ETSI TS 133 402 V19.0.0 (2025-10)

TECHNICAL SPECIFICATION

**Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
3GPP System Architecture Evolution (SAE);
Security aspects of non-3GPP accesses
(3GPP TS 33.402 version 19.0.0 Release 19)**

Reference
RTS/TSGS-0333402vj00

Keywords
GSM,LTE,SECURITY,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document specifies the security architecture, i.e., the security feature groups and the security mechanisms performed during inter working between non-3GPP accesses and the Evolved Packet System (EPS).

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] IETF RFC 4877: "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture".

[3] Void.

[4] IETF RFC 5778: "Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction".

[5] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[6] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[7] IETF RFC 4187 (January 2006): "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".

[8] 3GPP TS 23.003: "Numbering, addressing and identification".

[9] 3GPP TS 33.234: "3G: security; Wireless Local Area Network (WLAN) interworking security" (Release 12).

[10] IETF RFC 4072 (August 2005): "Diameter Extensible Authentication Protocol (EAP) Application".

[11] 3GPP TS 33.102: "3G security; Security architecture".

[12] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[13] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[14] 3GPP TS 23.203: "Policy and charging control architecture".

[15] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Overall description; Stage 2".

[16] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security Architecture".

[17] IETF RFC 3344: "IP Mobility Support for IPv4".

[18] IETF RFC 4555: "IKEv2 Mobility and Multihoming Protocol (MOBIKE)".

[19] IETF RFC 5295: "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)".

[20] 3GPPP TS 24.303: "Mobility Management based on Dual-Stack Mobile IPv6; Stage 3".

[21] IETF RFC 4433: "Mobile IPv4 Dynamic Home Agent (HA) Assignment".

[22] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3 ".

[23] IETF RFC 5448: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA') ".

[24] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[25] 3GPP TS 29.109: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3".

[26] - [28] Void.

[29] 3GPP TS 33.223: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function".

[30] IETF RFC 5996: "Internet Key Exchange Protocol Version 2 (IKEv2)".

[31] 3GPP TS 29.274: "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3".

[32] 3GPP TS 29.275: "Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols; Stage 3".

[33] IETF RFC 4739: "Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2) Protocol".

[34] 3GPP TS 33.203: "Access security for IP-based services".

[35] IETF RFC 3948: "UDP Encapsulation of IPsec ESP Packets".

[36] IETF RFC 2616: "Hypertext Transfer Protocol -- HTTP/1.1".

[37] IETF RFC 6347: "Datagram Transport Layer Security Version 1.2".

[38] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[39] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[40] Federal Information Processing Standard (FIPS) draft standard: "Advanced Encryption Standard (AES)", November 2001.

[41] RFC 1421, February 1993: "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures".

[42] Open Mobile Alliance OMA-WAP-OCSP V1.0: "Online Certificate Status Protocol Mobile Profile". URL: http://www.openmobilealliance.org/

[43] IETF RFC 4806, Februari 2007: Online Certificate Status Protocol ("OCS)P Extensions to IKEv2".

[44] IETF RFC 4282, December 2005: "The Network Access Identifier", (Obsoletes RFC2486)

[45] IETF RFC 2865, June 2000: "Remote Authentication Dial In User Service (RADIUS)".

[46] IETF RFC 6696: "EAP Extensions for the EAP Re-authentication Protocol (ERP)".

[47] IETF RFC 6942: "Diameter Support for the EAP Re-authentication Protocol (ERP)".

[48] 3GPP TS 24.502: "Access to the 3GPP 5G System (5GS) via non-3GPP access networks; Stage 3".

[49] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

IPsec Security Association (IPsec SA): A unidirectional logical connection created for security purposes. All traffic traversing an IPsec SA is provided the same security protection. The IPsec SA itself is a set of parameters to define security protection between two entities. An IPsec SA includes the cryptographic algorithms, the keys, the duration of the keys, and other parameters.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

S2a This interface is defined in TS 23.402 [5].
S7a Interface between a PCRF and a HS-GW
S101 Interface between a MME and a HRPD AN
S103 Interface between a SGW and a HS-GW

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

AAA Authentication Authorisation Accounting
AES Advanced Encryption Standard
AKA Authentication and Key Agreement
ANDSF Access Network Discovery and Selection Function
DSMIPv6 Dual-Stack MIPv6
EAP Extensible Authentication Protocol
EMSK Extended Master Session Key
EPC Evolved Packet Core
ePDG Evolved Packet Data Gateway
EPS Evolved Packet System
ERP EAP Re-authentication Protocol
ESP Encapsulating Security Payload
E-UTRAN Evolved UTRAN
HS-GW HRPD Serving GW
IKEv2 Internet Key Exchange Version 2
IPsec IP security protocols, algorithms, and key management methods
LMA Local Mobility Anchor
MAG Mobile Access Gateway
MIPv4 Mobile IP version 4
MIPv6 Mobile IP version 6
MME Mobility Management Entity
MSK Master Session Key
NDS Network Domain Security
NDS/IP NDS for IP based protocols
PMIP/PMIPv6 Proxy Mobile IP version 6
rIK re-authentication Integrity Key
rMSK re-authentication Master Session Key
rRK re-authentication Root Key

SA	Security Association
TWAN	Trusted WLAN Access Network
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module

3.4 Conventions

All data variables in the present document are presented with the most significant substring on the left hand side and the least significant substring on the right hand side. A substring may be a bit, byte or other arbitrary length bitstring. Where a variable is broken down into a number of substrings, the leftmost (most significant) substring is numbered 0, the next most significant is numbered 1, and so on through to the least significant.

4 Overview of Security Architecture for non-3GPP Accesses to EPS

4.1 General

The following subclauses outline an overview of the security architecture for trusted and untrusted non-3GPP accesses to connect to 3GPP EPS. It outlines the needed security features to connect such a non-3GPP access to the 3GPP EPS. Non-3GPP access specific security is outside the scope of the present document.

Figure 4.1-1 gives an overview of the security architecture of a typical non-3GPP access while connected to the 3GPP EPC.

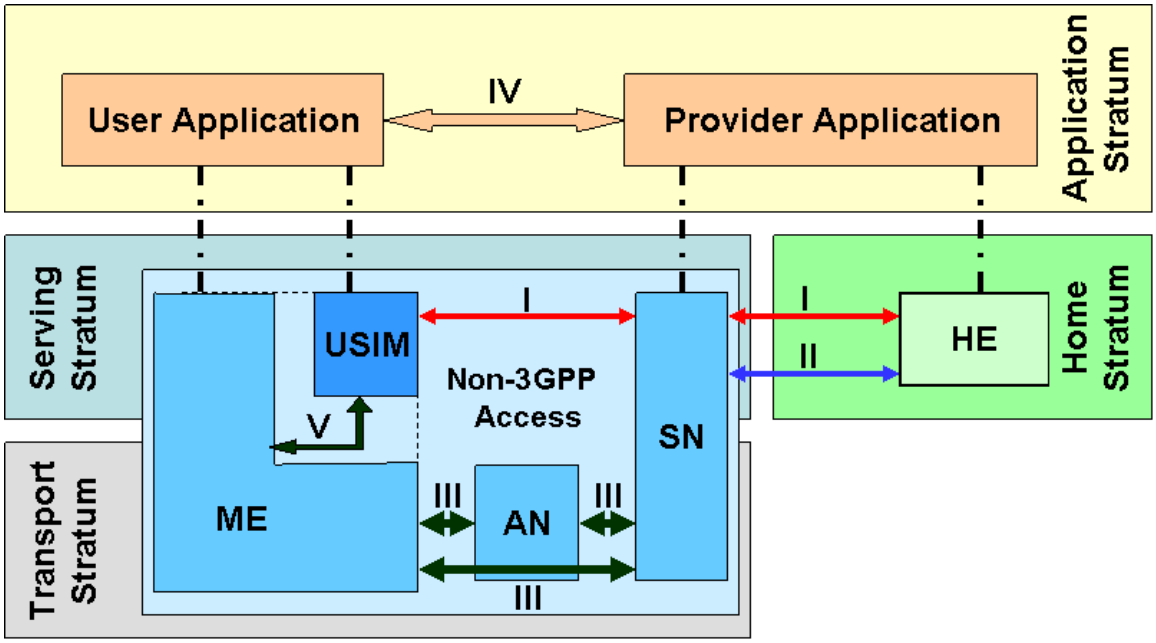

Figure 4.1-1: Security Architecture of Non-3GPP Access and 3GPP EPS

NOTE: USIM applies in case of terminal with 3GPP access capabilities, cf. clause 6.1.

Five security feature groups are defined. Each of these feature groups accomplishes certain security objectives:

- **Network access security (I):** the set of security features that provide users with secure access to services while terminated at 3GPP EPC. Radio Access protection is a non-3GPP access specific and outside the scope of the present document.

- **Network domain security (II):** the set of security features that enable nodes to securely exchange signaling data, and protect against attacks on the wireline network.

- **Non-3GPP domain security (III):** the set of security features are a non-3GPP access specific and outside the scope of the present document.
- **Application domain security (IV):** the set of security features that enable applications in the user and in the provider domain to securely exchange messages.
- **User domain security (V)**: the set of security features that secure access to the mobile station. If the terminal does not support 3GPP access capabilities, 3GPP does not specify how user domain security is achieved.

4.2 Trusted non-3GPP Access

As defined in clause 4.3.1.2 of TS 23.402[5] it is the home operator policy decision if a non-3GPP access network is treated as trusted non-3GPP access network.When all of the security feature groups provided by the non-3GPP access network are considered sufficiently secure by the home operator, the non-3GPP access may be identified as a trusted non-3GPP access for that operator. However, this policy decision may additionally be based on reasons not related to security feature groups.

NOTE: It is specified in clause 6.1 of the current specification how the UE gets the operator policy and how it will behave accordingly

4.3 Untrusted non-3GPP Access

As defined in clause 4.3.1.2 of TS 23.402[5] it is the home operator policy decision if a non-3GPP access network is treated as untrusted non-3GPP access network. When one or more of the security feature groups provided by the non-3GPP access network are considered not sufficiently secure by the home operator, the non-3GPP access may be identified as an untrusted non-3GPP access for that operator. However, this policy decision may additionally be based on reasons not related to security feature groups.

NOTE: It is specified in clause 6.1 of the current specification how the UE gets the operator policy and how it will behave accordingly.

5 Security Features Provided by EPS for non-3GPP Accesses

5.1 User-to-Network security

5.1.1 User identity and device identity confidentiality

User identity confidentiality for procedures between the UE and the Evolved Packet Core is provided as defined in clauses 6, 8 and 9 of the present document.

The protection of user identity confidentiality at the non-3GPP access network level is outside the scope of 3GPP specifications.

Device identity confidentiality is outside the scope of 3GPP specifications.

5.1.2 Entity authentication

Entity authentication is provided as defined in clauses 6, 8 and 9 of the present document.

5.2 User data and signalling data confidentiality

Signaling data confidentiality between the UE and an entity in the Evolved Packet Core is provided as defined in clauses 6, 8 and 9 of the present document.

Optionally, user data confidentiality between the UE and the PDN GW is provided as defined in clause 9.2.2 of the present document when DS-MIPv6 is used,

The establishment of security contexts for user data and signaling data confidentiality between the UE and an entity in a non-3GPP access network is defined in clause 7 of the present document. The detailed definition of the corresponding confidentiality mechanisms is, however, outside the scope of 3GPP specifications.

Signaling data confidentiality between an entity in the non-3GPP access network and an entity in the Evolved Packet Core, or between two entities in the Evolved Packet Core, is provided as defined in clause 11 (Network Domain Security) of the present document.

User data and signaling data confidentiality between two entities in a non-3GPP access network is outside the scope of 3GPP specifications.

5.3 User data and signalling data integrity

Signaling data integrity between the UE and an entity in the Evolved Packet Core is provided as defined in clauses 6, 8 and 9 of the present document.

Optionally, user data integrity between the UE and the PDN GW is provided as defined in clause 9.2.2 of the present document when DS-MIPv6 is used,

The establishment of security contexts for user data and signaling data integrity between the UE and an entity in a non-3GPP access network is defined in clause 7 of the present document. The detailed definition of the corresponding integrity mechanisms is, however, outside the scope of 3GPP specifications.

Signaling data integrity between an entity in the non-3GPP access network and an entity in the Evolved Packet Core, or between two entities in the Evolved Packet Core, is provided as defined in clause 11 (Network Domain Security) of the present document.

User data and signaling data integrity between two entities in a non-3GPP access network is outside the scope of 3GPP specifications.

6 Authentication and key agreement procedures

6.1 General

Access authentication for non-3GPP access in EPS shall be based on EAP-AKA (RFC 4187 [7]) or on EAP-AKA' (RFC 5448 [23]).

NOTE: It follows from the preceding sentence in particular that access authentication for non-3GPP access in EPS using EAP-SIM is not allowed.

The EAP server for EAP-AKA and EAP-AKA' shall be the 3GPP AAA server residing in the EPC.

The UE and 3GPP AAA server shall implement both EAP-AKA and EAP-AKA'. It is specified in this specification in which cases EAP-AKA and EAP-AKA' respectively shall be used.

If the terminal supports 3GPP access capabilities, the credentials used with EAP-AKA and EAP-AKA' shall reside on the UICC.

If the terminal does not support 3GPP access capabilities, 3GPP does not specify where the credentials used with EAP-AKA and EAP-AKA' reside.

NOTE: EAP-AKA and EAP-AKA' may use the same credentials.

The procedure in clause 6.2 shall be performed whenever the procedure in clause 8 of the present document is not performed with the following exception:

- if the security procedure in clause 9.2.2.2 for DS-MIPv6 is performed over a trusted access network and
- if the trusted access network has the properties listed in clause 9.2.2.1

then the procedure in clause 6.2 may be skipped.

However, it is recommended to use the procedure in clause 6.2 unless another strong authentication and key establishment method is used, which is documented in a standard covering the non-3GPP access network.

NOTE 1: There are cases when the procedure in clause 6.2 cannot be performed due to lack of support for EAP in the access network. DSL-based access networks are examples of such access networks.

In cases where it is difficult to assess whether a given access network has the properties listed in clauses 9.2.2.1 and 9.3.1.2, it is strongly recommended to use the procedures for untrusted access in clause 8.

The HSS shall send an authentication vector with AMF separation bit = 1 (cf. TS 33.401 [16]) to a 3GPP AAA server as specified for the EAP-AKA' procedures defined in the present document. For authentication vectors with the "separation bit" set to 1, the secret keys CK and IK generated during AKA shall never leave the HSS, and shall not be used in a non-EPS context.

The non-3GPP access networks, which are trusted, can be pre-configured in the UE. The UE can e.g. have a list with non-3GPP access technologies, or access networks, or serving network operators that allow procedures for trusted non-3GPP IP access. Additionally, during 3GPP-based access authentication the UE may receive an indication whether the non-3GPP IP access is trusted or not. If such an indication is sent it shall be sent by the 3GPP AAA server as part of an EAP-AKA or EAP-AKA' request. If no such indication is received by the UE, and there is no pre-configured information in the UE, the UE shall consider the non-3GPP IP access as untrusted. In case of pre-configured information and indication received as part of an EAP-AKA or EAP-AKA' request are in conflict, the received indication shall take precedence.

NOTE 2: The protection mechanisms of EAP-AKA and EAP-AKA' prevent that an indication sent as part of an EAP-AKA request could be forged.

Additionally, in roaming situations the visited 3GPP network may send an indication about the trust status of the non-3GPP access network to the 3GPP AAA server. The 3GPP AAA server may take this indication from the visited network into account in its decision about sending a trust indication to the UE.

EAP-AKA and EAP-AKA’ use pseudonyms and re-authentication identities. Pseudonyms and re-authentication identities should be generated using the method defined in clause 14 of the current specification.

NOTE 3: When using the method in clause 14 for the generation of pseudonyms and re-authentication identities the AAA server can resolve these identities without having to store them. In particular, they can be resolved even when the UE is not registered.

NOTE 4: Clause 14 defines Temporary Identities such that the leading six bits form the Temporary Identity Tag. This tag is converted to a printable character using the BASE64 method, according to clause 14. Compatibility with the NAI format defined in TS 23.003 [8] is achieved by choosing the temporary identity tag such that the printable character equals the leading digit for the NAI defined in TS 23.003.

The authentication and authorization of the UE's access over S2b to external networks from non-3GPP access networks can be based on PAP and CHAP procedures as specified further down in the present document. The corresponding procedures for DS-MIPv6 are given in TS 24.303 [20].

6.2 Authentication and key agreement for trusted access

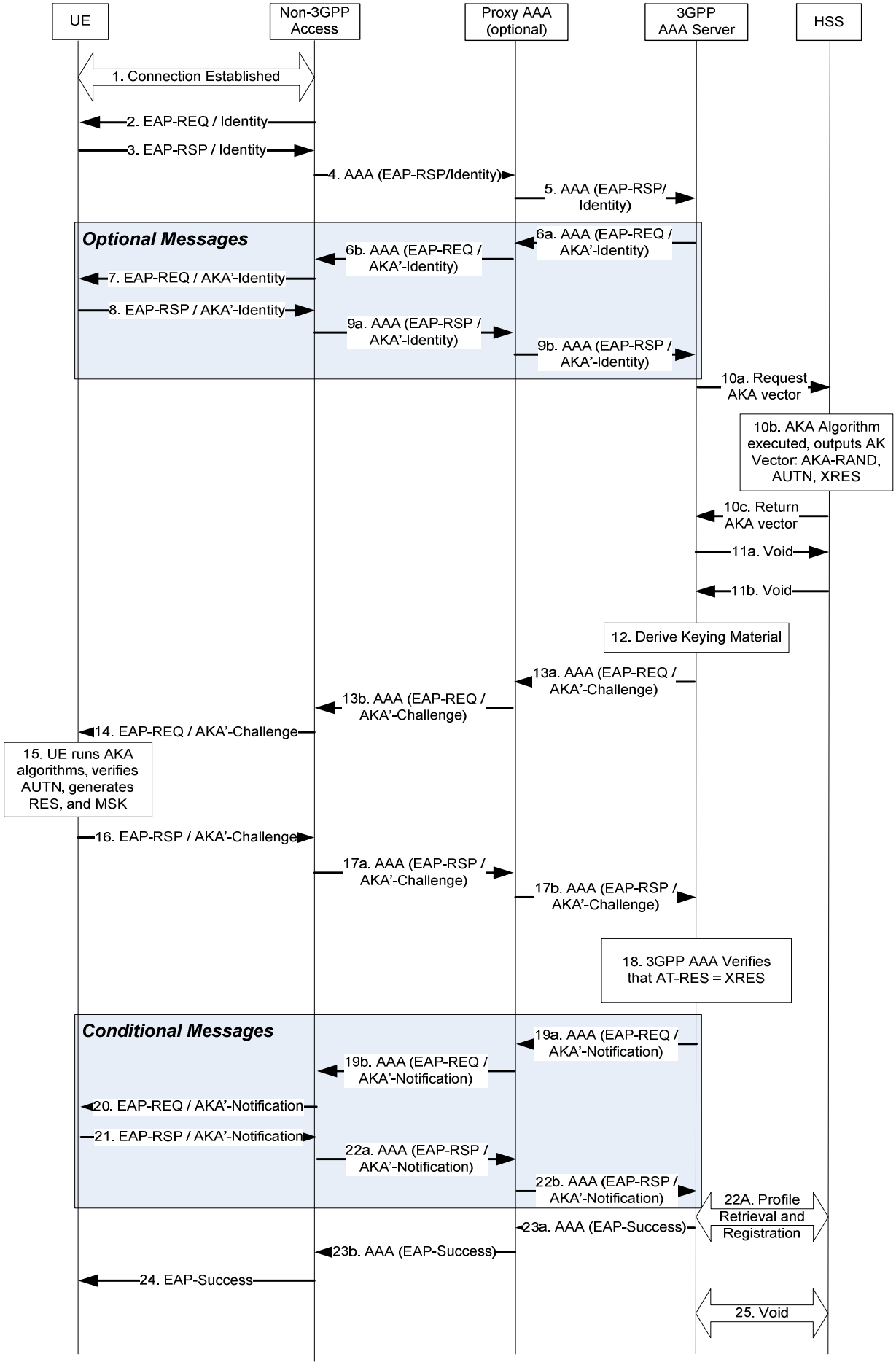
UE
Non-3GPP Access
Proxy AAA (optional)
3GPP AAA Server
HSS
1. Connection Established
2. EAP-REQ / Identity
3. EAP-RSP / Identity
4. AAA (EAP-RSP/Identity)
5. AAA (EAP-RSP/ Identity)
Optional Messages
6a. AAA (EAP-REQ / AKA'-Identity)
6b. AAA (EAP-REQ / AKA'-Identity)
7. EAP-REQ / AKA'-Identity
8. EAP-RSP / 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)
13b. AAA (EAP-REQ / AKA'-Challenge)
14. EAP-REQ / AKA'-Challenge
15. UE runs AKA algorithms, verifies AUTN, generates RES, and MSK
16. EAP-RSP / AKA'-Challenge
17a. AAA (EAP-RSP / AKA'-Challenge)
17b. AAA (EAP-RSP / AKA'-Challenge)
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)
22A. Profile Retrieval and Registration
23a. AAA (EAP-Success)
23b. AAA (EAP-Success)
24. EAP-Success
25. Void

Figure 6.2-1: Non-3GPP Access Authentication

EAP-AKA' as defined in RFC 5448 [23] shall be used for mutual authentication and key agreement.

