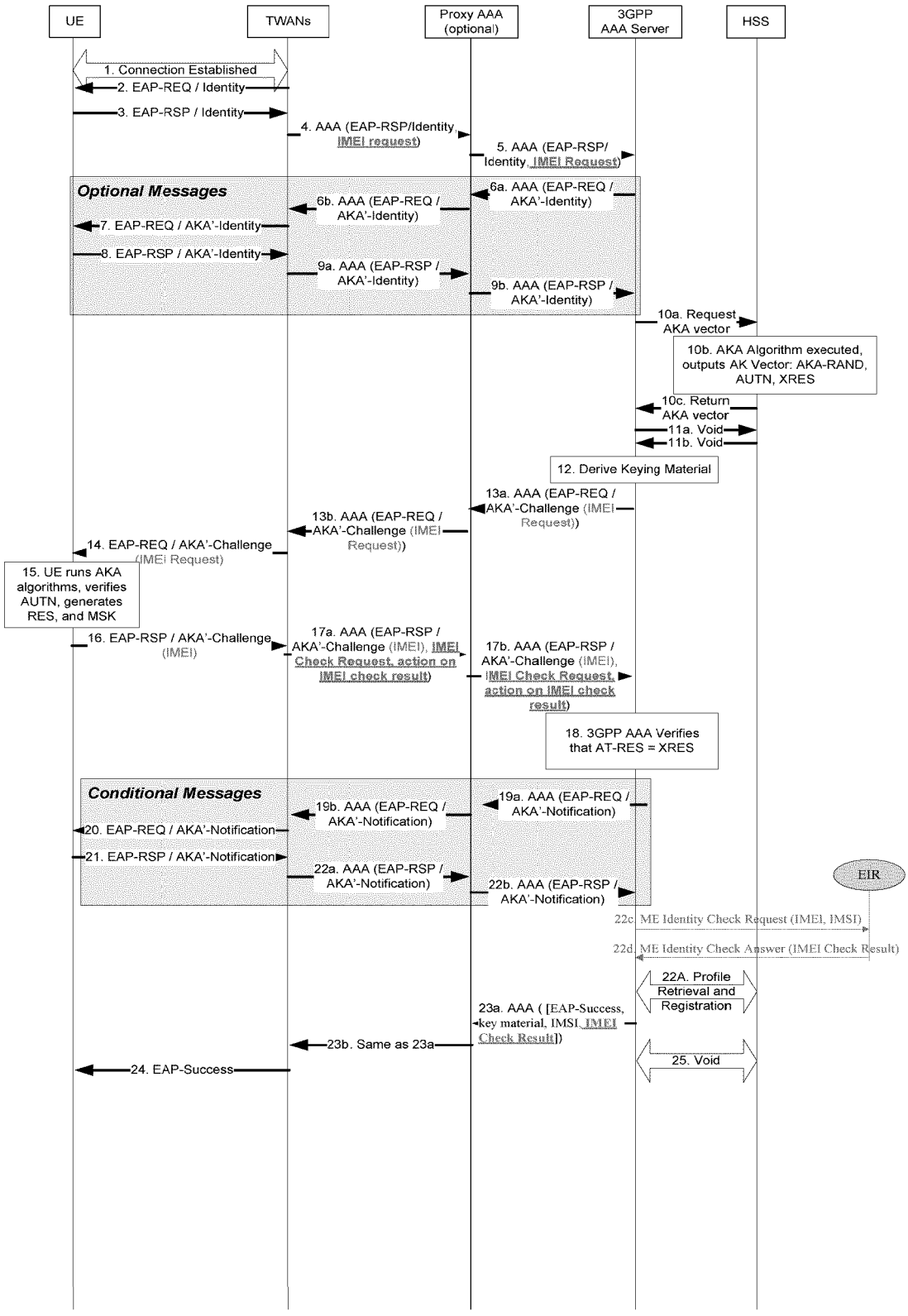
UE
TWANs
Proxy AAA (optional)
3GPP AAA Server
HSS
1. Connection Established
2. EAP-REQ / Identity
3. EAP-RSP / Identity
4. AAA (EAP-RSP/Identity IMEI request)
5. AAA (EAP-RSP/ Identity, IMEI Request)
Optional Messages
6a. AAA (EAP-REQ / AKA'-Identity)
6b. AAA (EAP-REQ / AKA'-Identity)
7. EAP-REQ / AKA'-Identity
8. EAP-RSP / AKA'-Identity
9a. AAA (EAP-RSP / AKA'-Identity)
9b. AAA (EAP-RSP / AKA'-Identity)
10a. Request AKA vector
10b. AKA Algorithm executed, outputs AK Vector: AKA-RAND, AUTN, XRES
10c. Return AKA vector
11a. Void
11b. Void
12. Derive Keying Material
13a. AAA (EAP-REQ / AKA'-Challenge (IMEI Request))
13b. AAA (EAP-REQ / AKA'-Challenge (IMEI Request))
14. EAP-REQ / AKA'-Challenge (IMEI Request)
15. UE runs AKA algorithms, verifies AUTN, generates RES, and MSK
16. EAP-RSP / AKA'-Challenge (IMEI)
17a. AAA (EAP-RSP / AKA'-Challenge (IMEI), IMEI Check Request, action on IMEI check result)
17b. AAA (EAP-RSP / AKA'-Challenge (IMEI), IMEI Check Request, action on IMEI check result)
18. 3GPP AAA Verifies that AT-RES = XRES
Conditional Messages
19a. AAA (EAP-REQ / AKA'-Notification)
19b. AAA (EAP-REQ / AKA'-Notification)
20. EAP-REQ / AKA'-Notification
21. EAP-RSP / AKA'-Notification
22a. AAA (EAP-RSP / AKA'-Notification)
22b. AAA (EAP-RSP / AKA'-Notification)
EIR
22c. ME Identity Check Request (IMEI, IMSI)
22d. ME Identity Check Answer (IMEI Check Result)
22A. Profile Retrieval and Registration
23a. AAA ([EAP-Success, key material, IMSI, IMEI Check Result])
23b. Same as 23a
25. Void
24. EAP-Success

FIG. 5

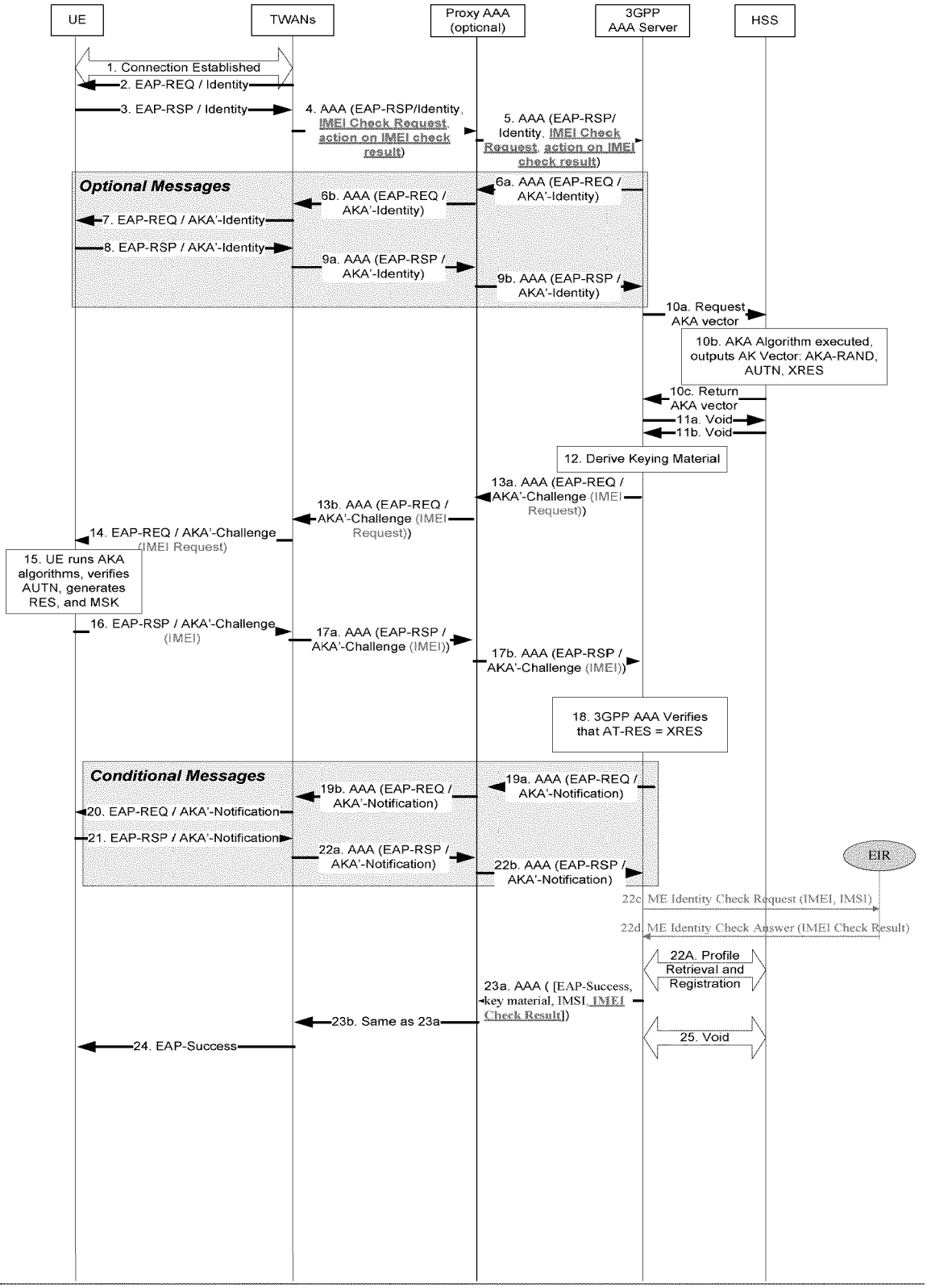
UE
TWANs
Proxy AAA (optional)
3GPP AAA Server
HSS
1. Connection Established
2. EAP-REQ / Identity
3. EAP-RSP / Identity
4. AAA (EAP-RSP/Identity, IMEI Check Request, action on IMEI check result)
5. AAA (EAP-RSP/ Identity, IMEI Check Request, action on IMEI check result)
Optional Messages
6a. AAA (EAP-REQ / AKA'-Identity)
6b. AAA (EAP-REQ / AKA'-Identity)
7. EAP-REQ / AKA'-Identity
8. EAP-RSP / AKA'-Identity
9a. AAA (EAP-RSP / AKA'-Identity)
9b. AAA (EAP-RSP / AKA'-Identity)
10a. Request AKA vector
10b. AKA Algorithm executed, outputs AK Vector: AKA-RAND, AUTN, XRES
10c. Return AKA vector
11a. Void
11b. Void
12. Derive Keying Material
13a. AAA (EAP-REQ / AKA'-Challenge (IMEI Request))
13b. AAA (EAP-REQ / AKA'-Challenge (IMEI Request))
14. EAP-REQ / AKA'-Challenge (IMEI Request)
15. UE runs AKA algorithms, verifies AUTN, generates RES, and MSK
16. EAP-RSP / AKA'-Challenge (IMEI)
17a. AAA (EAP-RSP / AKA'-Challenge (IMEI))
17b. AAA (EAP-RSP / AKA'-Challenge (IMEI))
18. 3GPP AAA Verifies that AT-RES = XRES
Conditional Messages
19a. AAA (EAP-REQ / AKA'-Notification)
19b. AAA (EAP-REQ / AKA'-Notification)
20. EAP-REQ / AKA'-Notification
21. EAP-RSP / AKA'-Notification
22a. AAA (EAP-RSP / AKA'-Notification)
22b. AAA (EAP-RSP / AKA'-Notification)
EIR
22c. ME Identity Check Request (IMEI, IMSI)
22d. ME Identity Check Answer (IMEI Check Result)
22A. Profile Retrieval and Registration
23a. AAA ([EAP-Success, key material, IMSI, IMEI Check Result])
23b. Same as 23a
25. Void
24. EAP-Success