1. A connection is established between the UE and the trusted non-3GPP access network, using a procedure specific to the non-3GPP access network (which is out of scope for the present document).

2. The authenticator in the trusted non-3GPP access network sends an EAP Request/Identity to the UE.

NOTE 1: EAP packets are transported over this access network using a protocol specific to this access network (which is out of scope for the present document).

3. The UE sends an EAP Response/Identity message. The UE shall send its identity complying with Network Access Identifier (NAI) format specified in TS 23.003 [8]. NAI contains either a pseudonym allocated to the UE in a previous run of the authentication procedure or, in the case of first authentication, the IMSI. In the case of first authentication, the NAI shall indicate EAP-AKA' as specified in TS 23.003 [8].

4. The message is routed towards the proper 3GPP AAA Server based on the realm part of the NAI as specified in TS 23.003 [8]. The routing path may include one or several AAA proxies. The access type and the identity of the access network in which the authenticator resides, shall be included by the authenticator in the Diameter message. In the case of roaming, the visited network AAA proxy shall also include the visited network identifier in the same Diameter message.
   The access network identity is defined separately for each access network type. For each access network type, the access network identity is documented in TS 24.302 [22] to ensure that UE and HSS use the same access network identities as input for key derivation.

NOTE 2: Diameter referral can also be applied to find the AAA server.

NOTE 3: The visited network identifier identifies a visited 3GPP network, and is to be distinguished from the access network identifier, which relates to a non-3GPP access network.

5. The 3GPP AAA Server receives the EAP Response/Identity message that contains the subscriber identity and the access type over the STa/SWd interface. In the case of roaming, the 3GPP AAA server also receives the visited network identifier in the same Diameter message that carried the EAP Response/Identity message.

6. The 3GPP AAA Server requests again the user identity, using the EAP Request/AKA' Identity message. This identity request is performed as the intermediate nodes may have changed or replaced the user identity received in the EAP Response Identity message, as specified in RFC 5448 [23]. However, in order to avoid this new request of the user identity, the home operator should ensure that the Authenticator and all AAA entities between the EAP peer and EAP server process the EAP-Response/Identity message inline with EAP-AKA' as specified in the present document and TS 23.003. Consequently, if the EAP server knows that the EAP-Response/Identity message was processed accordingly, the EAP server shall use the user identity which was received in the EAP-Response/Identity message in step 5 and skip this EAP Request/AKA' Identity request in steps 6 through 9.

7. The authenticator in the access network forwards the EAP Request/AKA' Identity message to the UE.

8. The UE responds with an identity that depends on the parameters contained in the EAP Request/AKA' Identity message; for details cf. TS 24.302 [22].

9. The authenticator in the access network forwards the EAP Response/AKA' Identity to the 3GPP AAA Server. The access type and the identity of the access network in which the authenticator resides, shall be included by the authenticator in this message. In the case of roaming, the visited network AAA proxy shall also include the visited network identifier in the same message.The identity received in this message will be used by the 3GPP AAA Server in the rest of the authentication process.

10. The 3GPP AAA Server shall identify the subscriber as a candidate for authentication with EAP-AKA’, based on the received identity in the EAP-Response/Identity or EAP Response/AKA' Identity message. If the leading digits in the NAI do not indicate that the UE supports EAP-AKA’, the 3GPP AAA server shall abort the authentication. If the UE does indicate that it supports EAP-AKA’, the 3GPP AAA server then checks whether it has an unused authentication vector with AMF separation bit = 1 and the matching access network identifier available for that subscriber. If not, a set of new authentication vectors is retrieved from HSS. The 3GPP AAA server includes an indication that the authentication vector is for EAP-AKA', as defined RFC 5448 [23], and the identity of the access network in which the authenticator resides in a message sent to the HSS. A mapping from the temporary identifier (pseudonym in the sense of RFC 4187 EAP-AKA [7]) to the IMSI is required.

NOTE 7a: As the UE moves around the access network identifier may change. But an authentication vector stored in the 3GPP AAA server can only be used if it is associated with the access network identifier of the current access network. This may make stored authentication vectors unusable. Furthermore, as the 3GPP AAA server resides in the home network there is no significant performance advantage in fetching batches of authentication vectors. It is therefore recommended that the 3GPP AAA server fetches only one authentication vector at a time.

Upon receiving from the 3GPP AAA server an indication that the authentication vector is for EAP-AKA' as defined in RFC 5448 [23], the HSS generates an authentication vector with AMF separation bit = 1. The HSS then transforms this authentication vector into a new authentication vector by computing CK' and IK' per Clauses A.1 and A.2 of the Normative Annex A with <access network identity> being one of the input parameters. The HSS then sends this transformed authentication vector to the 3GPP AAA server.

NOTE 7b: The 3GPP AAA server does not notice the transformation and treats this authentication vector like any other authentication vector.

The HSS and/or 3GPP AAA server need to ensure, based on local policy, that the non-3GPP access requesting the authentication data, which is identified by the information transmitted by the authenticator in step 4, is authorized to use the access network identity used to calculate CK' and IK'. The 3GPP AAA server shall have assurance of the origin of this information. The exact details of how to achieve this are not covered in this specification.

The HSS shall check if there is a 3GPP AAA Server already registered to serve for this subscriber. In case the HSS detects that another 3GPP AAA Server has already registered for this subscriber, it shall provide the current 3GPP AAA Server with the previously registered 3GPP AAA Server address. The authentication signalling is then routed to the previously registered 3GPP AAA Server with Diameter-specific mechanisms, e.g., the current 3GPP AAA Server transfers the previously registered 3GPP AAA Server address to the 3GPP AAA proxy or the AAA entity in the trusted non-3GPP access network, or the current 3GPP AAA Server acts as a AAA proxy and forwards the authentication message to the previously registered 3GPP AAA Server.

11. Void.

NOTE 8: Void.

12. New keying materials MSK and EMSK are derived from CK' and IK' according to RFC 5448 [23].

NOTE 9: The use of EMSK can refer to subclause 9.2.1 MIPv4.

A new pseudonym and/or re-authentication ID may be chosen and if chosen they shall be protected (i.e. encrypted and integrity protected) using keying material generated from EAP-AKA’.

13. The 3GPP AAA Server sends RAND, AUTN, a message authentication code (MAC) and two user identities (if they are generated), protected pseudonym and/or protected re-authentication id, to the authenticator in the access network in EAP Request/AKA'-Challenge message. The 3GPP AAA Server shall also include the access network identity in this message. The access network identity is defined in TS 24.302 [22]. The sending of the re-authentication id depends on 3GPP operator's policies on whether to allow fast re-authentication processes or not. It implies that, at any time, the 3GPP AAA Server decides (based on policies set by the operator) to include the re-authentication id or not, thus allowing or disallowing the triggering of the fast re-authentication process.

The 3GPP AAA Server may send as well a result indication to the authenticator in the access network, in order to indicate that it wishes to protect the success result message at the end of the process (if the outcome is successful). The protection of result messages depends on home operator's policies.

14. The authenticator in the access network sends the EAP Request/AKA’-Challenge message to the UE.

15. The UE first checks whether the AMF separation bit is set to 1. If this is not the case the UE shall reject the authentication. Otherwise, the UE runs AKA algorithms. The UE verifies that AUTN is correct and hereby authenticates the network. If AUTN is incorrect, the UE rejects the authentication (not shown in this example). If the sequence number is out of synch, the UE initiates a synchronization procedure, c.f. RFC 5448 [23]. If AUTN is correct, the UE computes RES, IK and CK.

The UE then computes CK' and IK' in the same way as the HSS, per Clauses A.1 and A.2 of the Normative Annex A with <access network identity> being one of the input parameters. The UE derives required additional new keying material, including the key MSK and EMSK, according to RFC 5448 [23] from the new computed CK', IK' and checks the received MAC with the new derived keying material.

If a protected pseudonym and/or re-authentication identity were received, then the UE stores the temporary identity(s) for future authentications.

The access network identity, which is input to key derivation to obtain CK', IK', shall be sent by the 3GPP AAA server in the EAP-request / AKA'-Challenge message as defined in RFC 5448 [23].

RFC 5448 [23] specifies a possibility for the UE to compare the access network identity received from the 3GPP AAA server with the access network identity received locally, e.g. from the link layer. It is defined in 3GPP TS 24.302 [22] for which access networks the comparison is done, how the UE shall determine the locally received network name and what the UE shall do if the check fails. If the comparison is done for a specific access network, it shall be done according to the rules specified in RFC 5448 [23]. The UE - or the human user - may use the network name as a basis for an authorization decision. E.g. the UE may compare the network name against a list of preferred or barred network names.

16. The UE calculates a new MAC value covering the EAP message with the new keying material. UE sends EAP Response/AKA'-Challenge containing calculated RES and the new calculated MAC value to the authenticator in the access network.

    The UE shall include in this message the result indication if it supports such indications and if it received the same indication from the 3GPP AAA Server. Otherwise, the UE shall omit this indication.

17. The authenticator in the access network sends the EAP Response/AKA'-Challenge packet to 3GPP AAA Server.

18. The 3GPP AAA Server checks the received MAC and compares XRES to the received RES.

19. If all checks in step 18 are successful, the 3GPP AAA Server shall send the message EAP Request/AKA'-Notification, previous to the EAP Success message, if the 3GPP AAA Server and the UE have indicated the use of protected successful result indications as in RFC 5448 [23]. This message is MAC protected.

NOTE 11: Steps 19 to 22 are conditional based on the EAP Server and the UE having indicated the use of protected successful result indications.

20. The authenticator in the access network forwards the message to the UE.

21. The UE sends the EAP Response/AKA'-Notification.

22. The authenticator in the access network forwards the EAP Response/AKA'-Notification message to the 3GPP AAA Server. The 3GPP AAA Server shall ignore the contents of this message

22A. The 3GPP AAA Server shall initiate the Subscriber Profile Retrieval and 3GPP AAA Server registration to the HSS. The 3GPP AAA Server shall keep access session information related to the subscriber including the access network identity. The 3GPP AAA Server shall implement a policy to limit the number of active access sessions.

23. The 3GPP AAA Server sends the EAP Success message to the authenticator in the access network (perhaps preceded by an EAP Notification, as explained in step 19). The 3GPP AAA Server also includes the key MSK, RFC 5448 [23], in the underlying AAA protocol message (i.e. not at the EAP level). The authenticator in the access network stores the keying material to be used in communication with the authenticated UE as required by the access network.

24. The authenticator in the access network informs the UE about the successful authentication with the EAP Success message. Now the EAP AKA' exchange has been successfully completed, and the UE and the authenticator in the access network share keying material derived during that exchange.

25. Void.

NOTE 12: It may happen in handover situations that, due to pre-registration, a subscriber is authenticated in a target access network while still being attached to the source access network.

NOTE 13: Void.

The authentication process may fail at any moment, for example because of unsuccessful checking of MACs or no response from the UE after a network request. In that case, the EAP AKA' process will be terminated as specified in RFC 5448 [23] and an indication shall be sent to HSS.

6.3 Fast re-authentication procedure for trusted access

Fast re-authentication for EAP-AKA' is specified in RFC 5448 [23]. Fast re-authentication re-uses keys derived on the previous full authentication. Fast re-authentication does not involve the HSS nor the credentials used with EAP-AKA' (e.g USIM application in case of terminal with 3GPP access capabilities), and does not involve the handling of AKA authentication vectors, which makes the procedure faster and reduces the load on the HSS and, in particular, the Authentication Centre.

UE and 3GPP AAA server shall implement fast re-authentication for EAP-AKA'. Its use is optional and depends on operator policy. If fast re-authentication for EAP-AKA' is used the 3GPP AAA server shall indicate this to the UE by means of sending the re-authentication identity to the UE as in step 13 of subclause 6.2.

The security level of fast re-authentication for EAP-AKA' is lower as it does not prove the presence of the credentials used with EAP-AKA' (e.g. presence of USIM application in case of terminal with 3GPP access capabilities) on the user side. The operator should take this into account when defining the policy on fast re-authentication.

Fast re-authentications for EAP-AKA' generates new keys MSK, which may be used for renewing session key used for protection in the non-3GPP access network.

The access network identity shall not change when going from the full to the fast re-authentication process. If this happens, the re-authentication process shall be terminated as defined in RFC 5448 [23].

In this section it is described how the process works for trusted non-3GPP access to EPS.

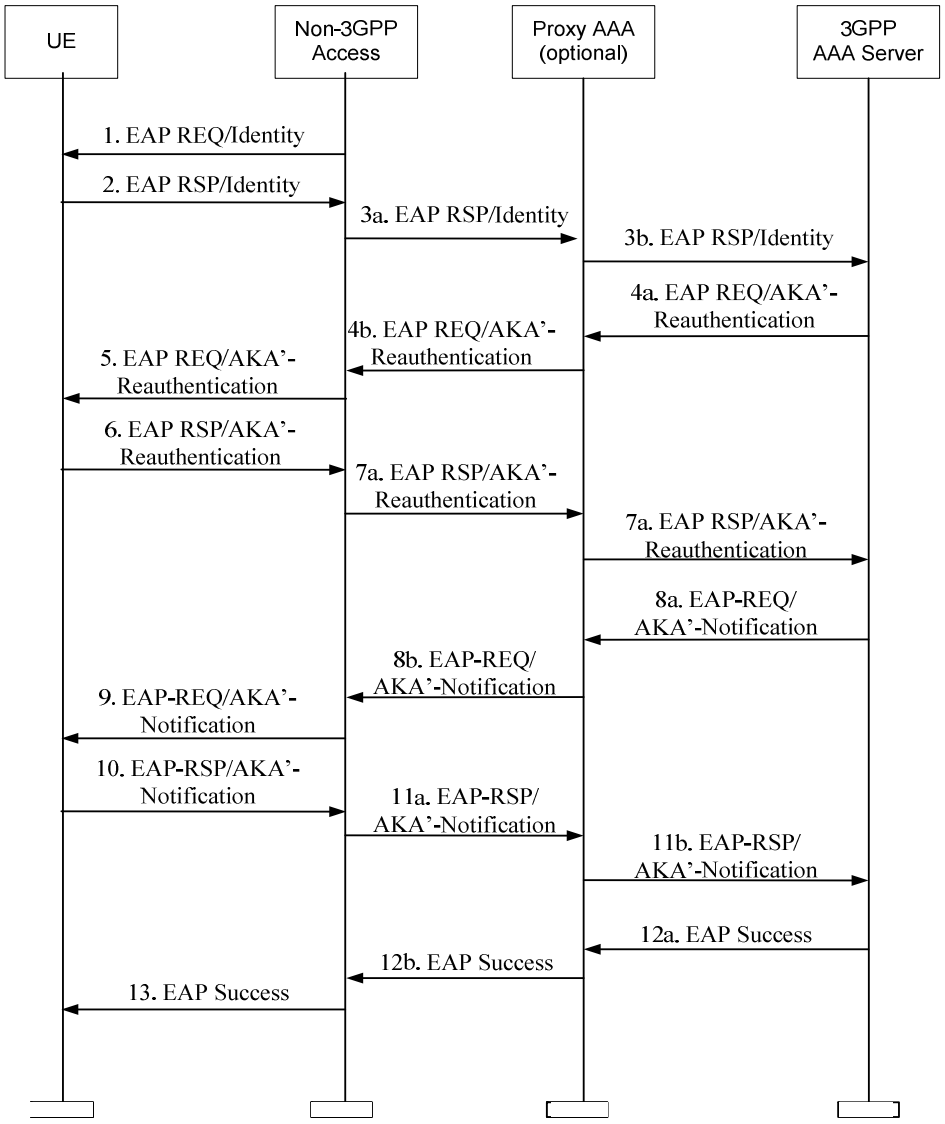

Figure 6.3-1: Non-3GPP Fast Re-authentication

1) Non-3GPP Access Network sends an EAP Request/Identity to the UE.

2) UE replies with an EAP Response/Identity containing a re-authentication identity (this identity was previously delivered by AAA server in a full authentication procedure).

3) The Non-3GPP Access Network forwards the EAP Response/Identity to the AAA server. Intermediate Proxy AAA's may perform routing and forwarding functions.

4) The AAA server initiates the Counter (which was initialized to one in the full authentication process) and sends it in the EAP Request message, together with the NONCE, the MAC (calculated over the NONCE) and a protected re-authentication ID for a next fast re-authentication. If the AAA server is not able to deliver a re-authentication identity, next time the UE shall force a full-authentication (to avoid the use of the re-authentication identity more than once).

5) The 3GPP AAA Server may send a result indication to the UE, in order to indicate that the success result message at the end of the process shall be protected (if the outcome is successful). The protection of result messages depends on home operator's policies.

6) The 3GPP AAA server may fail to recognize the identity as it may have been altered by proxies. In this case, the 3GPP AAA server may, as in the case of a full authentication, instead perform an EAP AKA' method specific identity request; i.e. "EAP-Request/AKA' identity [Any identity]" in order to obtain a more reliable identity, in analogy of step 7 of the full EAP AKA' authentication. This should however only be used in case the server fails to recognize the identity, as otherwise the purpose of fast re-authentication is defeated.

7) The Non-3GPP Access Network forwards the EAP Request message to the UE.

8) The UE verifies that the Counter value is fresh and the MAC is correct, and it sends the EAP Response message with the same Counter value (it is up to the AAA server to step it up) and a calculated MAC.

9) The UE shall include in this message the result indication if it received the same indication from the 3GPP AAA. Otherwise, the UE shall omit this indication.

10) The Non-3GPP Access Network forwards the response toward the AAA server.

11) The AAA server verifies that the Counter value is the same as it sent, and the MAC is correct, and sends the message EAP Request/AKA'-Notification, previous to the EAP Success message, if the 3GPP AAA Server requested previously to use protected success result indications. The message EAP Request/AKA'-Notification is MAC protected, and includes an encrypted copy the Counter used in the present re-authentication process.

12) The Non-3GPP Access Network forwards the EAP Request/AKA'-Notification message to the UE.

13) The UE sends the EAP Response/AKA'-Notification.

14) The Non-3GPP Access Network forwards the EAP Response/AKA'-Notification message toward the 3GPP AAA server. The 3GPP AAA Server shall ignore the contents of this message.

15) The AAA server sends an EAP Success message. If some extra keying material was generated for Access Network specific confidentiality and/or integrity protection, then the 3GPP AAA Server includes this derived keying material in the underlying AAA protocol message. (i.e., not at EAP level). The Non-3GPP Access Network stores the keying material which may be used in communication with the authenticated UE.

16) The EAP Success message is forwarded to the UE.

The re-authentication process may fail at any moment, for example because of unsuccessful checking of MACs or no response from the UE after a network request. In that case, the EAP AKA' process will be terminated as specified in RFC 5448 [23] and an indication shall be sent to HSS/HLR.

6.4 Authentication and key agreement for untrusted access

For untrusted access, UE and the ePDG shall perform mutual authentication during the IPsec tunnel establishment between the UE and the ePDG (SWu reference point). This procedure is specified in clause 8 of the present document.

In addition, before the IPsec tunnel establishment between the UE and the ePDG can be performed, the UE needs to obtain IP connectivity across the access network, which may require an access authentication, which is independent of the EAP-AKA authentication run in conjunction with the IPsec tunnel establishment. This additional access authentication and key agreement is not required for the security of the Evolved Packet Core. However, it may be required for the security of the untrusted non-3GPP access network. Any authentication and key agreement procedure deemed appropriate by the access network provider, including EAP-AKA', may be used.

6.5 Authentication and authorization with S2b for Private network access from Untrusted non-3GPP Access networks

6.5.1 General

Two procedures for the authentication and authorization for the Private network access are possible with S2b. The first procedure described in clause 6.5.2 is applicable in the scenario where the External AAA Server supports the PAP procedure. The second procedure described in clause 6.5.3 is applicable in the scenario where the External AAA Server supports the CHAP procedure.