FIG. 6

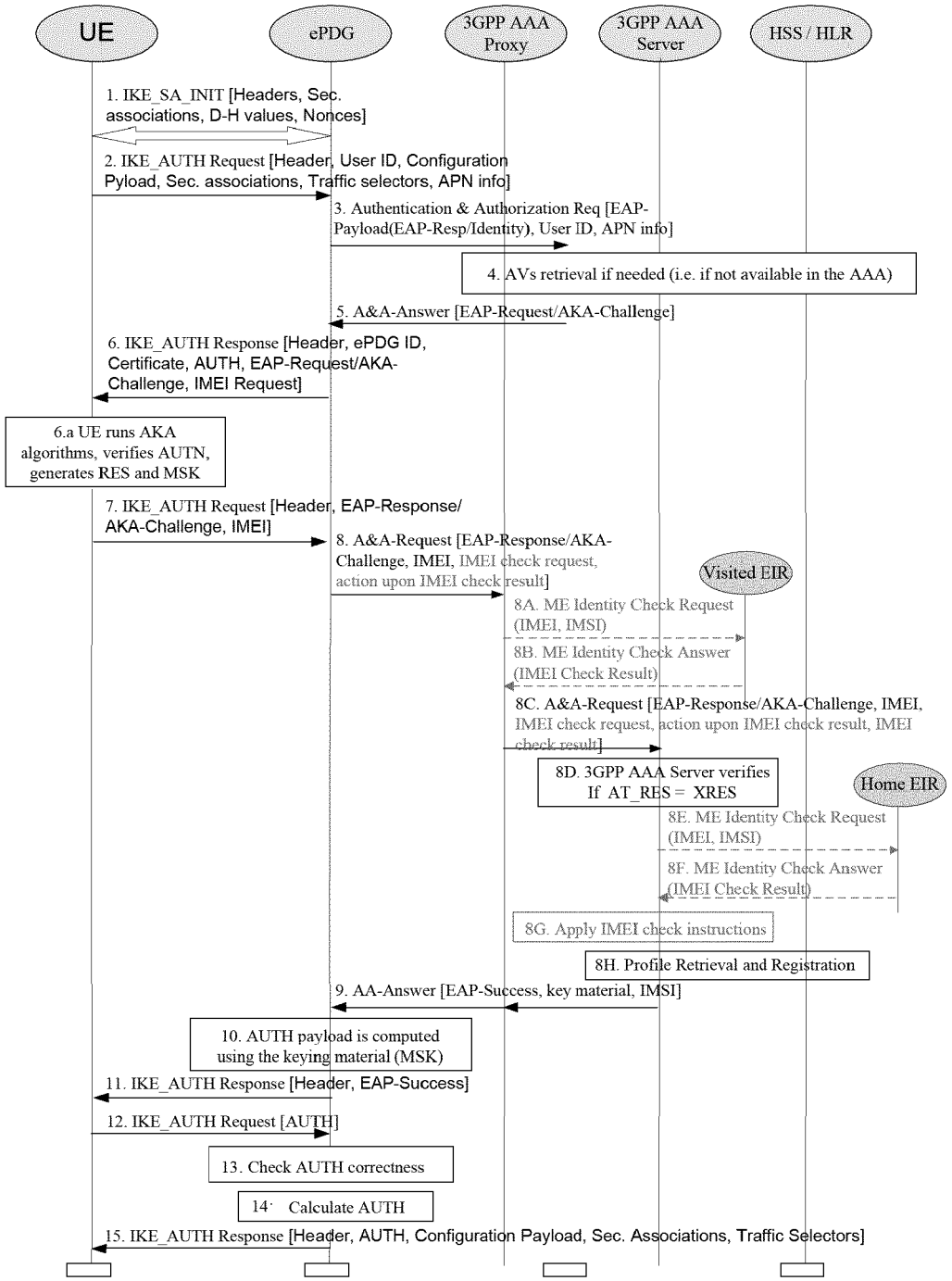
UE
ePDG
3GPP AAA Proxy
3GPP AAA Server
HSS / HLR
1. IKE_SA_INIT [Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request [Header, User ID, Configuration Pyload, Sec. associations, Traffic selectors, APN info]
3. Authentication & Authorization Req [EAP-Payload(EAP-Resp/Identity), User ID, APN info]
4. AVs retrieval if needed (i.e. if not available in the AAA)
5. A&A-Answer [EAP-Request/AKA-Challenge]
6. IKE_AUTH Response [Header, ePDG ID, Certificate, AUTH, EAP-Request/AKA-Challenge, IMEI Request]
6.a UE runs AKA algorithms, verifies AUTN, generates RES and MSK
7. IKE_AUTH Request [Header, EAP-Response/ AKA-Challenge, IMEI]
8. A&A-Request [EAP-Response/AKA-Challenge, IMEI, IMEI check request, action upon IMEI check result]
Visited EIR
8A. ME Identity Check Request (IMEI, IMSI)
8B. ME Identity Check Answer (IMEI Check Result)
8C. A&A-Request [EAP-Response/AKA-Challenge, IMEI, IMEI check request, action upon IMEI check result, IMEI check result]
8D. 3GPP AAA Server verifies If AT_RES = XRES
Home EIR
8E. ME Identity Check Request (IMEI, IMSI)
8F. ME Identity Check Answer (IMEI Check Result)
8G. Apply IMEI check instructions
8H. Profile Retrieval and Registration
9. AA-Answer [EAP-Success, key material, IMSI]
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response [Header, EAP-Success]
12. IKE_AUTH Request [AUTH]
13. Check AUTH correctness
14. Calculate AUTH
15. IKE_AUTH Response [Header, AUTH, Configuration Payload, Sec. Associations, Traffic Selectors]