NOTE 1: TS 33.234 [9] also covers the case of the External AAA Server supporting the EAP procedure, but EAP is only supported for I-WLAN, not for S2b (nor for S2a or 3GPP accesses).

NOTE 2: External network operators wanting to use PAP for authentication are warned that PAP is an obsolete protocol from a security point of view. CHAP provides stronger security than PAP.

6.5.2 Authentication and authorization for the Private network access (the External AAA Server performs PAP procedure)

The signalling sequence when the External AAA server performs the PAP procedures in a network based mobility system to authenticate and authorize the UE's access to a Private network over an Untrusted non-3GPP Acess network using S2b is illustrated in Figure 6.5.3-1. In this procedure, the External AAA Server supports the PAP procedure.

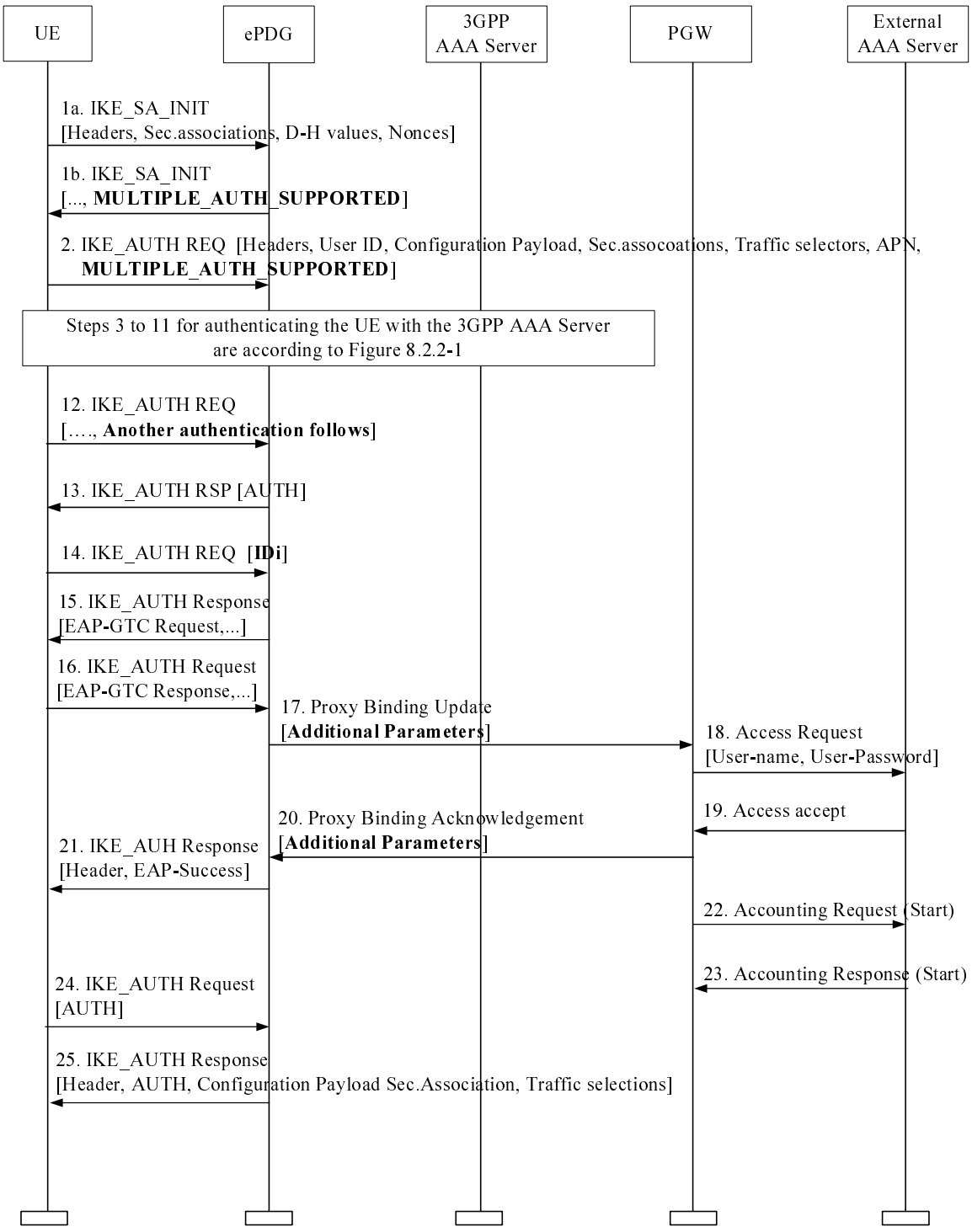

Figure 6.5.2-1: Authentication and authorization for the Private network access over S2b (The External AAA Server performs PAP procedure)

NOTE: The parameters indicated with bold character denote support for "the multiple authentication and authorization", as specified in RFC 4739 [30].

1. The UE and the ePDG exchange the first pair of IKE_SA_INIT messages, in which the ePDG and the UE negotiate cryptographic algorithms, exchange nonces and perform a Diffie-Hellman exchange. If the ePDG supports multiple authentication procedures, it indicates MULTIPLE_AUTH_SUPPORTED in step 1b.

2. The UE sends the user identity (in the IDi payload) and the APN information (in the IDr payload) to the ePDG and begins negotiation of child security associations. The UE omits the AUTH parameter in order to indicate to the ePDG that it wants to use EAP over IKEv2. The user identity shall be compliant with the Network Access Identifier (NAI) format specified in 3GPP TS 23.003[8], containing the IMSI or the pseudonym as defined for EAP-AKA in RFC 4187 [7]).
   If the UE's Remote IP address needs to be configured dynamically, then the UE shall send the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to obtain a Remote IP Address. If the APN requires authentication and authorization with the External AAA Server and the ePDG indicated that multiple authentication procedures are supported in step 1b, then MULTIPLE_AUTH_SUPPORTED is included.

3.-11. The steps 3 to 11 clause 8.2.2 apply here.

12. The UE shall take its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the ePDG. The UE includes a Notify payload ANOTHER_AUTH_FOLLOWS indicating to the ePDG that another authentication and authorization round will follow.

13. The ePDG checks the correctness of the AUTH received from the UE and calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. The AUTH parameter is sent to the UE.

NOTE: At this point the UE is authenticated from EPC point of view. PMIP/GTP signalling between ePDG and PDN GW could start anytime after this step but since an additional authentication with the external network was indicated in step 12, the ePDG needs to collect additional authentication parameters from the UE before initiating the PMIP binding update / GTP session creation procedure in Step 15.

14. The UE sends the identity in the private network in IDi payload that is used for the next authentication and authorization with the External AAA Server and without an AUTH payload.

15. If the External AAA Server supports the PAP procedure, the ePDG sends an EAP-GTC request to the UE for the next authentication.

16. The UE returns an EAP-GTC response containing the user‘s password to the ePDG.

17. The ePDG includes the user-name and user-password as Additional Parameters in the PBU it sends to PGW as defined in 3GPP TS 29.275 [32]. The corresponding message in GTP for S2b is Create Session Request as defined in 3GPP TS 29.274 [31].

18. The PGW sends a AAA Access request message with user-name and user-password attributes which are copied from the PBU Additional Parameters to the external AAA server.

19. The external AAA server returns the Access accept to the PGW.

20. The PGW sends PBA (PMIP) /Create Session Response (GTP) to the ePDG with the Additional Parameters indicating authentication success.

21. The EAP-success message is sent to the UE over IKEv2.

22.-23. The PGW sends the Accounting request (Start) message to the External AAA Server and the External AAA Server returns the Accounting response (Start) message to the PGW if needed.

24. The UE shall generate the AUTH parameter calculated by the SK_pi as a shared secret as specified in RFC 5996 [30] in order to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the ePDG.

25. The ePDG checks the correctness of the AUTH received from the WLAN UE and calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. The ePDG shall send the assigned Remote IP address in the configuration payload (CFG_REPLY), if the WLAN UE requested a Remote IP address through the CFG_REQUEST. Then the AUTH parameter calculated by the SK_pr as a shared secret (see RFC 5996 [30]) is sent to the WLAN UE together with the configuration payload, security associations and the rest of the IKEv2

parameters and the IKEv2 negotiation terminates.

6.5.3 Authentication and authorization for the private network access (the external AAA server performs CHAP procedure)

The signalling sequence when the External AAA server performs the CHAP procedures in a network based mobility system to authenticate and authorize the UE's access to a Private network over an Untrusted non-3GPP Acess network is illustrated in Figure 6.5.3-1. In this procedure, the External AAA Server supports the CHAP procedure.

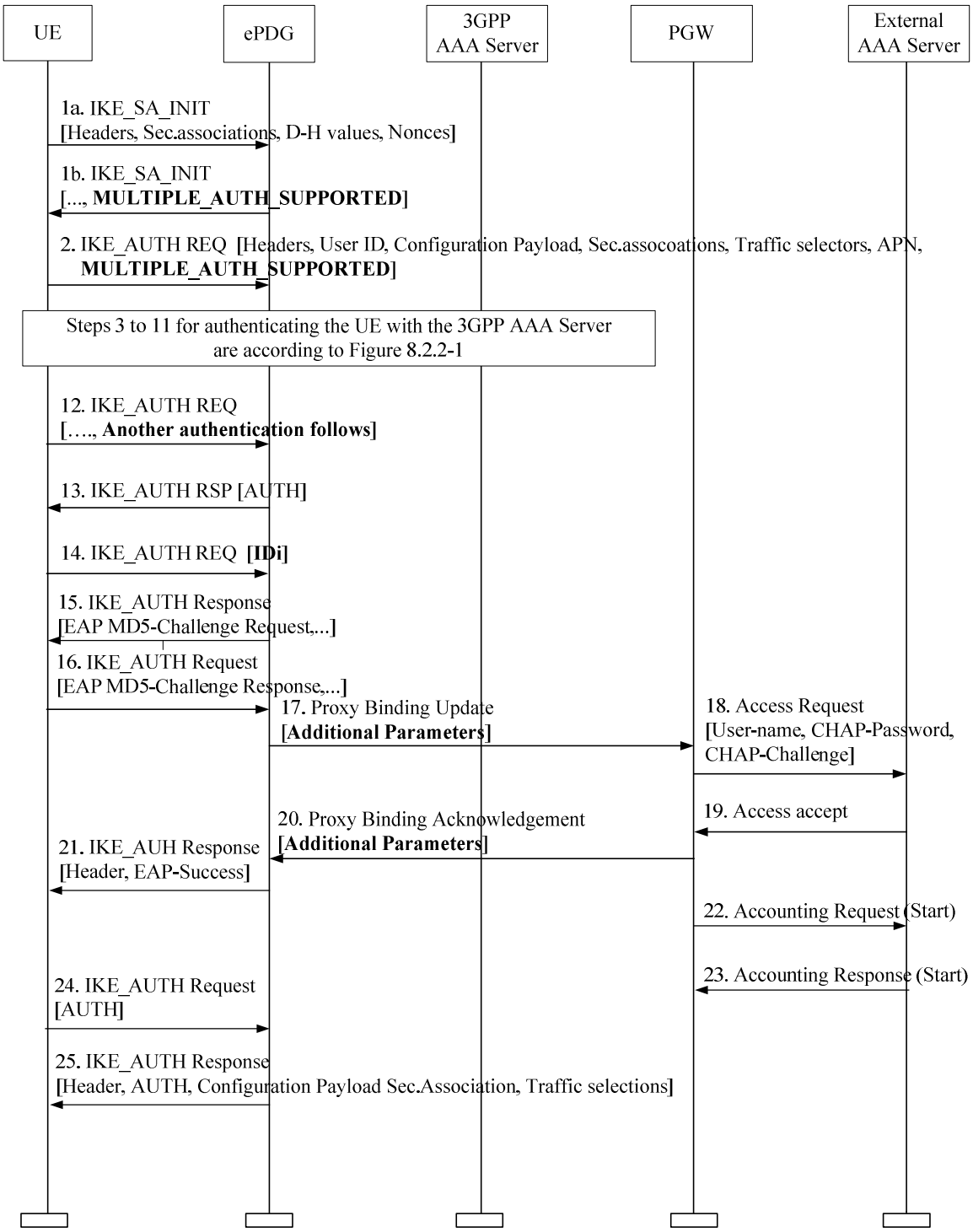

Figure 6.5.3-1: Authentication and authorization for the Private network access over S2b (The External AAA Server performs CHAP procedure)

NOTE 1: The parameters indicated with bold character denote support for "the multiple authentication and authorization", as specified in RFC 4739 [33]. Only the PMIP case is shown in this figure for the sake of clarity, but the text below also covers the GTP case.

1. The UE and the ePDG exchange the first pair of IKE_SA_INIT messages, in which the ePDG and the UE negotiate cryptographic algorithms, exchange nonces and perform a Diffie-Hellman exchange. If the ePDG supports multiple authentication procedures, it indicates MULTIPLE_AUTH_SUPPORTED in step 1b.

2. The UE sends the user identity (in the IDi payload) and the APN information (in the IDr payload) to the ePDG and begins negotiation of child security associations. The UE omits the AUTH parameter in order to indicate to the ePDG that it wants to use EAP over IKEv2. The user identity shall be compliant with the Network Access Identifier (NAI) format specified in 3GPP TS 23.003 [8], containing the IMSI or the pseudonym as defined for EAP-AKA in RFC 4187 [7]).
   If the UE's Remote IP address needs to be configured dynamically, then the UE shall send the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to obtain a Remote IP Address. If the APN requires authentication and authorization with the External AAA Server and the ePDG indicated that multiple authentication procedures are supported in step 1b, then MULTIPLE_AUTH_SUPPORTED is included.

3.-11. The steps 3 to 11 in clause 8.2.2 apply here.

12. The UE shall take its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the ePDG. The UE includes a Notify payload ANOTHER_AUTH_FOLLOWS indicating to the ePDG that another authentication and authorization round will follow.

13. The ePDG checks the correctness of the AUTH received from the UE and calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. The AUTH parameter is sent to the UE.

NOTE 2: At this point the UE is authenticated from EPC point of view. PMIP/GTP signalling between ePDG and PDN GW could start anytime after this step but since an additional authentication with the external network was indicated in step 12, the ePDG needs to collect additional authentication parameters from the UE before initiating the PMIP binding update / GTP session creation procedure in Step 15.

14. The UE sends the identity in the private network in IDi payload that is used for the next authentication and authorization with the External AAA Server and without an AUTH payload.

15. If the External AAA Server supports the CHAP procedure, the ePDGsends an EAP MD5-challenge request to the UE for the next authentication.

16. The UE returns an EAP MD5-Challenge response to the ePDG.

17. The ePDG includes the user-name, CHAP-password and CHAP-Challenge as Additional Parameters in the PBU it sends to PGW as defined in 3GPP TS 29.275 [32]. The corresponding message in GTP for S2b is Create Session Request as defined in 3GPP TS 29.274 [31].

18. The PGW sends a AAA Access request message with user-name, CHAP-password and CHAP-Challenge attributes, which are copied from the Additional Parameters in the PBU, to the External AAA server.

19. The External AAA server returns the Access accept to the PGW.

20. The PGW sends PBA (PMIP) /Create Session Response (GTP) to the ePDG with the Additional Paramters indicating authentication success.

21. The EAP success message is sent to the UE over IKEv2.

22.-23. The PGW sends the Accounting request (Start) message to the External AAA Server and the External AAA Server returns the Accounting response (Start) message to the PGW if needed.

24. The UE shall generate the AUTH parameter calculated by the SK_pi as a shared secret as specified in RFC 5996 [30] in order to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the ePDG.

25. The ePDG checks the correctness of the AUTH received from the UE and calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. The ePDG shall send the assigned Remote IP address in the configuration payload (CFG_REPLY), if the UE requested a Remote IP address through the CFG_REQUEST. Then the AUTH parameter calculated by the SK_pr as a shared secret (see RFC 5996 [30]) is sent to the UE

together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.

6.6 Re-authentication based on ERP

6.6.1 Introduction

The EAP Re-authentication protocol (ERP) is specified in IETF RFC 6696 [x]. It is independent on the EAP method in use but it permits a re-authentication based on key material (unexpired) derived from a previous authentication. As for the Fast re-authentication method (clause 6.3), it re-uses the key derived from the previous full authentication. It does not involve the HSS, nor the credentials used by EAP-AKA' and does not involve the handling of EAP-AKA' authentication vectors, which makes the procedure faster and reduces the load on (the 3GPP AAA server and) the HSS and, in particular the Authentication Centre.

The ERP protocol permits to perform the re-authentication process at the 3GPP AAA Server avoiding signalling on SWx. It also permits to delegate the re-authentication process to the TWAP (Trusted WLAN AAA Proxy) avoiding signalling on STa (and SWd in case of roaming) or to the 3GPP AAA Proxy avoiding signalling on SWd, thus reducing the load as well on the 3GPP AAA server.

To use ERP, the basic assumption is that ERP is supported by the WLAN. For non-roaming scenarios, the ER server (as described in IETF RFC 6696[x]) may reside in the TWAP or the 3GPP AAA server. In roaming scenarios, there is an additional case where the ER server resides within the 3GPP AAA Proxy.

The EAP server, which resides in the 3GPP AAA server, shall support the ERP related functionalities as defined in IETF RFC 6696 [46].

The ER Authenticator resides in the EAP Authenticator.

6.6.2 ERP bootstrapping

6.6.2.1 General

In order to perform re-authentication, the UE and the network shall derive corresponding ERP Keys. Those ERP keys are derived from the EMSK that is derived during the first EAP exchange in clause 6.2 step 12. The ERP implicit bootstrapping consists of deriving the ERP keys and providing those keys to the ER server during the full EAP authentication. At the end of the ERP bootstrap phase both UE and ER server share keying material for further re-authentication.

NOTE: Only the ERP Implicit Bootstrapping mode defined in IETF RFC 6696 [46] is supported.

6.6.2.2 ERP Implicit bootstrapping

In the implicit mode, the ERP Keys are derived during the EAP exchange.

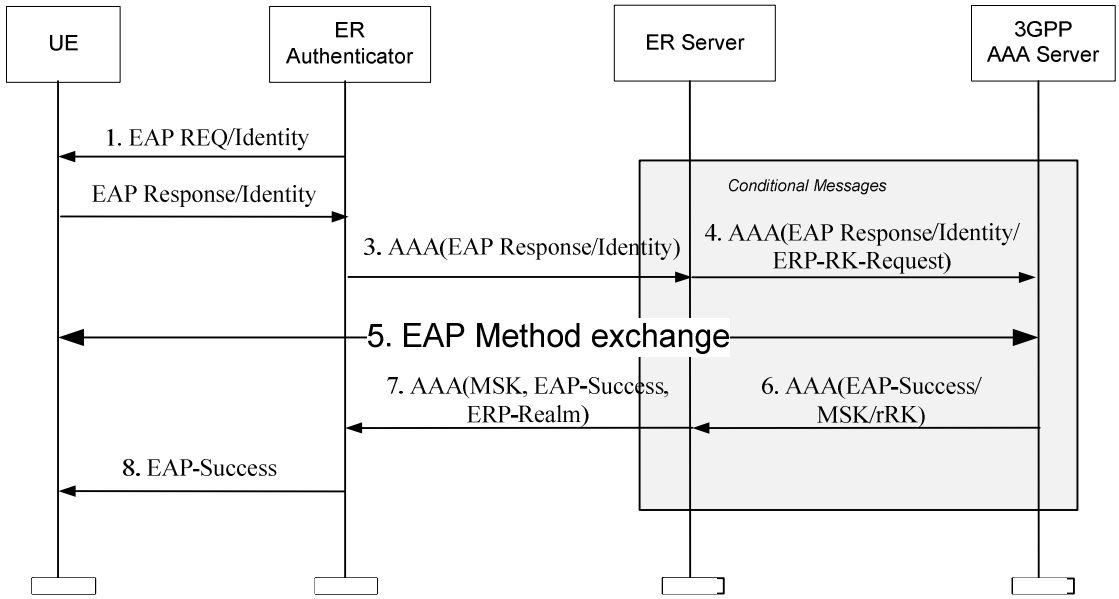

Figure 6.6.2.2-1: Implicit ERP Bootstrapping

1. The ER Authenticator sends an EAP Request/Identity to the UE.
2. The UE sends an EAP Response/Identity message.
3. The ER Authenticator sends the message towards the home EAP server.

If ER server is located in TWAP or 3GPP AAA Proxy:

4. The ER server receives the message. It shall include, in the request fowarded to the 3GPP AAA server, the domain name and the ERP-RK-Request to retrieve an ERP key specific for that domain as specified in IETF RFC 6942 [47].
5. The complete EAP exchange continues as described in clause 6.2 (from step 6 to step 23a). The HSS indicates to the 3GPP AAA Server if the subscriber is authorized to use ERP.
6. If the authentication is successfull and the subscriber is authorized to use ERP and the use of ERP in the visited domain is authorized, the 3GPP AAA server sends the ERP keying material as described in IETF RFC 6942 [47] along with the EAP-Success.
7. The ER server removes from the message and stores the ERP Keying material and forwards the Diameter message with the MSK and the ERP-Realm to the ER authenticator.

If ER server is located in the 3GPP AAA server, message 4 and 6 do not apply. In this case, ER server and EAP server are internal to the 3GPP AAA server.

5. The complete EAP exchange continues as described in clause 6.2 (from step 6 to step 23a). The HSS indicates to the 3GPP AAA Server if the subsriber is authorized to use ERP.
7. If the authentication is successful and the subscriber is authorized to use ERP, the ER serversends the Diameter message with the MSK and the ERP-Realm to the ER authenticator.

6.6.2.3 Void

6.6.3 ERP exchange for re-authentication

The UE either by the implicit or the explicit bootstrapping owns necessary keying information for ERP re-authentication.

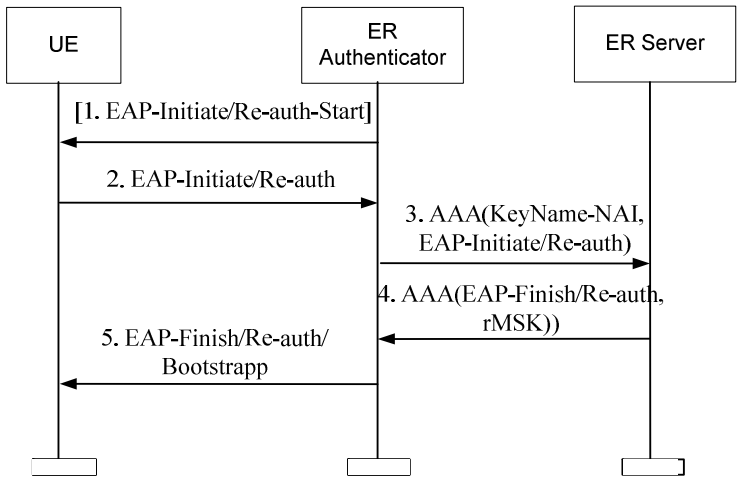

Figure 6.6.3-1:ERP Re-authentication exchange

1) The ERP exchange is optionnally triggered by the ER Authenticator sending an EAP-Initiate/Re-auth-Start.
2) The UE sends an EAP-Initiate/Re-auth message to the ER Authenticator.
3) The ER Authenticator processes the message as in IETF RFC 6696 [46] and sends a AAA message to the ER server as described in IETF RFC 6942 [47].
4) The ER server verifies the validity of the ERP message as described in IETF RFC 6942 [47] and if the re-authentication is successful, it replies to the ER Authenticator with the rMSK.
5) The ER Authenticator retrieves the rMSK and forwards the EAP-Finish/Re-auth to the UE.

6.6.4 ERP key derivation

The key derivation mechanism for ERP is described in IETF RFC 6696 [46].

7 Establishment of security contexts in the target access system

7.1 General assumptions

The following sub-clauses describe all the specifics that are related to the establishment of the security context of the non-3GPP target access for the purpose of Interworking with EPS system. The target access system may have other specifics that are used for the establishment of the security context while interworking with EPS system is not considered. These specifics are outside the scope of the present document.

7.2 Establishment of security context for trusted non-3GPP access

In this case, the credentials the UE shares with the 3GPP AAA server are used to establish security contexts in the access system.

It is assumed that the EPS user always uses EAP-AKA' credentials (e.g. a USIM application in case of terminal with 3GPP access capabilities) to perform mutual authentication and establish security contexts with the Home Network.

7.2.1 CDMA-2000 HRPD EPS interworking

NOTE: General Concepts for Interworking between E-UTRAN and CDMA2000 are described in TS 23.402 [5] subclause 4.1.1.

7.2.1.1 EPS-HRPD architecture

Figure 7.2.1.1-1 depicts the basic non-roaming architecture for HRPD-LTE Interworking.

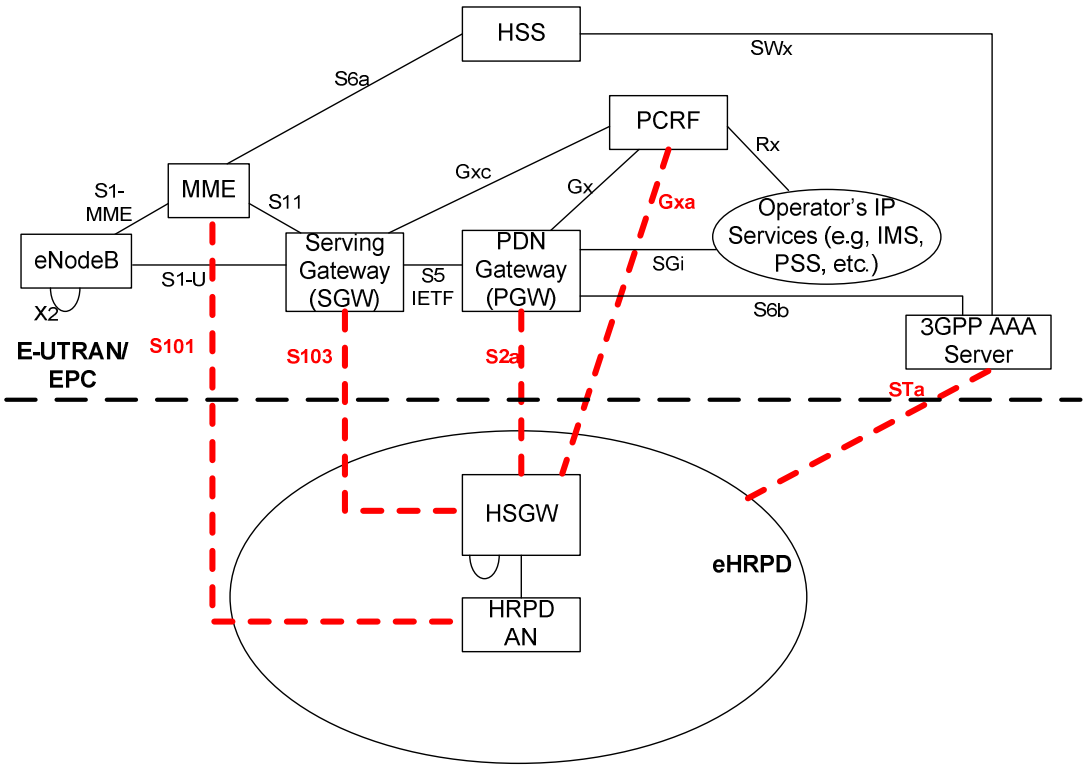

Figure 7.2.1.1-1: Basic non-roaming architecture for HRPD-LTE Interworking. Interworking reference points are highlighted.

7.2.1.2 Network elements

7.2.1.2.1 E-UTRAN

E-UTRAN is described in detail in TS 36.300 [15] with additional functions listed in TS 23.401 [13].

7.2.1.2.2 MME

The details of the MME functionality are described in the TS 23.401 [13], while additional MME functionality, related to the interoperability with non-3GPP systems is described in the TS 23.402 [5].

The following are additional MME functions:

In the EPS, the security functions of the MME are described in TS 33.401 [16]. During the pre-registration towards the EPS from HRPD (as part of HRPD to EUTRAN HO), the procedures and functions are as defined in TS 33.401 [16], with the exception the NAS procedures will occur over S101. This is described in greater detail in clause 10.

7.2.1.2.3 Gateway

7.2.1.2.3.1 General

The functional split of PDN GW and Serving GW is described in TS 23.401 [13].

7.2.1.2.3.2 Serving GW

The details of the Serving GW functionality are described in the TS 23.401 [13], while additional Serving GW functionality, related to the interoperability with non-3GPP systems is described in the TS 23.402 [5].

7.2.1.2.3.3 PDN GW

The details of the PDN GW functionality are described in the TS 23.401 [13], while additional PDN GW functionality, related to the interoperability with non-3GPP systems is described in the TS 23.402 [5].

7.2.1.2.4 PCRF

The details of the PCRF functionality are described in the TS 23.401 [13] and TS 23.203 [14], while additional PCRF functionality, related to the roaming scenario is described in the TS 23.402 [5].

7.2.1.3 Reference points

7.2.1.3.1 List of reference points

NOTE: S1-MME, S1-U, S2a, S2b, S2c, ,S3, S4, S5-MIP, S6a, Gx, S8, S9, S10, S11, S101, S103 are defined in TS 23.401 [13].

Additional reference points descriptions, related to the interoperability with non-3GPP systems are presented in the TS 23.402 [5].

7.2.1.3.2 Protocol assumptions

The protocol assumptions are described in the TS 23.402 [5].

NOTE: S103 is expected to be based on GRE, and as such does not involve any secure signalling to exchange GRE keys.

7.2.1.4 Security of the initial access to EPS via HRPD

EAP-AKA' access authentication shall be used according to section 6. As a result of EAP-AKA', the two keys, MSK and EMSK, are generated, cf. RFC 5448 [23].

In addition, according to subclause 6.2 of the present document, the 3GPP AAA Server sends the key MSK to the authenticator in the access network. The 3GPP AAA server shall retain the EMSK either until the subsequent EAP-AKA' authentication, or until it receives an indication that the current authenticated session is finished.

The security contexts in the HRPD access network may be based on keys derived from MSK. The HRPD access network is required to ensure that the identity of a user with whom a security context is established is securely tied to the identity of a user authenticated by EAP-AKA'.

The further details of the establishment of security contexts in the HRPD access network are outside the scope of the present document.

NOTE: Initial access to the EPS via HRPD is described in the TS 23.402 [5].

7.2.1.5 Security of handoff and pre-registration

NOTE: Security of handoff and pre-registration is described in the Section 10 of the present document.

7.2.2 WIMAX EPS Interworking

General Concepts for interworking between EPS and WIMAX are described in TS 23.402 [5].Computation of mobility keys used for MIPv4 interworking with WiMAX access system is specified in clause 9.2.1

7.2.3 Trusted WLAN Access (TWAN)

7.2.3.1 General

A Trusted WLAN Access Network (TWAN) is interfaced with the EPC as a trusted non-3GPP access via the STa interface to the 3GPP AAA Server/Proxy and the S2a interface to the PDN GW as described in clause 16 of TS 23.402 [5].

Authentication and key agreement shall be performed as described in clause 6 and clause 7.2.3.2 of the present document for trusted non-3GPP access. The authenticator shall reside in the TWAN.

The 3GPP AAA Server sendsthe key MSK and key derived from EMSK to the TWAN. The security contexts in the TWAN are based on MSK and key derived from EMSK

The interfaces inside the TWAN shall be integrity- and confidentiality-protected.

NOTE: Integrity- and confidentiality-protection may be provided by cryptographical or physical means.

7.2.3.2 Security for WLAN Control Protocol (WLCP)

7.2.3.2.1 Authentication and key agreement

When multi-connection mode is negotiated as defined in clause 16 of TS 23.402 [39], WLAN Control Protocol (WLCP) is used between the UE and TWAG to control (e.g. setup and teardown) PDN connections over a TWAN access. In this case authentication and key agreement as defined in clause 6.2 of the present document shall be used with the following exceptions and additions:

In step 23, the 3GPP AAA Server derives the WLCP key from the EMSK as defined in Annex A.3, and sends it to the Trusted WLAN AAA Proxy (TWAP) in the TWAN in addition to the MSK, in the underlying AAA protocol message (i.e. not at the EAP level). Upon receiving the EAP Success message, the MSK, and the WLCP key, the TWAP provides the WLCP key, together with the IMSI and the UE MAC address, to the TWAG to be used for protecting the WLCP between the UE and TWAG. The TWAG shall store the received WLCP key together with the IMSI, the UE MAC address and the identity of the tunnel it establishes with the P-GW. The TWAG may also associate the WLCP key with the IP address once the latter has been allocated to the UE. The AAA server, TWAP, and TWAG shall behave as described in this paragraph irrespective of whether the UE MAC address is already in use or not.

NOTE: Using the IP address allocated to the UE, once it has been allocated, as an index for finding the WLCP key needed to verify an incoming WLCP message has the advantage that there is only one WLCP key associated with the IP address while there may be several WLCP keys associated with a UE MAC address when the latter is used at different APs.

Upon successful authentication, the UE derives the WLCP key from the EMSK in the same way as the 3GPP AAA Server does as defined in clause 7.2.3.2.3.

7.2.3.2.2 Fast re-authentication

In case of fast re-authentication the procedures as defined in clause 6.3 shall be used with the exception that the WLCP key is derived and handled in the same way as in the clause 7.2.3.2.1.

7.2.3.2.3 Protection of WLCP signalling

DTLS with pre-shared key as defined in RFC 6347 [37] shall be used to protect WLCP signalling between the UE and TWAG. The key for DTLS is the WLCP key derived as defined in Annex A.3.

The UE shall establish a DTLS connection with the TWAG after successful authentication in case of multi-connection mode.

When receiving a WLCP message, the TWAG shall retrieve the WLCP key(s) associated with the UE MAC address or UE IP address, if already allocated, of the message. If DTLS message authentication is successful for a retrieved WLCP key the TWAG shall use the IMSI and tunnel identifier associated with this WLCP key for further handling of the WLCP message.

7.2.3.2.4 DTLS profile

The UE and the TWAG shall support the DTLS profile as defined in TS 33.310 [38], annex E. DTLS confidentiality is optional for use with WLCP..

7.3 Establishment of security context between UE and untrusted non-3GPP Access

If authentication and key agreement procedure as described optional in subclause 6.4 is performed then also security contexts may be established between UE and non-3GPP access network. However, such additional establishment of security contexts is not required for the security of the Evolved Packet Core in the case of untrusted access.

8 Establishment of security between UE and ePDG

8.1 General

This section details the security mechanisms for procedures for untrusted Non-3GPP IP Accesses specified in TS 23.402 [5].

8.2 Mechanisms for the set up of UE-initiated IPsec tunnels

8.2.1 General

- The UE and the ePDG shall use IKEv2, as specified in RFC 5996 [30],in order to establish IPSec security associations.
- Public key signature based authentication with certificates, as specified in RFC 5996 [30], shall be used to authenticate the ePDG. The ePDG shall authenticate itself to the UE with an identity. This identity shall be the same as the FQDN of the ePDG determined by the ePDG selection procedures defined in TS 23.402 [5]. This identity shall be contained in the IKEv2 ID_FQDN payload and shall match a dNSName SubjectAltName component in the ePDG's certificate.
- EAP-AKA, as specified in RFC 4187 [7], within IKEv2, as specified in RFC 5996 [30], shall be used to authenticate UEs.
- For profile for IKEv2, IPsec ESP and certificate contents and processing refer to subclause 8.2.4.
- For the security aspects of emergency calls, cf. clause 13 of this specification.

8.2.2 Tunnel full authentication and authorization

The tunnel end point in the network is the ePDG. As part of the tunnel establishment attempt the use of a certain APN is requested. When a new attempt for tunnel establishment is performed by the UE the UE shall use IKEv2 as specified in RFC 5996 [30]. The authentication of the UE in its role as IKEv2 initiator terminates in the 3GPP AAA Server. The UE shall send EAP messages over IKEv2 to the ePDG. The ePDG shall extract the EAP messages received from the UE over IKEv2, and send them to the 3GPP AAA Server. The UE shall use the Configuration Payload of IKEv2 to obtain the Remote IP address.

The EAP-AKA message parameters and procedures regarding authentication are omitted. Only decisions and processes relevant to the use of EAP-AKA within IKEv2 are explained.

The message flow for the full authentication is depicted in the Figure 8.2.2-1.

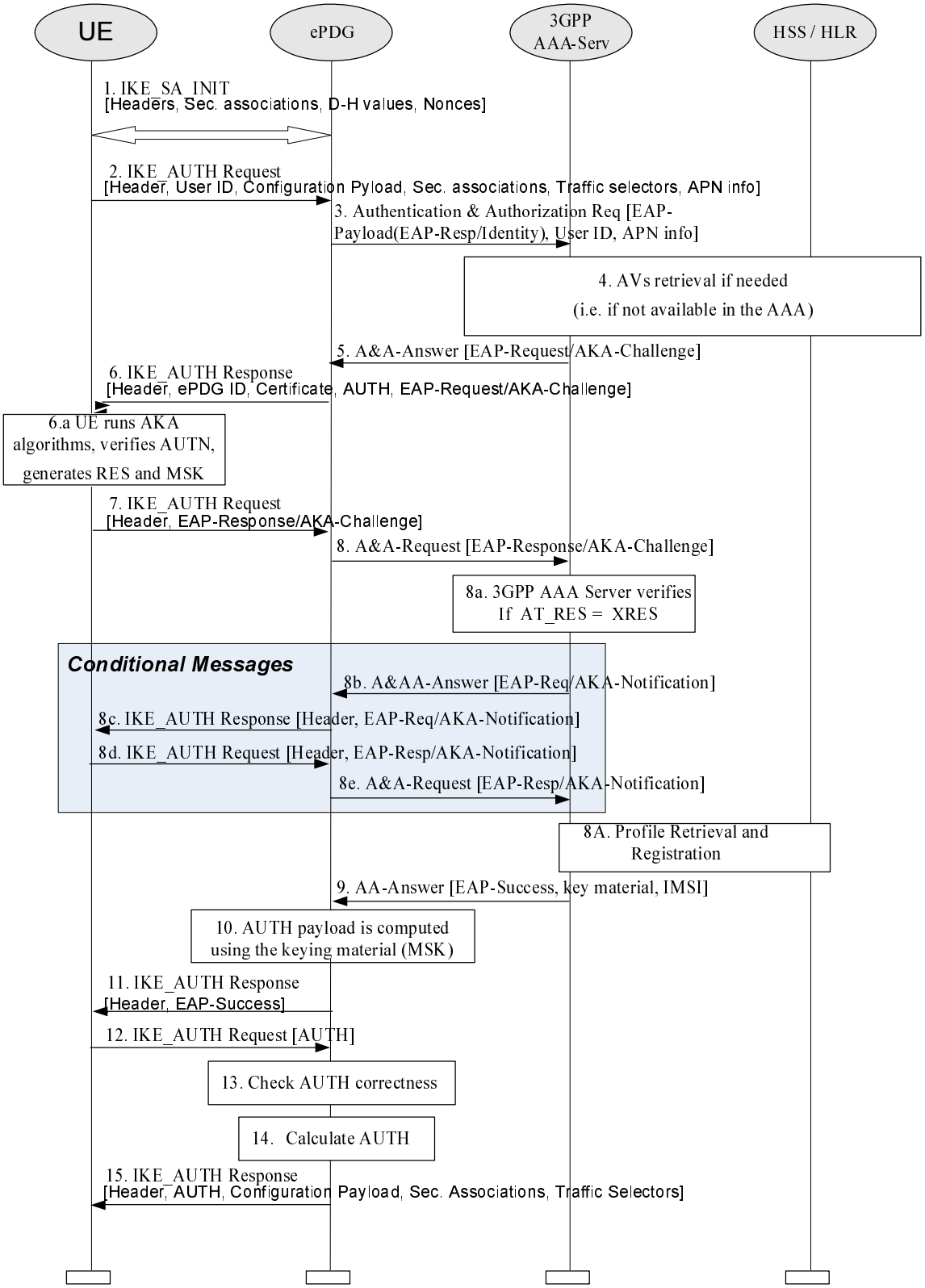

Figure 8.2.2-1: Tunnel full authentication and authorization

As the UE and ePDG generate nonces as input to derive the encryption and authentication keys in IKEv2, replay protection is provided. For this reason, there is no need for the 3GPP AAA Server to request the user identity again using the EAP-AKA specific methods (as specified in RFC 4187 [7]), because the 3GPP AAA Server is certain that no intermediate node has modified or changed the user identity.

1. The UE and the ePDG exchange the first pair of messages, known as IKE_SA_INIT, in which the ePDG and UE negotiate cryptographic algorithms, exchange nonces and perform a Diffie_Hellman exchange.