FIG. 7

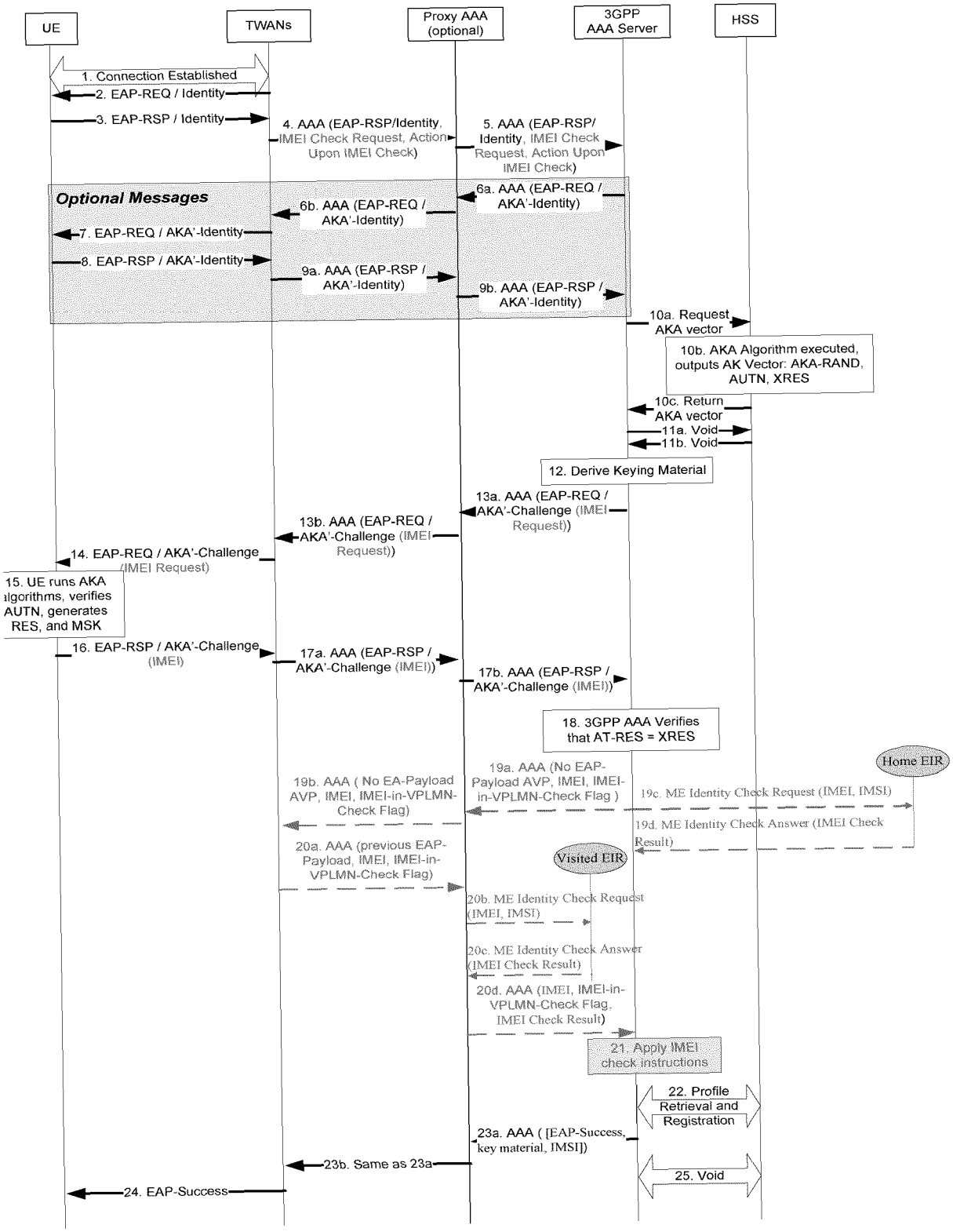
UE
TWANs
Proxy AAA (optional)
3GPP AAA Server
HSS
1. Connection Established
2. EAP-REQ / Identity
3. EAP-RSP / Identity
4. AAA (EAP-RSP/Identity, IMEI Check Request, Action Upon IMEI Check)
5. AAA (EAP-RSP/ Identity, IMEI Check Request, Action Upon IMEI Check)
Optional Messages
6a. AAA (EAP-REQ / AKA'-Identity)
6b. AAA (EAP-REQ / AKA'-Identity)
7. EAP-REQ / AKA'-Identity
8. EAP-RSP / AKA'-Identity
9a. AAA (EAP-RSP / AKA'-Identity)
9b. AAA (EAP-RSP / AKA'-Identity)
10a. Request AKA vector
10b. AKA Algorithm executed, outputs AK Vector: AKA-RAND, AUTN, XRES
10c. Return AKA vector
11a. Void
11b. Void
12. Derive Keying Material
13a. AAA (EAP-REQ / AKA'-Challenge (IMEI Request))
13b. AAA (EAP-REQ / AKA'-Challenge (IMEI Request))
14. EAP-REQ / AKA'-Challenge (IMEI Request)
15. UE runs AKA algorithms, verifies AUTN, generates RES, and MSK
16. EAP-RSP / AKA'-Challenge (IMEI)
17a. AAA (EAP-RSP / AKA'-Challenge (IMEI))
17b. AAA (EAP-RSP / AKA'-Challenge (IMEI))
18. 3GPP AAA Verifies that AT-RES = XRES
Home EIR
19a. AAA (No EAP-Payload AVP, IMEI, IMEI-in-VPLMN-Check Flag)
19b. AAA (No EA-Payload AVP, IMEI, IMEI-in-VPLMN-Check Flag)
19c. ME Identity Check Request (IMEI, IMSI)
19d. ME Identity Check Answer (IMEI Check Result)
Visited EIR
20a. AAA (previous EAP-Payload, IMEI, IMEI-in-VPLMN-Check Flag)
20b. ME Identity Check Request (IMEI, IMSI)
20c. ME Identity Check Answer (IMEI Check Result)
20d. AAA (IMEI, IMEI-in-VPLMN-Check Flag, IMEI Check Result)
21. Apply IMEI check instructions
22. Profile Retrieval and Registration
23a. AAA ([EAP-Success, key material, IMSI])
23b. Same as 23a
25. Void
24. EAP-Success