2. The UE sends the user identity (in the IDi payload) and the APN information (in the IDr payload) in this first message of the IKE_AUTH phase, and begins negotiation of child security associations. The UE omits the AUTH parameter in order to indicate to the ePDG that it wants to use EAP over IKEv2. The user identity shall be compliant with Network Access Identifier (NAI) format specified in TS 23.003 [8], containing the IMSI or the pseudonym, as defined for EAP-AKA in RFC 4187 [7]). The UE shall send the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to obtain an IPv4 and/or IPV6 home IP Address and/or a Home Agent Address. If the UE is provisioned with the ePDG root certificate, it shall include the CERTREQ payload within the IKE_AUTH request message to request ePDG's certificate.

3. The ePDG sends the Authentication and Authorization Request message to the 3GPP AAA Server, containing the user identity and APN. The UE shall use the NAI as defined in accordance with clause 19.3 of 3GPP TS 23.003 [8], the 3GPP AAA server shall identify based on the realm part of the NAI that combined authentication and authorization is being performed for tunnel establishment with an ePDG which allows only EAP-AKA (and not an I-WLAN PDG as defined in TS 33.234 [9], which would allow also EAP-SIM). The different Diameter application IDs will help the 3GPP AAA Server distinguish among authentications for trusted access, as specified in clause 6 of the present document (which requires EAP-AKA' authentication), and authentications for tunnel setup in EPS (which allows only EAP-AKA).

4. The 3GPP AAA Server shall fetch the authentication vectors from HSS/HLR (if these parameters are not available in the 3GPP AAA Server). The 3GPP AAA Server shall lookup the IMSI of the authenticated user based on the received user identity (root NAI or pseudonym) and include the EAP-AKA as requested authentication method in the request sent to the HSS. The HSS shall then generate authentication vectors with AMF separation bit = 0 and send them back to the 3GPP AAA server.

5. The 3GPP AAA Server initiates the authentication challenge. The user identity is not requested again.

6. The ePDG shall respond with its identity, a certificate if the UE has requested with a CERTREQ payload in step 2, and send the AUTH parameter to protect the previous message it sent to the UE (in the IKE_SA_INIT exchange). The EAP message received from the 3GPP AAA Server (EAP-Request/AKA-Challenge) is included in order to start the EAP procedure over IKEv2.

7. The UE checks the authentication parameters and responds to the authentication challenge. The IKE_AUTH request message includes the EAP message (EAP-Response/AKA-Challenge) containing UE's response to the authentication challenge.

8. The ePDG forwards the EAP-Response/AKA-Challenge message to the 3GPP AAA Server.

8.a The AAA checks, if the authentication response is correct.

8.b-e If dynamic IP mobility selection is executed embedded to the authentication and authorization, the selected mobility mode is sent to the user in an AKA-Notification request, over Diameter A&A answer and IKE_AUTH message. The UE responds to this over IKEv2 and the ePDG forwards the response to the 3GPP AAA Server.

8A. The 3GPP AAA Server shall initiate the Subscriber Profile Retrieval and 3GPP AAA Server registration to the HSS. The 3GPP AAA Server checks in user's subscription if he/she is authorized for non-3GPP access.

9. When all checks are successful, the 3GPP AAA Server sends the final Authentication and Authorization Answer (with a result code indicating success) including the relevant service authorization information, an EAP success and the key material to the ePDG. This key material shall consist of the MSK generated during the authentication process. When the SWm and SWd interfaces between ePDG and 3GPP AAA Server are implemented using Diameter, the MSK shall be encapsulated in the EAP-Master-Session-Key-AVP, as defined in RFC 4072 [10].

10. The MSK shall be used by the ePDG to generate the AUTH parameters in order to authenticate the IKE_SA_INIT phase messages, as specified for IKEv2 in RFC 5996 [30]. These two first messages had not been authenticated before as there was no key material available yet. According to RFC 5996 [30], the shared secret generated in an EAP exchange (the MSK), when used over IKEv2, shall be used to generated the AUTH parameters.

11. The EAP Success/Failure message is forwarded to the UE over IKEv2.

12. The UE shall take its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the ePDG.

13. The ePDG checks the correctness of the AUTH received from the UE. At this point the UE is authenticated. In case S2b is used, PMIP signalling between ePDG and PDN GW can now start, as specified in TS 23.402 [5]. The ePDG continues with the next step in the procedure described here only after successful completion of the PMIP binding update procedure.

14. The ePDG calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. The ePDG shall send the assigned Remote IP address in the configuration payload (CFG_REPLY).

15 The AUTH parameter is sent to the UE together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.

8.2.3 Tunnel fast re-authentication and authorization

Fast re-authentication for EAP-AKA is specified in RFC 4187 [7]. Fast re-authentication re-uses keys derived on the previous full authentication. Fast re-authentication does not involve the HSS nor the credentials used with EAP-AKA (e.g. USIM application in case of terminal with 3GPP access capabilities), and does not involve the handling of AKA authentication vectors, which makes the procedure faster and reduces the load on the HSS and, in particular, the Authentication Centre.

The UE and the 3GPP AAA server shall implement fast re-authentication for EAP-AKA. Its use is optional and depends on operator policy.

The security level of fast re-authentication for EAP-AKA is lower as it does not prove the presence of the credentials used with EAP-AKA (e.g.presence of USIM application in case of terminal with 3GPP access capabilities) on the user side. The operator should take this into account when defining the policy on fast re-authentication.

Fast re-authentications for EAP-AKA generates new keys MSK, which may be used for renewing session key used for protection in the non-3GPP access network.

The procedure is very similar to the tunnel full authentication and authorization. The only difference is that EAP fast re-authentication is used in this case.

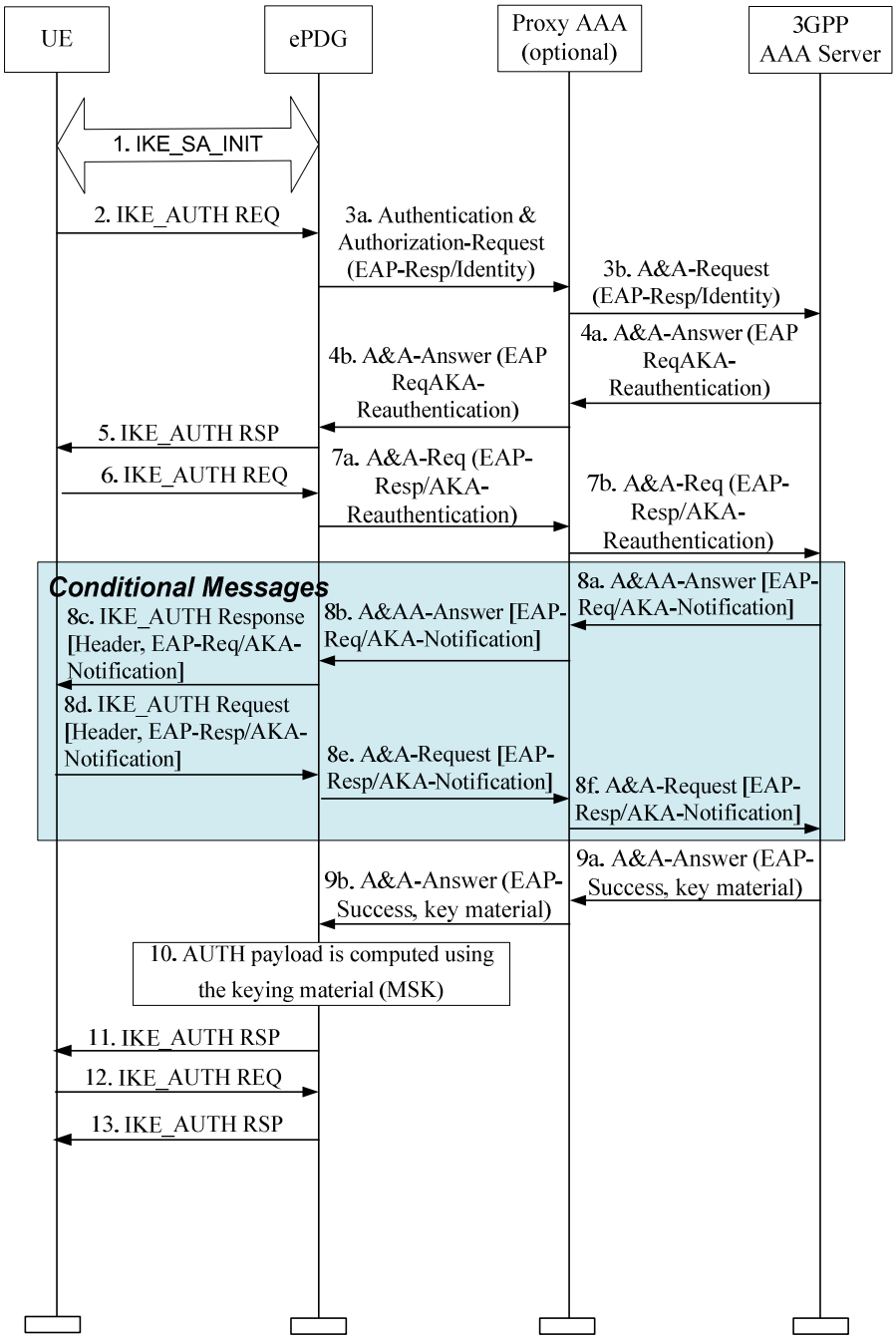

Figure 8.2.3-1: Untrusted Tunnel - Fast Re-authentication

1) The UE and the ePDG exchange the first pair of messages, known as IKE_SA_INIT, in which the ePDG and UE negotiate cryptographic algorithms, exchange nonces and perform a Diffie_Hellman exchange.

2) The UE sends the fast re-authentication identity (in the IDi payload) and the APN information (in the IDr payload) in this first message of the IKE_AUTH phase, and begins negotiation of child security associations. The UE omits the AUTH parameter in order to indicate to the ePDG that it wants to use EAP over IKEv2. The fast re-authentication identity used by the UE shall be the one received in the previous authentication process. If the UE's Remote IP address needs to be configured dynamically, then the UE shall send the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to obtain a Remote IP Address.

3) The ePDG sends the Authentication and Authorization Request message with an EAP-Payload AVP toward the 3GPP AAA Server, containing the fast re-authentication identity. The UE shall use the fast re-authentication

identityto create an NAI, as defined in clause 19.3 of 3GPP TS 23.003 [8]. The 3GPP AAA server shall identify based on the realm part of the NAIthat the combined authentication and authorization is being performed for tunnel establishment with an ePDG (and not an I-WLAN PDG as defined in TS 33.234 [9] , which would allow also EAP-SIM). The different Diameter application IDs will help the 3GPP AAA Server distinguish among authentications for trusted access, as specified in clause 6 of the present document(which requires EAP-AKA' authentication), and authentications for tunnel setup in EPS (which allows only EAP-AKA).

4) The 3GPP AAA Server initiates the fast re-authentication challenge.

5) The ePDG sends an IKE_AUTH Response message to the UE, containing its identity, a certificate, and the AUTH parameter to protect the previous message it sent to the UE (in the IKE_SA_INIT exchange). The EAP message (EAP-Request/AKA-Reauthentication) received from the 3GPP AAA Server is included in order to start the EAP procedure over IKEv2.

6) The UE checks the authentication parameters and responds to the fast re-authentication challenge. The IKE_AUTH request message includes the EAP message (EAP-Response/AKA-Challenge) containing UE's response to the authentication challenge.

7) The ePDG forwards the EAP-Response/AKA-Reauthentication message toward the 3GPP AAA Server.

8) When all checks are successful, if dynamic IP mobility mode selection is executed during the tunnel setup, the selected IP mobility mode is sent via Diameter and IKEv2signaling to the UE.

9) When all checks are successful, the 3GPP AAA Server sends the Authentication Answer including the user's IMSI, the relevant service authorization information, an EAP success and the key material toward the ePDG. This key material shall consist of the MSK generated during the fast re-authentication process. When the SWm interface (ePDG-AAA) is implemented using Diameter, the MSK shall be encapsulated in the EAP-Master-Session-Key AVP, as defined in RFC 4072 [10].

10) The MSK shall be used by the ePDG to generate the AUTH parameters in order to authenticate the IKE_SA_INIT phase messages, as specified in RFC 5996 [30]. These two first messages had not been authenticated before as there were no key material available yet. According to RFC 5996 [30], the shared secret generated in an EAP exchange (the MSK), when used over IKEv2, shall be used to generated the AUTH parameters.

11) The EAP Success message is forwarded to the UE over IKEv2.

12) The UE shall take its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the ePDG.

13) The ePDG checks the correctness of the AUTH received from the UE and calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. The ePDG shall send the assigned Remote IP address in the configuration payload (CFG_REPLY), if the UE requested for a Remote IP address through the CFG_REQUEST. Then the AUTH parameter is sent to the UE together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.

8.2.4 Security profiles

8.2.4.1 Profile of IKEv2

When IKEv2 [30] is used in the context of this specification the profile specified in this section shall be supported by the ePDG and the WLAN-UE. IKEv2 shall meet the profiling given in clause 5.4.2 of TS 33.210 [6] and clause 6.2.1b of TS 33.310 [12].

For the certificate based IKEv2 authentication using the ePDG certificate the profiling given in TS 33.310 [12] shall apply.

For NAT traversal, the NAT support of IKEv2 shall be supported as specified in section 2.23 of IETF RFC 5996 [30].

8.2.4.2 Profile of IPSec ESP

When IPSec ESP [30] is used in the context of this specification the profile specified in this section shall be supported. IPsec ESP shall meet the profiling of encryption and authentication transforms given clause 5.3 of TS 33.210 [6] with the following additions:

- Tunnel mode shall be used.

For NAT traversal, the UDP encapsulation for ESP tunnel mode specified in reference [35] shall be supported.

8.2.4.3 Profile for ePDG certificates

Certificates used for authentication of the ePDG shall meet the certificate profiles given in TS 33.310 [12] as follows: clause 6.1.3, for SEG certificates shall apply to ePDG certificates, and clause 6.1.4 for SEG CA certificates shall apply to any CA certificates used in a chain to validate ePDG certificates, with the following additions and exceptions:

a) The subject name may be empty in ePDG certificates.

b) The issuerUniqueID or subjectUniqueID fields shall not be present.

c) The SubjectAltName extension shall contain at least one dNSName component.

d) CA certificates should contain the NameConstraints extension with appropriate dNSName components in the permittedSubtrees field.

e) The keyCertSign bit shall be set in CA certificates, and digitalSignature bit shall be set in ePDG certificates.

f) The CRLDistributionPoint extension may be present, and shall not be marked critical. At least one of the distribution points should use HTTP for retrieving the CRL.

g) The AuthorityInformationAccess extension may be present with id-ad-ocsp access method, and shall not be marked critical.

h) Other extensions should not be used; if they are, they shall not be marked as critical.

i) The root CA and any intermediate CAs shall be trusted by the operator, but may be located outside the security domain of the operator.

Certificate processing requirements:

a) UE shall send one or more CERTREQ payloads with encoding value 4 (X.509 certificate - Signature).

b) IKEv2 Certificate encoding value shall be 4 (X.509 certificate - Signature).

c) UE shall not assume that any except the first IKEv2 CERT payload is ordered in any way.

d) UE shall be able to support certificate paths containing up to four certificates (e.g. self-signed CA certificate, intermediate CA 1, intermediate CA 2, ePDG certificate) (and may support longer path lengths), where the intermediate CA certificates and the ePDG certificate are obtained from the IKEv2 CERT payload and the self-signed CA certificate is obtained from a UE local store of trusted root certificates.

e) ePDG shall not send paths containing more than four certificates.

f) UE shall be prepared to receive irrelevant certificates, or certificates they do not understand.

g) UE shall be able to process certificates (for e.g. chain building) even if naming attributes are unknown.

h) UE shall support both UTCTime and GeneralizedTime encoding for validity time.

i) UE shall check the validity time, and reject certificates that are either not yet valid or are expired.

j) UE shall support processing of the BasicConstraints, NameConstraints, and KeyUsage extensions.

k) UE may check the validity of the certificates using CRLs or OCSP [42]. Support for CRLs is optional in the UE. Support for OCSP is mandatory in the UE. In addition, the UE and the ePDG may support the extensions to IKEv2, which enable the use of OCSP for in-band signalling of certificate revocation status, according to [43].

The signature algorithm for CRLs and OCSP responses shall comply with the requirements for the CRL profile in TS 33.310 [12], clause 6.1a. If the OCSP profile in [42] is used, support for WAP specific protocols shall not be required.

NOTE 2: A UE that initiates 3GPP IP Access according to the tunnel full authentication and authorization procedure, may want to check the validity of the ePDG certificate, but it might not gain access to the OCSP server. This situation can be handled in the following way: After the UE initiated tunnel is successfully established and before user data is transmitted in the tunnel, the UE sends an OCSP request message to OCSP server. When the UE receives the OCSP response, it checks the certificate status. If the certificate of ePDG is valid, the UE will allow user data to be transmitted to the ePDG in the tunnel. If the certificate is not valid, the UE may terminate the tunnel that just was established.

8.2.5 Handling of IPsec tunnels in mobility events

8.2.5.1 General

The below sections describe the handling of IPsec tunnels in the idle and active mode mobility events when the target access has a UE and an ePDG, e.g. I-WLAN 3GPP IP Access System. In general, the IPsec tunnel handling during mobility events is managed by the end nodes where the IPsec tunnel is terminated, i.e. the UE and the ePDG.

In the case when the UE moves from the coverage area of the source ePDG and connect to another ePDG or a different access, the management of the IPsec tunnel between the UE and the source ePDG should be handled as follows:

1. The UE may keep all related IPsec tunnel security association parameters until its lifetime expires.
2. If after repeated attempts to contact the UE, the source ePDG concludes that the other endpoint (UE) has failed and all of its attempts have gone unanswered for a timeout period as specified in RFC 5996 [30], the source ePDG may delete all the UE IPsec tunnel SA parameters.
3. If the source ePDG receieves an indication from a trusted network element that the UE has moved outside its coverage area, e.g. 3GPP AAA server, the source ePDG can delete all of the UE IPsec tunnel security association parameters.

8.2.5.2 Idle mode mobility

When the UE moves from a source access where the UE is connected to an ePDG to a target access that involves the UE and the same ePDG, the UE shall use MOBIKE as per RFC 4555 [18] to update the ePDG with its new IP address. However, when the UE moves where the target access involves the UE and a different ePDG, the UE shall establish a new IPsec tunnel with the new ePDG as described in subclause 8.2.2.

On the other hand, if the UE is connected to EPS without being connected to an ePDG and then moves to a target access which involves the UE and an ePDG, the UE SHALL establish a new IPsec tunnel with the new ePDG as described in subclause 8.2.2.

8.2.5.3 Active mode mobility

When the UE moves from a source access where the UE is connected to an ePDG to a target access that involves the UE and the same ePDG, the UE shall use MOBIKE as per RFC 4555 [18] to update the ePDG with its new IP address. However, when the UE moves where the target access involves the UE and a different ePDG, the UE shall establish a new IPsec tunnel with the new ePDG as described in subclause 8.2.2.

On the other hand, if the UE is connected to EPS without being connected to an ePDG and then moves to a target access which involves the UE and an ePDG, the UE SHALL establish a new IPsec tunnel with the new ePDG as described in subclause 8.2.2.

9 Security for IP based mobility signalling

9.1 General

Clause 9.2 covers security for host based mobility and section 9.3 covers security for network based mobility.

9.2 Host based Mobility

9.2.1 MIPv4

9.2.1.1 General

MIPv4 FACoA and DSMIPv6 host based mobility protocols are supported over S2a and S2c interfaces respectively TS 23.402 [5].

The MIPv4 security is based on MIP Authentication extensions as defined in RFC 3344 [17]. The MIPv4 signalling messages shall be protected between the UE and the node acting as HA (i.e PDN GW) using MIP authentication extensions and optionally between the UE and the node acting as FA (non-3GPP access specific).

9.2.1.2 Bootstrapping of MIPv4 FACoA parameters

9.2.1.2.1 Procedures

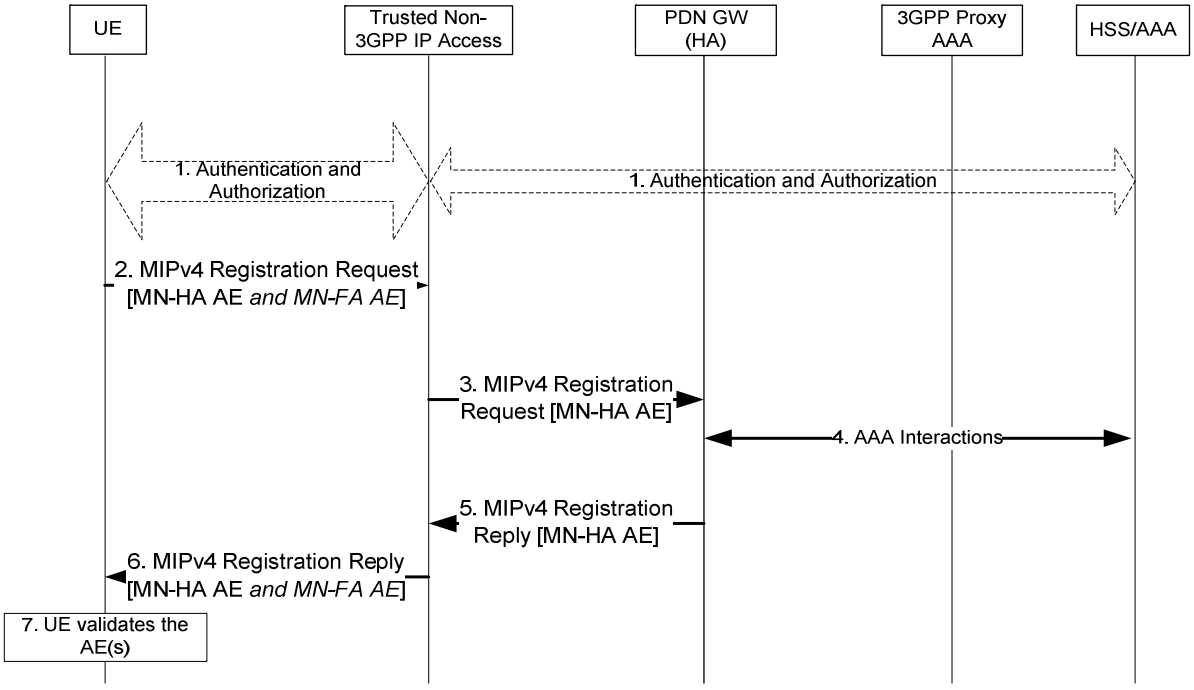

Figure 9.2.1.2.1-1: MIPv4 bootstrapping

The event that triggers Authentication and Authorization in step 1 between the Trusted Non-3GPP IP Access and the EAP Server, depends on the specific access technology cfr.TS 23.402 [5].

1) The Non-3GPP access specific authentication procedure based on EAP-AKA' is performed as specified in clause 6.2. Depending on the type of non-3GPP access system, the PDN GW address (HA address) may be determined at this point. The details of this procedure and IPMM protocol selection procedure are specified in TS 23.402 [5].

If the network selects mobility management protocol as MIPv4 FACoA for the UE, then the UE and the EPC derive the keys required for MIPv4 bootstrapping.

The key EMSK that result from the EAP-AKA' authentication procedure is used to derive MIPv4 bootstrapping keys. Section 9.2.1.2.2 shows the derivation of MIPv4 bootstrapping keys in the UE and in the 3GPP AAA server and the key distribution from the 3GPP AAA server to the mobility agents. The trusted non-3GPP network receives a set of mobility keys and other keys in the Access-Accept message as a result of successful authentication.

2) The UE sends a Registration Request (RRQ) message to the FA as specified in TS 23.402 [5]. The UE includes the MN-HA Authentication Extension (AE) and optionally the MN-FA Authentication Extension (AE) as specified in RFC 3344 [17].

3) The FA processes the message according to RFC 3344 [17] and validates the MN-FA Authentication extension if present. The FA then forwards the RRQ message to the PDN GW. The RRQ message shall be protected between the FA and the PDN GW according to TS 33.210 [6].

4) The selected PDN GW obtains Authentication and Authorization information from the AAA/HSS.

5) The PDN GW validates the MN-HA authentication extension. After successful authentication extension validation, the PDN GW sends a Registration Reply (RRP) to the UE through the FA. The RRP message shall be protected between the PDN GW and the FA according to TS 33.210 [6].

6) The FA processes the RRP according to RFC 3344 [17]. The FA then forwards the RRP message to the UE. The FA includes the MN-FA authentication extension, if the FA received MN-FA authentication extension in the RRQ message.

7) The UE validates the MN-HA authentication extension and MN-FA authentication extension, if present.

9.2.1.2.2 MIPv4 Key Derivation

The Mobile IP Root Key (MIP-RK) is generated at the 3GPP AAA Server and the UE. The MIP-RK is generated from the EMSK according to RFC 5295[19] using the following formula:

MIP-RK-1 = HMAC-SHA256(EMSK , usage-data | 0x01)

MIP-RK-2 = HMAC-SHA256(EMSK, MIP-RK-1 | usage data | 0x02)

MIP-RK = MIP-RK-1 | MIP-RK-2

where:

"|"denotes concatenation

usage-data = key label + "\0" + length

key label = miprk@wimaxforum.org in ASCII

length = 0x0200 the length in bits of the MIP-RK expressed as a 2 byte unsigned integer in network order

The length of the MIP-RK is 64 octets. The lifetime of MIP-RK is set to the lifetime of EMSK. The MIP-RK is stored in the 3GPP AAA Server. At the 3GPP AAA Server each user session is associated with a single MIP-RK. The MIP-RK is used to generate mobility keys. The MIPv4 keys are generated at the 3GPP AAA Server and at the UE. The keys generated at the 3GPP AAA Server are transported to the HA and the Authenticator in the trusted non-3GPP network by the use of the AAA protocol.

Security Parameter Indices (SPI) is generated from the MIP-RK as follows:

MIP-SPI = the 4 most significant bytes of HMAC-SHA256 (MIP-RK, "SPI CMIP PMIP "| APN))

SPI-CMIP4 = MIP-SPI,

Values MIP-SPI+1, MIP-SPI+2, and MIP-SPI+3 are reserved.

APN is used as an input parameter for deriving unique MIP-SPI, MN-HA key and MN-FA key per PDN connection. For default PDN connection, the UE does not provide an APN. In this case APN shall be omitted from the derivation of MIP-SPI, MN-HA key and MN-FA key.

The MIP-SPI and SPI-CMIP4 are derived at the UE and at the 3GPP AAA server.

The following procedure prevents collision between SPI values used for different Mobility keys, for example, mobility keys used by other access technologies, during the same Mobile IP session. The procedure SHALL be executed as follows:

a. First, if the absolute value of the difference between the MIP-SPI and any currently active SPI is less than 4, the MIP-SPI value SHALL be incremented by FOUR until the current condition is satisfied.

b. Next, if the MIP-SPI value is less than THREE smaller than the maximum possible value of SPI (2^{32} - 1), the MIP-SPI value SHALL be incremented by 259.

c. Last, the process specified in Step 1 SHALL be applied again until the condition specified in Step 1 is satisfied.

The SPI value is used by the UE, HA, and 3GPP AAA server to identify the MN-HA key used to compute the MN-HA Authentication Extension in the RRQ message. In addition, MIP-SPI is distributed to the authenticator during Access Authentication, in AAA protocol attribute FA-RK-SPI, to identify the FA-RK key. FA-RK key and FA-RK-SPI will be used to further derive MN-FA key and MN-FA-SPI, to compute the MN-FA Authentication Extension in the RRQ message. When the lifetime of the MIP-RK expires the lifetime of the SPIs derived from it shall also expire.

The derivation of mobility key is given below:

MN-HA = HMAC-SHA1(MIP-RK," CMIP4 MN HA" | HA-IPv4 | MN-NAI | APN)

The lifetime of all MN-HA keys shall be set to the lifetime of the MIP-RK. During the initial attach or additional PDN connectivity, the UE may not know the HA IP address. In this case, the UE use ALL-ZERO-ONE-ADDR [21] in the RRQ message to request for dynamic HA assignment. Under this case, the UE shall derive the MN-HA key using the ALL-ZERO-ONE-ADDR as the HA-IPv4 address and use this key for deriving MN-HA Authentication Extension and send in the RRQ. Then the HA informs this to the 3GPP AAA server in the AAA protocol message. In response from the 3GPP AAA server, the HA will receive RRQ-MN-HA-KEY that is calculated based on ALL-ZERO-ONE-ADDR address and also MN-HA key that is calculated based on HA IP address. The HA shall use the RRQ-MN-HA-KEY for validation of MN-HA Authentication Extension in the received RRQ. The HA then use MN-HA key for deriving RRP MN-HA Authentication Extension and sends the HA IP address as part of the RRP message. The UE shall recalculate the MN-HA key using the HA IP address received in the RRP and use this key for MN-HA Authentication Extension validation for the RRP. If the MN-HA authentication extension is valid, the new MN-HA key shall be in effect.

The derivation of FA-RK and MN-FA mobility keys are given below:

FA-RK = HMAC-SHA1(MIP-RK, "FA-RK")

MN-FA = HMAC-SHA1(FA-RK, "MN FA" | FA-IP | MN-NAI | APN)

The FA-RK is generated by the 3GPP AAA Server and distributed to the Authenticator. It is used by the Authenticator to derive MN-FA keys as requested by the FA. The MN-FA key is derived based on the FA-IP address to separate keys between different FAs for the same authentication session. The lifetime of FA-RK and MN-FA shall be set to the lifetime of the MIP-RK. The SPI associated with the MN-FA (MN-FA-SPI) is set to the same value of FA-RK-SPI distributed during Access Authentication.

During EAP-Re-authentication, the 3GPP AAA server and the UE generate new MIP-RK, SPI, MN-HA and FA-RK. The old MIP-RK and its derivatives (MN-HA, FA-RK, MN-FA) shall be deprecated after confirming that the newly generated mobility keys in the 3GPP AAA server and the UE are the same. Upon receipt of an MIP-RRQ from the UE, the HA shall determine whether re-authentication has occurred since the last MIP-RRQ by comparing the SPI contained in the MN-HA Authentication extension of the received MIP-RRQ to the locally stored value. If the two SPIs are different, the HA shall assume that re-authentication has occurred, and the new MN-HA key shall be retrieved from the 3GPP AAA server. After verifying the MIP-RRQ message with the new MN-HA key and creating the MIP-RRP Authentication Extension, the HA deprecate the old key. The UE shall deprecate the old key, once it successfully verifies the MIP-RRP using the new key.

9.2.1.2.3 Key Usage

Key	Generated by	Used at
MN-HA	UE and 3GPP AAA server	HA and UE
FA-RK	UE and 3GPP AAA server	UE and Authenticator
MN-FA	UE and Authenticator	FA and UE

The keys that are used by the UE are generated by the UE and shall not be transported outside the UE. The keys generated by the 3GPP AAA Server are transported to the HA or the Authenticator using AAA protocols.

9.2.1.2.4 Key Distribution for MIPv4

In this section, key distribution for MIP4 is described. Two scenarios are possible, where in the first scenario Authenticator and FA are co-located and in the case of FA relocation, also the Authenticator changes based on EAP re-authentication. In the second scenario, no re-authentication takes place when the FA is relocated, so the anchor Authenticator is continued to be used, and provisions the new FA with the required mobility keys. However key handling between Authenticator and FA is out of scope of the present document.

The Authenticator receives FA_RK in the RADIUS/DIAMETER Access-Accept message as a result of successful authentication. The keys are stored at the authenticator.

The 3GPP AAA Server distributes the MN-HA key, if requested, to the HA using RADIUS/DIAMETER Access-Accept.

9.2.2 DS-MIPv6

9.2.2.1 General

The DS-MIPv6 security is based on IPsec as defined in RFC 4877 [2]. The IPsec security association is established between the UE and the node acting as HA (i.e. PDN GW).

The following principles apply:

- The UE and the HA shall use IKEv2, as specified in RFC 5996 [30], in order to establish IPsec security associations.
- Public key signature based authentication with certificates, as specified in RFC 5996 [30], is used to authenticate the HA. The HA shall authenticate itself to the UE with an identity. This identity shall be the same as the FQDN of the HA if the HA is found via DNS cfr. TS 23.402 [5].
- EAP-AKA, as specified in RFC 4187 [7], within IKEv2, as specified in RFC 4877 [2] and RFC 5996 [30], is used to authenticate UEs.

The following properties are needed to provide secure S2c over a Trusted Non-3GPP Access:

- The Trusted Access will authenticate the UE and provide a secure link for the data to be transferred from the UE to the Trusted Access.
- The Trusted Access protects against source IP address spoofing.
- The Trusted Access and PDN GW will have a secure link between them to transfer the user's data across.
- The Trusted Access and EPC need to co-ordinate when the UE detaches from the Trusted Access in order to ensure that the IP address that was assigned to the UE is not be used by another UE without EPC being aware of the change (i.e. enable the PDN GW to remove the CoA address binding for the old UE).

These properties ensure that the traffic the PDN GW is receiving has originated at the UE while UE is attached to the Trusted Access. These properties may be provided using enhanced security mechanisms defined in clause 9.2.2.4.

NOTE 1: If Trusted Access and EPC do not co-ordinate regarding UE detachment then the UE that was re-assigned the IP address would be capable of impersonating traffic until the binding in PDN GW timed out. NOTE 2: Procedures internal to the Trusted Access are outside the scope of the present document.

The allocation of IP addresses in the access network may provide the last property listed above. If the IP address is not re-allocated until after the MIP Binding has expired or IKE Dead Peer Detection has been run. This means that the PDN GW will no longer associate the old UE to the IP address once the new UE gets the IP address and hence there is no risk of impersonation attacks.

PCC may also be used to provide the last property listed above in access networks that support it. In the case that PCC is used, a GW control session is established between the Trusted Access and the PCRF. This GW control session is identified by the UE ID and the IP address allocated to the UE (i.e. CoA if DSMIPv6 is used). Using the GW control session, the UE is restricted to limited access; in particular, the Trusted Access restricts the forwarding of the packets only to IKEv2 and BU messages until the binding at the PDN GW is established. The Trusted Access knows when the binding is established at the PDN GW because it receives an update of the GW control session. The flows for this control of policy are given in section(s) 6.3 and 6.6.2 of TS 23.402. This prevents a UE that attaches to the Trusted Access from sending non-signalling traffic to the PDN GW until it has completed a BU with the PDN GW and prevents an impersonation attack.

9.2.2.2 Bootstrapping of DSMIPv6 parameters

9.2.2.2.1 Full Authentication and authorization

The first procedure that must be performed by the MN is the discovery of the HA address, which in case of EPS is the IP address of the PDN GW. The detailed of this procedure are specified in TS 23.402 [5] and TS 24.303 [20].

As soon as the Mobile Node has discovered the PDN GW address, it establishes an IPsec Security Association with the Home Agent itself through IKEv2. The detailed description of this procedure is provided in RFC4877 [2]. The IKEv2 Mobile Node to Home Agent authentication is performed using Extensible Authentication Protocol (EAP).

When the Mobile Node runs IKEv2 with its Home Agent, it shall request an IPv6 Home Network Prefix through the Configuration Payload in the IKE_AUTH exchange by including an MIP6_HOME_PREFIXattribute.

When the Home Agent processes the message, it allocates a Home Network Prefix and sends it a CFG_REPLY message. The UE shall then auto-configure a Home Address from the IPv6 prefix received from the HA.

The IPv6 Home Network Prefix allocation through IKEv2 allows to bind the Home Address with the IPsec security association so that the MN can only send Binding Updates for its own Home Address and not for other MN's Home Addresses.

Figure 9.2.2.2.1-1 provides the flow for the initial DS-MIPv6 bootstrapping, focusing on the security aspects of the flow.

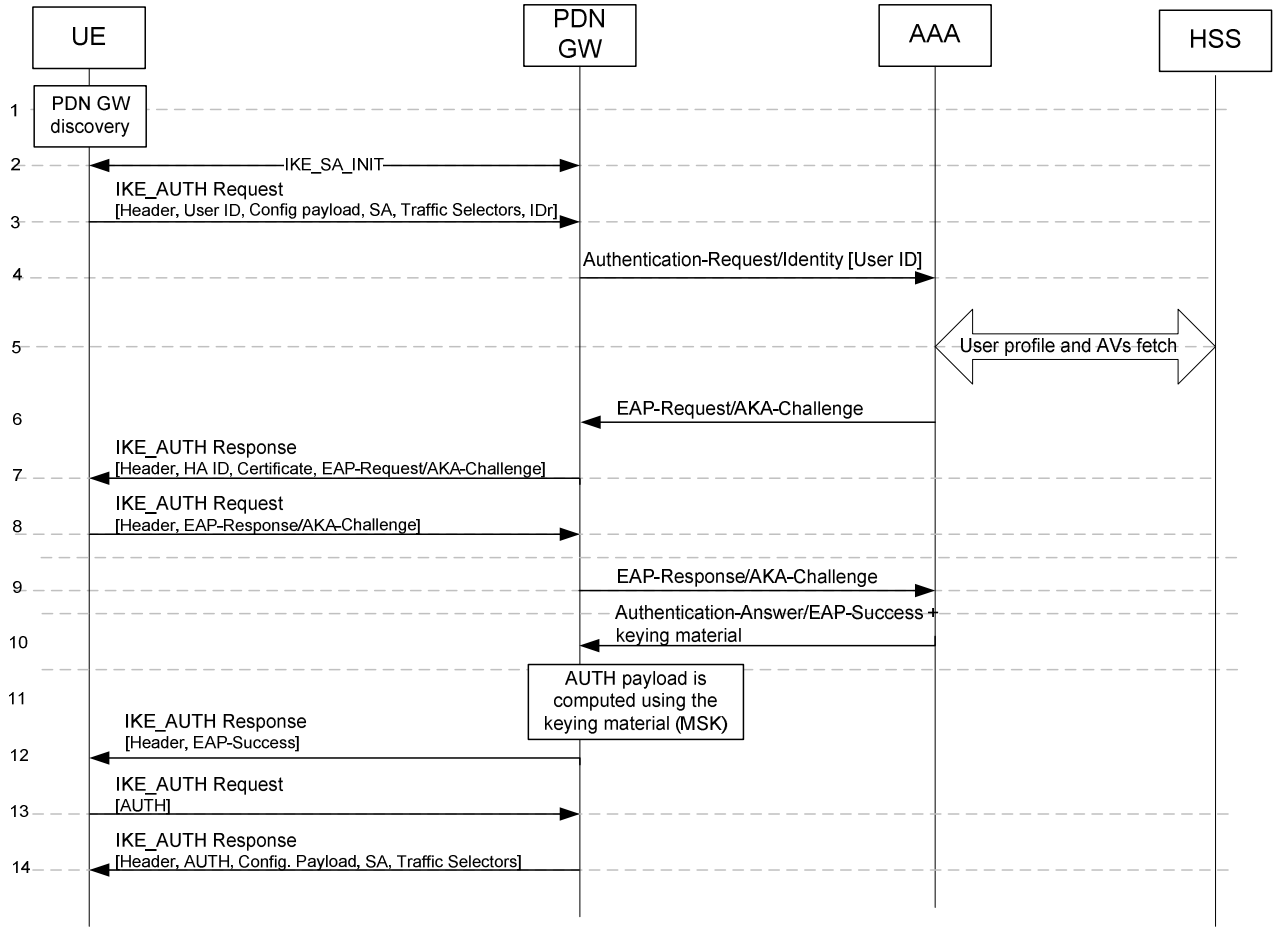

Figure 9.2.2.2.1-1: DS-MIPv6 bootstrapping based on IKEv2

1) The UE discovers the PDN GW address based on the procedure specified in TS 23.402 [5].

2) The UE starts an IKEv2 exchange with the PDN GW. The first part of this exchange is an IKE_SA_INIT exchange. In this phase the PDN GW and UE negotiate cryptographic algorithms, exchange nonces and perform a Diffie-Hellman exchange.

3) The UE sends the user identity (in the IDi payload) and the APN identifier (in the IDr payload) in this first message of the IKE_AUTH phase, and begins negotiation of child security associations. The UE omits the AUTH parameter in order to indicate to the PDN GW that it wants to use EAP over IKEv2. The user identity shall be compliant with Network Access Identifier (NAI) format specified in TS 23.003 [8], containing the IMSI or the pseudonym, as defined for EAP-AKA in RFC 4187 [7]). The UE shall send the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to obtain an IPv6 Home Network Prefix as specified in 3GPP TS 24.303 [20]. The UE shall include the Traffic Selectors to protect DS-MIPv6 signalling as specified in RFC4877 [2].

4) The PDN GW sends the Authentication Request message with an EAP AVP to the 3GPP AAA Server, containing the user identity, APN and a parameter indicating that the authentication is being performed for DS-MIPv6 security. For the communication between PDN GW and 3GPP AAA server, cf. also [4].