FIG. 8

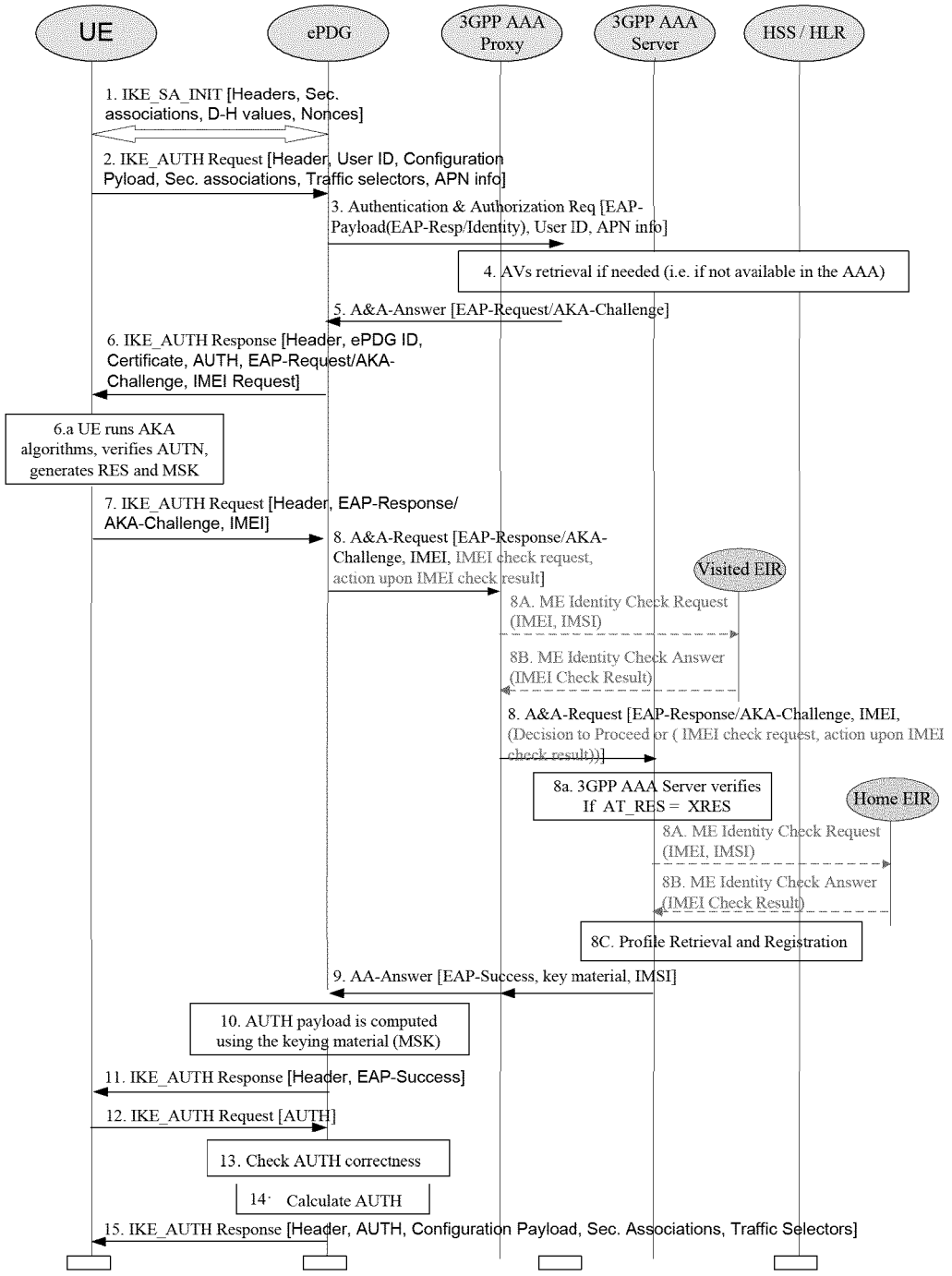
UE
ePDG
3GPP AAA Proxy
3GPP AAA Server
HSS / HLR
1. IKE_SA_INIT [Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request [Header, User ID, Configuration Pyload, Sec. associations, Traffic selectors, APN info]
3. Authentication & Authorization Req [EAP-Payload(EAP-Resp/Identity), User ID, APN info]
4. AVs retrieval if needed (i.e. if not available in the AAA)
5. A&A-Answer [EAP-Request/AKA-Challenge]
6. IKE_AUTH Response [Header, ePDG ID, Certificate, AUTH, EAP-Request/AKA-Challenge, IMEI Request]
6.a UE runs AKA algorithms, verifies AUTN, generates RES and MSK
7. IKE_AUTH Request [Header, EAP-Response/ AKA-Challenge, IMEI]
8. A&A-Request [EAP-Response/AKA-Challenge, IMEI, IMEI check request, action upon IMEI check result]
Visited EIR
8A. ME Identity Check Request (IMEI, IMSI)
8B. ME Identity Check Answer (IMEI Check Result)
8. A&A-Request [EAP-Response/AKA-Challenge, IMEI, (Decision to Proceed or (IMEI check request, action upon IMEI check result))]
8a. 3GPP AAA Server verifies If AT_RES = XRES
Home EIR
8A. ME Identity Check Request (IMEI, IMSI)
8B. ME Identity Check Answer (IMEI Check Result)
8C. Profile Retrieval and Registration
9. AA-Answer [EAP-Success, key material, IMSI]
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response [Header, EAP-Success]
12. IKE_AUTH Request [AUTH]
13. Check AUTH correctness
14. Calculate AUTH
15. IKE_AUTH Response [Header, AUTH, Configuration Payload, Sec. Associations, Traffic Selectors]