5) The 3GPP AAA Server shall fetch the user profile and authentication vectors from HSS/HLR (if these parameters are not available in the 3GPP AAA Server). The 3GPP AAA Server shall include the parameter received in step 4 indicating that the authentication is being performed for DSMIPv6 in the request to the HSS. The HSS shall then generate authentication vectors with AMF separation bit = 0 and send them back to the 3GPP AAA server. The AAA checks that the UE is authorised to use the APN.

6) Based on the identity received, the 3GPP AAA server selects an Authentication Vector (RAND, AUTN, CK, IK, XRES) for the UE. The 3GPP AAA Server then initiates the authentication challenge by sending the EAP-Request/AKA-Challenge containing RAND and AUTN as described by RFC 4187 [7]. The user identity is not requested again, as in a normal authentication process, because there is the certainty that the user identity received in the EAP Identity Response message has not been modified or replaced by any intermediate node.

The reason is that the user identity was received via an IKEv2 secure channel which can only be decrypted and authenticated by the end points (the PDN GW and the UE).

7) The PDN GW responds to the UE with its identity, a certificate, and sends the AUTH parameter to protect the previous message it sent to the UE (in the IKE_SA_INIT exchange). The EAP message received from the 3GPP AAA Server (EAP-Request/AKA-Challenge), which contains RAND and AUTN, is included in order to start the EAP procedure over IKEv2.

8) The UE checks whether the AUTN is correct [11] and if so calculates CK, IK and RES and passes these to the UE. The UE checks the IKE authentication parameters and responds to the authentication challenge. The IKE_AUTH request message includes the EAP message (EAP-Response/AKA-Challenge) containing UE's response to the authentication challenge.

9) The PDN GW forwards the EAP-Response/AKA-Challenge message to the 3GPP AAA Server.

10) The 3GPP AAA Server checks the EAP message including that RES = XRES and then calculates MSK from CK and IK as described in RFC 4187 [7]. The 3GPP AAA Server sends the Authentication Answer including an EAP success and the key material to the PDN GW. This key material shall consist of the MSK generated during the authentication process. In case of PDN GW reallocation upon attach on S2c, the AAA shall include the target PDN GW's identity as specified in 3GPP TS 23.402 [5].

11) The AUTH payload is computed using the received MSK.

12) The EAP Success message is forwarded to the UE over IKEv2.

13) The UE also generates MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the PDN GW.

14) The PDN GW checks the correctness of the AUTH received from the UE and calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. The PDN GW shall send the assigned Home Network prefix in the configuration payload (CFG_REPLY) as specified in 3GPP TS 24.303 [20], except in the case of PDN GW reallocation upon attach on S2c, when the PDN GW shall send to the UE the target PDN GW's address as specified in 3GPP TS 23.402 [5]. Then the AUTH parameter is sent to the UE together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.

    In the case PDN GW reallocation, the UE shall begin a new DSMIPv6 bootstrapping with the target PDN GW.

9.2.2.2.2 Fast re-authentication and authorization

Fast re-authentication for EAP-AKA is specified in RFC 4187 [7]. Fast re-authentication re-uses keys derived on the previous full authentication. Fast re-authentication does not involve the HSS nor the credentials used with EAP-AKA (e.g. USIM application in case of terminal with 3GPP access capabilities), and does not involve the handling of AKA authentication vectors, which makes the procedure faster and reduces the load on the HSS and, in particular, the Authentication Centre.

The UE and the 3GPP AAA server shall implement fast re-authentication for the use of EAP-AKA with DSMIPv6. Its use is optional and depends on operator policy.

The security level of fast re-authentication for EAP-AKA is lower as it does not prove the presence of the EAP-AKA credentials (e.g. USIM application in case of terminal with 3GPP access capabilities) on the user side. The operator should take this into account when defining the policy on fast re-authentication.

Fast re-authentications for EAP-AKA generates new keys MSK, which may be used for renewing session key used for protection in the non-3GPP access network.

The procedure is very similar to the tunnel full authentication and authorization. The only difference is that EAP fast re-authentication is used in this case.

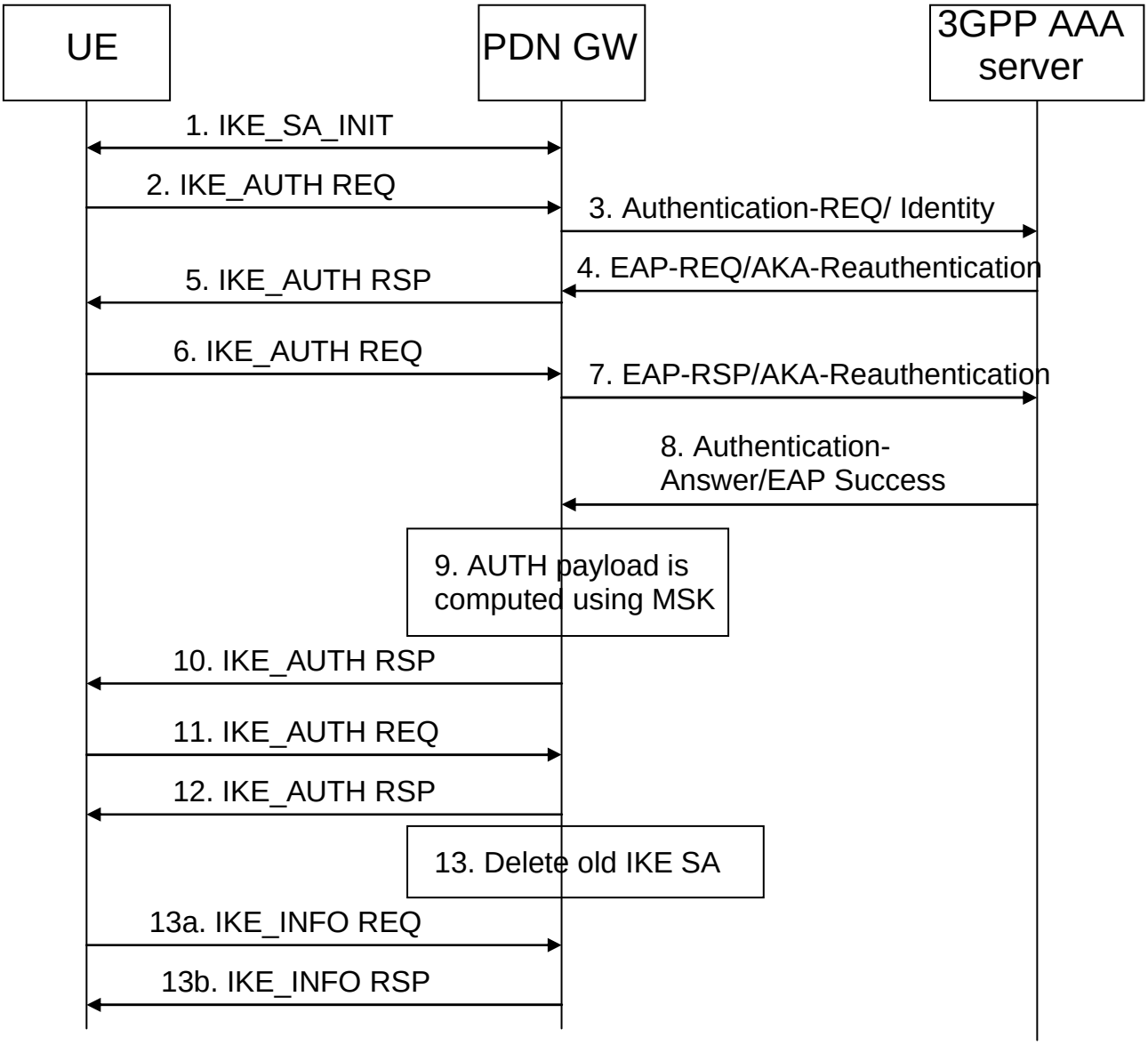

Figure 9.2.2.2.2-1: Fast Re-authentication for DSMIPv6

1) The UE and the PDN GW exchange the first pair of messages, known as IKE_SA_INIT, in which the PDN GW and UE negotiate cryptographic algorithms, exchange nonces and perform a Diffie_Hellman exchange.

2) The UE sends the re-authentication identity (in the IDi payload) and the APN information (in the IDr payload) in this first message of the IKE_AUTH phase, and begins negotiation of child security associations. The UE omits the AUTH parameter in order to indicate to the PDN GW that it wants to use EAP over IKEv2. The re-authentication identity used by the UE shall be the one received in the previous authentication process. If the UE's Remote IP address needs to be configured dynamically, then the UE shall send the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to obtain a Remote IP Address.

3) The PDN GW sends the Authentication Request message with an EAP AVP toward the 3GPP AAA Server, containing the re-authentication identity. The PDN GW shall include the APN and a parameter indicating that the authentication is being performed for DSMIPv6 with a PDN GW. This will help the 3GPP AAA Server distinguish among authentications for DSMIPv6, trusted access, as specified in clause 6 of the present document, authentications for tunnel setup in I-WLAN (which would allow also EAP-SIM) and authentications for tunnel setup in EPS (which allow only EAP-AKA). The AAA checks that the UE is authorised to use the APN.

4) The 3GPP AAA Server initiates the fast re-authentication challenge.

5) The PDN GW sends an IKE_AUTH Response message to the UE, containing its identity, a certificate, and the AUTH parameter to protect the previous message it sent to the UE (in the IKE_SA_INIT exchange). The EAP

message (EAP-Request/AKA-Reauthentication) received from the 3GPP AAA Server is included in order to start the EAP procedure over IKEv2.

6) The UE checks the authentication parameters and responds to the fast re-authentication challenge. The IKE_AUTH request message includes the EAP message (EAP-Response/AKA-Challenge) containing UE's response to the authentication challenge.

7) The PDN GW forwards the EAP-Response/AKA-Reauthentication message toward the 3GPP AAA Server.

8) When all checks are successful, the 3GPP AAA Server sends the Authentication Answer including an EAP success and the key material toward the PDN GW. This key material shall consist of the MSK generated during the fast re-authentication process. When the Wm interface (ePDG-AAA) is implemented using Diameter, the MSK shall be encapsulated in the EAP-Master-Session-Key parameter, as defined in RFC 4072 [10].

9) The MSK shall be used by the PDN GW to generate the AUTH parameters in order to authenticate the IKE_SA_INIT phase messages, as specified in RFC 5996 [30]. These two first messages had not been authenticated before as there was no key material available yet. According to RFC 5996 [30], the shared secret generated in an EAP exchange (the MSK), when used over IKEv2, shall be used to generated the AUTH parameters.

10) The EAP Success message is forwarded to the UE over IKEv2.

11) The UE shall take its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the PDN GW.

12) The PDN GW checks the correctness of the AUTH received from the UE and calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. The PDN GW shall send the assigned Remote IP address in the configuration payload (CFG_REPLY), if the UE requested for a Remote IP address through the CFG_REQUEST. Then the AUTH parameter is sent to the UE together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.

9.2.2.3 Security Profiles

The profiles for IKEv2 and IPsec ESP as defined in clauses 8.2.4.1 and 8.2.4.2 of the present specification shall be used with the exception that ESP in transport mode shall be used.

For PDN GW certificates, the certificate profiles as defined in clause 8.2.4.3 of the present specification shall be used.

9.2.2.4 Enhanced Security Support

The UE and the PDN GW may support integrity protection and/or confidentiality protection of user plane traffic exchanged over the S2c tunnel when the UE is in a trusted non-3GPP access.This is achieved as follows: after the establishment of the s2c tunnel, the UE or the PDN GW may trigger the creation of a pair of IPsec child SAs as specified in RFC 4877 [2]. This may be deactivated by the UE or the PDN GW by initiating the deletion of the corresponding child SAs.

The profiles for IKEv2 and IPsec ESP in tunnel mode as defined in clause 8.2.4.2 of the present specification shall be used.

9.3 Network based Mobility

9.3.1 Proxy Mobile IP

9.3.1.1 Introduction

Subclause 9.3.1.2 defines the security requirements and mechanisms for Proxy Mobile IP (PMIP) when used in EPS. In particular, it addresses how PMIP messages need to be protected within the Evolved Packet Core and how PMIP protection needs to be handled if the PMIP messages originate from a trusted non-3GPP network node.

9.3.1.2 PMIP security requirements

Trust model:

- For the reference points S2a (MAG in trusted non-3GPP access network) and S2b, S5 and S8 (MAG in ePDG or Serving GW), the MAG shall be trusted by the LMA to register only those Mobile Nodes that are attached.

Requirements on mechanisms for securing PMIP messages on the reference points S2a, S2b, S5 and S8:

Security for PMIP messages between MAG and LMA shall be provided:

- either by a chain of security associations in a hop-by-hop fashion according to TS 33.210 [6]. For each hop in such a chain, one security association per direction shall be used for all PMIP messages relating to any user, or
- by one security association per direction for all PMIP messages relating to any user in an end-to-end fashion according to TS 33.210 [6] for the intra-domain case.

In order to protect PMIP messages, integrity protection is required, confidentiality protection is optional.

Strong access authentication:

- PMIP shall be used only in conjunction with AKA-based access authentication.

9.3.1.3 PMIP security mechanisms

TS 33.210 [6] shall be applied to secure PMIP messages on the reference points S2a, S2b, S5 and S8. TS 33.310 [12] may be applied regarding the use of certificates with the security mechanisms of TS 33.210 [6].

NOTE: For the case of an interface between two entities in the same security domain, TS 33.210 [6] does not mandate the protection of the interface by means of IPsec.

10 Security interworking between 3GPP access networks and non-3GPP access networks

10.1 General

The requirements and specifics for the security interworking of 3GPP access networks with different non-3GPP access networks during idle mode and active mode mobility are described in the following subclauses.

10.2 CDMA2000 Access Network

This clause captures all the security requirements for the interworking between HRPD and E-UTRAN during idle mode and active mode mobility. The present document assumes that no security context exchange is performed between E-UTRAN and HRPD access systems.

10.2.1 Idle Mode Mobility

The security interworking specifics between E-UTRAN and HRPD during idle mode mobility are defined in this clause which covers the UE idle mobility in both directions, i.e. from E-UTRAN to HRPD and HRPD to E-UTRAN.

10.2.1.1 E-UTRAN to HRPD Interworking

For pre-registration, the UE interacts directly with HRPD system to perform authentication through the HS-GW and establish security association with this system directly. The procedures are the same as in the case when the UE connects directly to the HRPD access network except that it is tunneled over the E-UTRAN/EPS. In these procedures, the UE follows the authentication and key agreement procedure described in subclause 6.2. Tunneled signaling is exchanged over S101 interface which shall be secured as described in clause 11.

NOTE: Network domain security as specified in TS 33.210 [6] and TS 33.310 [12] applies to secure signalling between eAN/PCF in the HRPD access network and MME in the serving network.

In the case when the UE is not aware of its movement from E-UTRAN to HRPD, the UE may access the HRPD system directly without performing a pre-registration through E-UTRAN/EPS system.

For UEs with an established emergency call the authentication is subject to the requirements in clause 13.

10.2.1.2 HRPD to E-UTRAN Interworking

The security interworking specifics of the UE idle mode mobility from HRPD to E-UTRAN follows the EPS network entry procedures as described in TS 33.401 [16].

10.2.2 Active mode mobility

The security interworking specifics during active mode mobility between E-UTRAN and HRPD are defined in this clause which covers the UE active mobility in both directions, i.e. from E-UTRAN to HRPD and HRPD to E-UTRAN.

10.2.2.1 E-UTRAN to HRPD Interworking

The UE behaviour is the same as in E-UTRAN-HRPD security Interworking for idle mode mobility described in subclause 10.2.1.

10.2.2.2 HRPD to E-UTRAN Interworking

The UE interacts directly with the MME to perform authentication with EPS and establish a security association with this system directly. The procedures are the same as in the case when the UE connects directly to the E-UTRAN system, except that it is tunneled over the HRPD AN. In these procedures, the UE uses EPS-AKA with the MME.

11 Network Domain Security

For all interfaces between network elements relevant in the context of the present document,

- TS 33.210 [6] shall be applied to secure signalling messages on the reference points unless specified otherwise, and
- TS 33.310 [12] may be applied regarding the use of certificates with the security mechanisms of TS 33.210 [6] unless specified otherwise in the present document.

NOTE: For the case of an interface between two entities in the same security domain, TS 33.210 [6] does not mandate the protection of the interface by means of IPsec.

12 UE-ANDSF communication security

12.1 UE-ANDSF communication security requirements

In order to address the security of communication over S14 reference point (i.e. between UE and ANDSF), the following requirements apply:

- UE and ANDSF shall be mutually authenticated;
- The UE shall be able to verify that the ANDSF is authorized to serve it.
- Signalling over S14 reference point shall be integrity protected
- Signalling over S14 reference point shall be confidentiality protected.
- Signalling over S14 reference point shall be protected against possible replay attacks.

12.2 UE-ANDSF communication security solution

UE and ANDSF server shall establish a security association to protect the messages of Access Network Info Request and Access Network Info Response. UE and ANDSF server shall mutually authenticate each other. UE and ANDSF server shall use the following mechanism to meet the security requirements as specified in clause 12.1:

For ANDSF pull messages, PSK TLS with GBA based shared key-based mutual authentication between UE and ANDSF server as specified by clause 5.4 of TS33.222 [24].

For ANDSF push messages one of the following mechanisms shall be used:

- If a PSK TLS connection has been established as a part of a pull message and is still available, the available PSK TLS session shall be used.
- Otherwise, PSK TLS with GBA push based shared key-based mutual authentication between the UE and the ANDSF server shall be used. GBA push is specified in TS 33.223 [29].

NOTE: If a TLS connection is released, it can only be re-established by the client side, i.e. UE, even though the TLS session including security association would be alive on both sides. TLS connection, in turn, is dependent on the underlying TCP connection.

The ANDSF shall request the User Security Settings (USS) from the BSF and deducts the authorization information for this UE from USS as specified in TS 29.109 [25].

For the authorization of the ANDSF server to the UE, the UE shall check that the ANDSF that the UE discovered and is connecting to is on the configured list of ANDSF names.

13 Security aspects of emergency call handling

13.1 General

NOTE: Support for EPS emergency calling is defined in the TS 23.402 [5]. Per TS 23.402 [5], this release of this specification is limited to support of handover of emergency sessions from E-UTRAN access to HRPD access only. In this release of this specification, handover of IMS Emergency Sessions from HRPD access to E-UTRAN access is not supported.

Support for IMS Emergency sessions over an WLAN access is supported as specified in subclause 4.5.7.2 of TS 23.402[5]. Rel-14 added support for emergency services over trusted and untrusted WLAN for:

- UEs with IMSI's that cannot be authenticated (for eg., unauthorized IMSI),
- UEs without IMSIs (UICC-less UEs).

13.2 Requirements for emergency call handling

If the UE is authenticated in E-UTRAN and has an emergency call established and at that point attempts a hand over to HRPD, authentication and authorization of the UE to HRPD is executed according to operator policy and local regulatory requirements. If the HRPD network chooses to perform authentication and authorization at the handover and either one of them fail, then it is up to operator policy and local regulatory requirements whether the UE shall be allowed to get service from the HRPD network.

If the UE has established an unauthenticated emergency call in E-UTRAN and attempts a handover to HRPD, then it is up to local regulations and operator policy if the UE shall receive service from HRPD network. E-UTRAN provides an indication to HRPD access whether the UE has been authenticated in E-UTRAN or not, as described in TS 23.402 [5].