FIG. 9

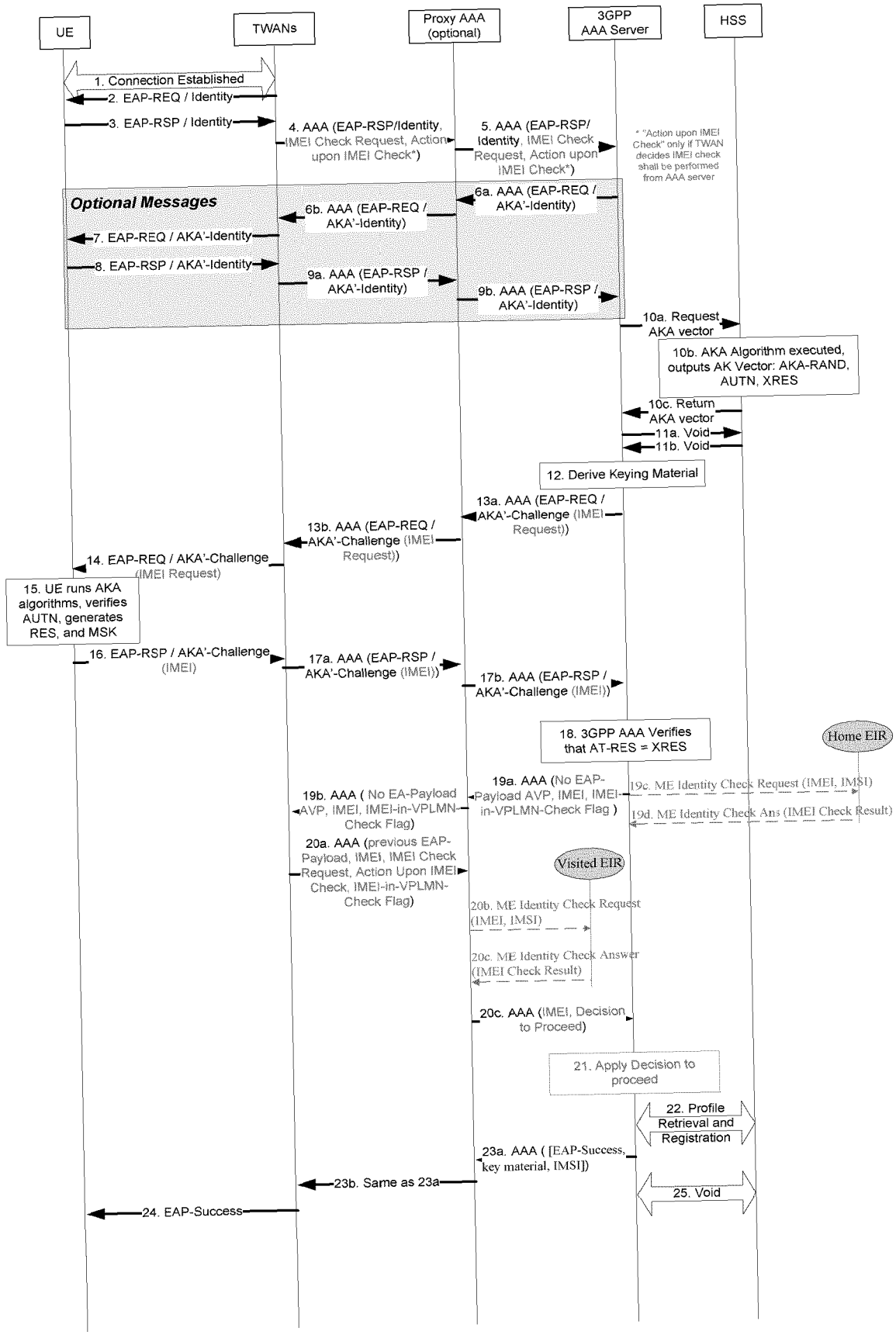
UE
TWANs
Proxy AAA (optional)
3GPP AAA Server
HSS
1. Connection Established
2. EAP-REQ / Identity
3. EAP-RSP / Identity
4. AAA (EAP-RSP/Identity, IMEI Check Request, Action upon IMEI Check*)
5. AAA (EAP-RSP/ Identity, IMEI Check Request, Action upon IMEI Check*)
* "Action upon IMEI Check" only if TWAN decides IMEI check shall be performed from AAA server
Optional Messages
6a. AAA (EAP-REQ / AKA'-Identity)
6b. AAA (EAP-REQ / AKA'-Identity)
7. EAP-REQ / AKA'-Identity
8. EAP-RSP / AKA'-Identity
9a. AAA (EAP-RSP / AKA'-Identity)
9b. AAA (EAP-RSP / AKA'-Identity)
10a. Request AKA vector
10b. AKA Algorithm executed, outputs AK Vector: AKA-RAND, AUTN, XRES
10c. Return AKA vector
11a. Void
11b. Void
12. Derive Keying Material
13a. AAA (EAP-REQ / AKA'-Challenge (IMEI Request))
13b. AAA (EAP-REQ / AKA'-Challenge (IMEI Request))
14. EAP-REQ / AKA'-Challenge (IMEI Request)
15. UE runs AKA algorithms, verifies AUTN, generates RES, and MSK
16. EAP-RSP / AKA'-Challenge (IMEI)
17a. AAA (EAP-RSP / AKA'-Challenge (IMEI))
17b. AAA (EAP-RSP / AKA'-Challenge (IMEI))
18. 3GPP AAA Verifies that AT-RES = XRES
Home EIR
19a. AAA (No EAP-Payload AVP, IMEI, IMEI-in-VPLMN-Check Flag)
19b. AAA (No EA-Payload AVP, IMEI, IMEI-in-VPLMN-Check Flag)
19c. ME Identity Check Request (IMEI, IMSI)
19d. ME Identity Check Ans (IMEI Check Result)
20a. AAA (previous EAP-Payload, IMEI, IMEI Check Request, Action Upon IMEI Check, IMEI-in-VPLMN-Check Flag)
Visited EIR
20b. ME Identity Check Request (IMEI, IMSI)
20c. ME Identity Check Answer (IMEI Check Result)
20c. AAA (IMEI, Decision to Proceed)
21. Apply Decision to proceed
22. Profile Retrieval and Registration
23a. AAA ([EAP-Success, key material, IMSI])
23b. Same as 23a
25. Void
24. EAP-Success

FIG. 10

REFERENCES CITED IN THE DESCRIPTION

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

Patent documents cited in the description

- WO 2010013914 A **[0011]**