13.3 Unauthenticated emergency calls over untrusted WLAN

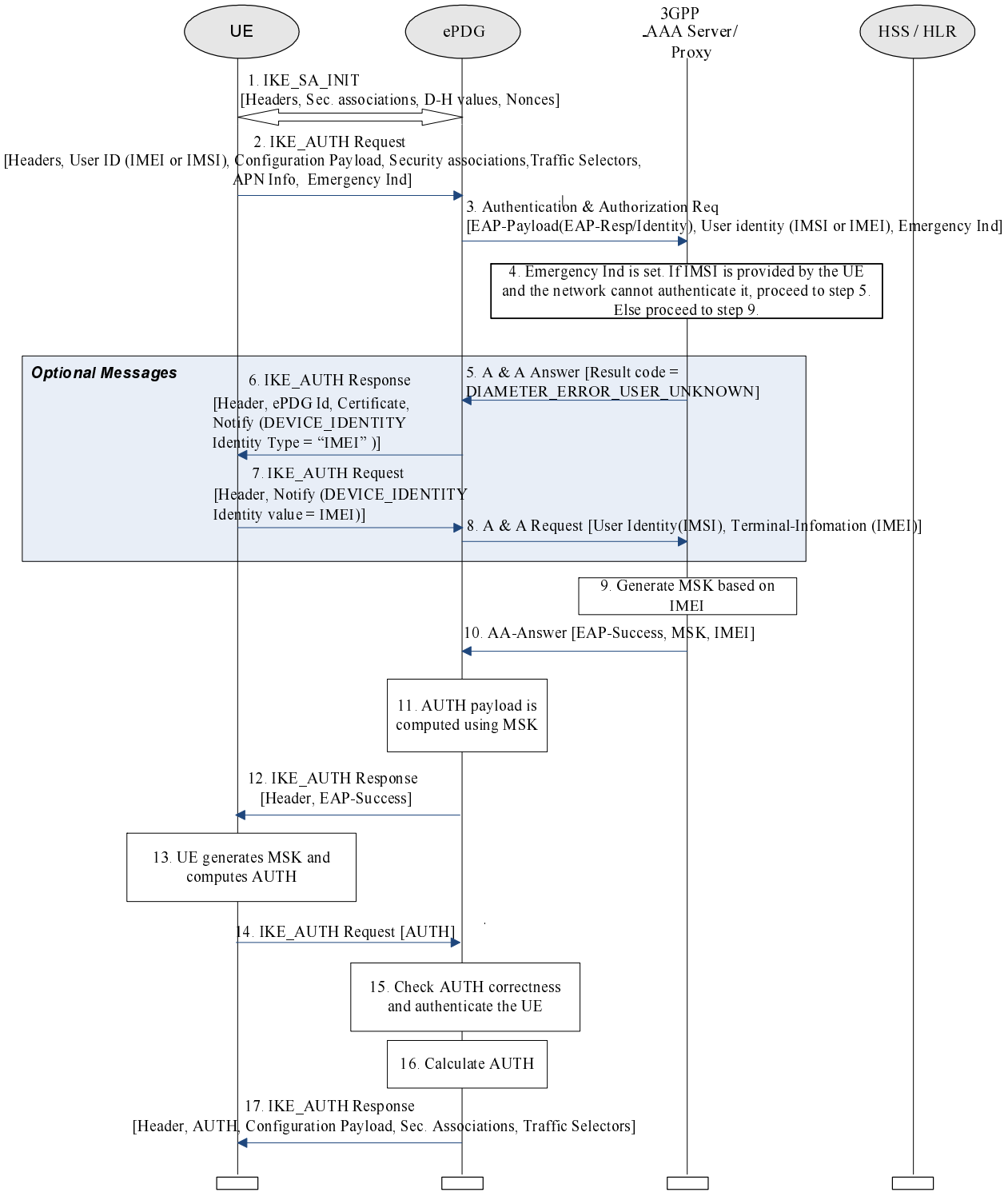

Figure: 13.3-1 Unauthenticated Emergency Calls over untrusted WLAN

1. As in step 1 from Figure 8.2.2-1.
2. As in step 2 from Figure 8.2.2-1 with the following modification
   - The UE provides an indication that the EPC access is for emergency services.

- UICC-less UE shall send its IMEI value as its identity in the Emergency NAI for Limited Service format as defined in clause 19 of TS 23.003

3. As in step 3 from Figure 8.2.2-1 with the following modification –

- If the ePDG supports emergency services over WLAN, it shall send the Authentication and Authorization Request message to the 3GPP AAA Server with an additional IE to indicate the establishment of an emergency session.

- In case of UICC-less UEs, the User Identity IE in the request shall contain IMEI received from the UE.

4. 3GPP AAA Server receives the message with an indication from the UE that it is an Emergency Attach. If the 3GPP AAA Server supports IMS Emergency sessions over WLAN, it shall proceed as follows:

- When the received subscriber identity is an IMSI but the IMSI authentication cannot proceed (because IMSI is not present in HSS, for ex.) or if AAA server cannot determine if authentication is successful, and if local policies allow emergency sessions for unauthenticated UEs with an IMSI, the 3GPP AAA Server shall skip EAP-AKA authentication procedures and proceed to execute step 5.

- When the received subscriber identity is an IMEI and if local policies allow emergency sessions for all UEs, the 3GPP AAA Server shall proceed to step 9 to generate an MSK

5. The 3GPP AAA Server indicates to the ePDG that authentication cannot proceed with the Result code IE in Authentication and Authorization Answer message set to DIAMETER_ERROR_USER_UNKNOWN.

6. The ePDG processes the A&A Answer message as follows:

- If the ePDG supports unauthenticated emergency services over WLAN and Mobile Equipment Identity Signaling procedure, it shall request the IMEI from the UE by including the DEVICE_IDENTITY Notify payload in the IKE_AUTH response sent to the UE. The Identity Type field in the Notify payload is set to “IMEI”.

- Else the ePDG shall reject the requested PDN connection for emergency session.

NOTE: TS 24.302[22] cf. 7.4.5 describes Mobile Equipment Identity signaling procedure.

7. The UE provides its IMEI in the DEVICE_IDENTITY Notify payload of the IKE_AUTH Request message. The Identity Value field in the Notify payload is used to carry the IMEI value.

8. The ePDG forwards the received IMEI to the 3GPP AAA server in the Terminal-Information AVP

The Authentication and Authorization Request (A&A Request) in step 8 shall contain the same parameters as provided in the first Authentication and Authorization Request (step 3) with the addition of the received IMEI from the UE. The A&A Request message includes EAP Payload, Emergency-Indication and user identity set to the IMSI of the UE.

The ePDG rejects the request if IMEI is not provided by the UE.

9. The 3GPP AAA Server generates MSK based on UE’s IMEI value

MSK is derived per clause A.4 in Annex A.

10. The 3GPP AAA Server sends the final Authentication and Authorization Answer (with a result code indicating success) including EAP success and the MSK key material to the ePDG. The Permanent User Identity IE in the answer contains UEs IMEI.

11. As in step 10 from Figure 8.2.2-1

12. As in step 11 from Figure 8.2.2-1

13. The UE generates MSK based on its IMEI as per clause A.4 in Annex A and computes AUTH

14-17. As in steps 12 to 15 from Figure 8.2.2-1

13.4 Unauthenticated emergency calls over trusted WLAN

For unautheticated emergency calls over trusted WLAN, the authentication and key agreement procedure for trusted access described in clause 6.2 cannot be performed. However, the UE and the AAA server exchange UE identity information and connection parameters, and generate a shared key, according to the procedure described in this clause.The exchange of the connection parameters and possibly the exchange of the IMEI of the UE are performed using a 3GPP vendorspecific EAP method called EAP-3GPP-LimitedService, with messages called 3GPP-LimitedService-Init-Info and 3GPP-LimitedService-Notif. A list of 3GPP vendor specific EAP methods is provided in Annex C.

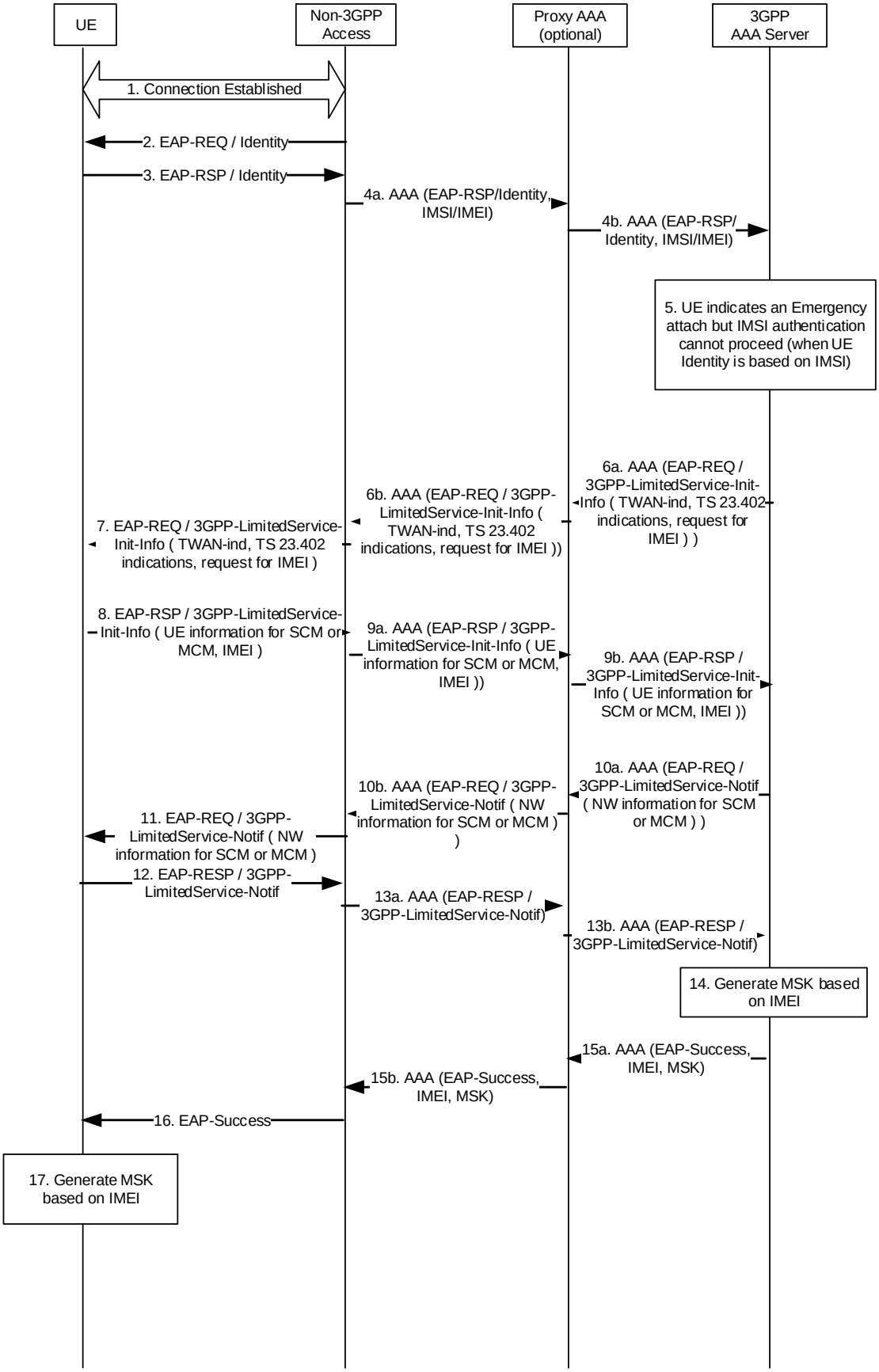
UE
Non-3GPP Access
Proxy AAA (optional)
3GPP AAA Server
1. Connection Established
2. EAP-REQ / Identity
3. EAP-RSP / Identity
4a. AAA (EAP-RSP/Identity, IMSI/IMEI)
4b. AAA (EAP-RSP/ Identity, IMSI/IMEI)
5. UE indicates an Emergency attach but IMSI authentication cannot proceed (when UE Identity is based on IMSI)
6a. AAA (EAP-REQ / 3GPP-LimitedService-Init-Info (TWAN-ind, TS 23.402 indications, request for IMEI))
6b. AAA (EAP-REQ / 3GPP-LimitedService-Init-Info (TWAN-ind, TS 23.402 indications, request for IMEI))
7. EAP-REQ / 3GPP-LimitedService-Init-Info (TWAN-ind, TS 23.402 indications, request for IMEI)
8. EAP-RSP / 3GPP-LimitedService-Init-Info (UE information for SCM or MCM, IMEI)
9a. AAA (EAP-RSP / 3GPP-LimitedService-Init-Info (UE information for SCM or MCM, IMEI))
9b. AAA (EAP-RSP / 3GPP-LimitedService-Init-Info (UE information for SCM or MCM, IMEI))
10a. AAA (EAP-REQ / 3GPP-LimitedService-Notif (NW information for SCM or MCM))
10b. AAA (EAP-REQ / 3GPP-LimitedService-Notif (NW information for SCM or MCM))
11. EAP-REQ / 3GPP-LimitedService-Notif (NW information for SCM or MCM)
12. EAP-RESP / 3GPP-LimitedService-Notif
13a. AAA (EAP-RESP / 3GPP-LimitedService-Notif)
13b. AAA (EAP-RESP / 3GPP-LimitedService-Notif)
14. Generate MSK based on IMEI
15a. AAA (EAP-Success, IMEI, MSK)
15b. AAA (EAP-Success, IMEI, MSK)
16. EAP-Success
17. Generate MSK based on IMEI

Figure: 13.4-1 Unauthenticated Emergency Calls over trusted WLAN

1. As in step 1 from Figure 6.2-1.

2. As in step 2 from Figure 6.2-1.

3. As in step 3 from Figure 6.2.1 with the following enhancement

   - UICC-less UEs shall send its identity complying with the Emergency NAI for Limited Service State format for IMEI as specified in TS 23.003[8].

4a. As in step 4 from Figure 6.2-1

4b. As in step 5 from Figure 6.2-1.

5. 3GPP AAA Server receives the message with an indication from the UE that it is an Emergency Attach. If the 3GPP AAA Server supports IMS Emergency sessions over WLAN, it shall proceed as follows:

   - When the received subscriber identity is an IMSI but the IMSI authentication cannot proceed (because IMSI is not present in HSS, for example) or if AAA server cannot determine if authentication is successful, and if local policies allow emergency sessions for unauthenticated UEs with an IMSI, the 3GPP AAA Server shall skip EAP-AKA' authentication procedures and proceed to execute step 6a to obtain IMEI from the UE and to provide indications specified in TS 23.402 to the UE.

   - When the received subscriber identity is an IMEI and if local policies allow emergency sessions for all UEs, the 3GPP AAA Server shall proceed to step 6a to provide indications specified in TS 23.402 to the UE.

6a-6b. The 3GPP AAA Server sends the EAP-Request/3GPP-LimitedService-Init-Info message. The 3GPP AAA Server shall indicate that the WLAN is trusted non-3GPP access and shall include the indications specified in TS 23.402. If an IMEI is to be obtained, the 3GPP AAA server shall also indicate a request for IMEI.

7. The authenticator in the access network forwards the EAP-Request/3GPP-LimitedService-Init-Info message to the UE

8. The UE responds with an EAP-Response/3GPP-LimitedService-Init-Info message. The UE shall include the UE information needed for single-connection mode or multi-connection mode, as specified in TS 23.402. If the EAP-Request/3GPP-LimitedService-Init-Info message contains a request for IMEI, the UE shall also include its IMEI value.

9a-9b. The authenticator forwards the EAP-Response/3GPP-LimitedService-Init-Info message to the 3GPP AAA Server. Network rejects the request if a request for IMEI was indicated in the EAP-Request/3GPP-LimitedService-Init-Info message but IMEI value is not provided by the UE.

10a-10b The 3GPP AAA Server sends EAP-Request/3GPP-LimitedService-Notif message to the UE. The 3GPP AAA Server shall include the network information for single-connection mode or multi-connection mode, as specified in TS 23.402.

11. The authenticator in the access network forwards the EAP-Request/3GPP-LimitedService-Notif message to the UE

12. The UE responds an EAP-Response/3GPP-LimitedService-Notif message.

13a-13b. The authenticator forwards the EAP-Response/3GPP-LimitedService-Notif message to the 3GPP AAA Server.

14. The 3GPP AAA Server generates MSK based on UE's IMEI identity.

    MSK is derived per clause A.4 in Annex A.

15. The 3GPP AAA Server sends the final Authentication and Authorization Answer (with a result code indicating success) including EAP success and the MSK key material to the authenticator. The Permanent User Identity IE in the answer contains IMEI obtained previously from the UE.

16. The authenticator in the access network stores the keying material to be used in communication with the unauthenticated UE as required by the access network. It informs the UE with the EAP Success message.

17. The UE generates MSK based on its IMEI as per clause A.4 in Annex A

The UE and the authenticator in the access network share MSK keying material.

14 Temporary identity management

14.1 Temporary identity generation

Temporary Identities (Pseudonyms or re-authentication identities) are generated as some form of encrypted IMSI. Advanced Encryption Standard (AES) (see ref. [40]) in Electronic Codebook (ECB) mode of operation with 128-bit keys is used for this purpose.

In order to encrypt with AES in ECB mode, it is necessary that the length of the clear text is a multiple of 16 octets. This clear text is formed as follows:

1. A *Compressed IMSI* is created utilising 4 bits to represent each digit of the IMSI. According to TS 23.003 [8], the length of the IMSI is not more than 15 digits (numerical characters, 0 through 9). The length of the *Compressed IMSI* shall be 64 bits (8 octets), and the most significant bits shall be padded by setting all the bits to 1.

   e.g.: IMSI = 214070123456789 (MCC = 214 ; MNC = 07 ; MSIN = 0123456789)

   Compressed IMSI = 0xF2 0x14 0x07 0x01 0x23 0x45 0x67 0x89

   Observe that, at reception of a temporary identity, it is easy to remove the padding of the *Compressed IMSI* as none of the IMSI digits will be represented with 4 bits set to 1. Moreover, a sanity check should be done at reception of a temporary identity, by checking that the padding, the MCC and the MNC are correct, and that all characters are digits.

2. A *Padded IMSI* is created by concatenating an 8-octet random number to the *Compressed IMSI*.

A 128-bit secret key, Kpseu, is used for the encryption. The same secret key shall be configured at all the AAA servers in the operator network so that any AAA server can obtain the permanent identity from a temporary identity generated at any other AAA server (see section 14.2).

Figure 14.1-1 summarises how the *Encrypted IMSI* is obtained.

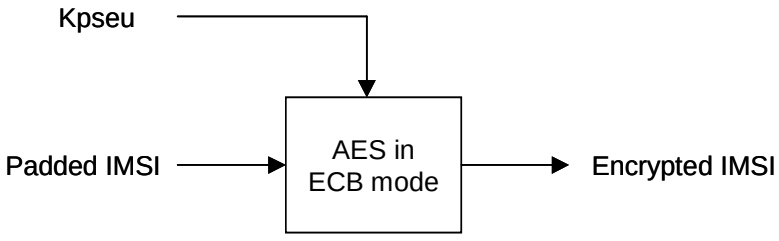

Figure 14.1-1: Encrypted IMSI generation

Once the *Encrypted IMSI* has been generated, the following fields are concatenated:

- *Encrypted IMSI*, so that a AAA server can later obtain the IMSI from the temporary identity.
- *Key Indicator*, so that the AAA server that receives the temporary identity can locate the appropriate key to de-encrypt the Encrypted IMSI (see clause 14.2).
- *Temporary identity Tag*, used to mark the identity as temporary pseudonym or re-authentication identity.

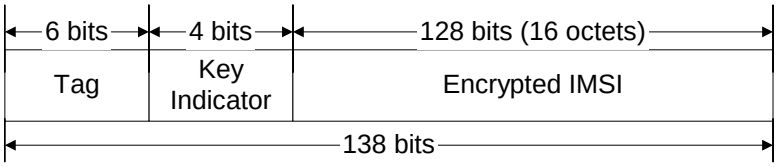

Figure 14.1-2

The Temporary Identity *Tag* is necessary so that when a AAA receives a user identity it can determine whether to process it as a permanent or a temporary user identity. Moreover, according to EAP-AKA/EAP-AKA' specifications, when the Authenticator node (i.e. the AAA server) receives a temporary user identity which is not able to map to a permanent user identity, then the permanent user identity (if the AAA server recognises it as a pseudonym) or a full authentication identity (if theAAA server recognises it as a re-authentication id) shall be requested from the client.

The last step in the generation of the temporary identities consists on converting the concatenation above to a printable string using the BASE64 method described in section 4.3.2.4 of RFC 1421 [41]. With this mechanism, each 6-bit group is used as an index into an array of 64 printable characters. As the length of the concatenation is 138 bits, the length of the resulting temporary identity is 23 characters, and no padding is necessary. Observe that the length of the Temporary identity*Tag* has been chosen to be 6 bits, so that it directly translates into one printable character after applying the transformation. Therefore, at reception of a user identity, the AAA server can recognise that it is a temporary identity for EAP-AKA without performing any reverse transformation (i.e. without translating any printable character into the corresponding 6 bits).

14.2 Key management

A 128-bit encryption key shall be used for the generation of temporary identities for a given period of time determined by the operator. Once that time has expired, a new key shall be configured at all the AAA servers. The old key shall not be used any longer for the generation of temporary identities, but the AAA servers shall keep a number of suspended (old) keys for the interpretation of received temporary identities that were generated with those old keys. The number of suspended keys kept in the AAA servers (up to 16) should be set by the operator, but it shall be at least one, in order to avoid that a just-generated temporary identity becomes invalid immediately due to the expiration of the key.

Each key shall have associated a Key Indicator value. This value is included in the temporary identity (see *Key Indicator* field in clause 6.4.1), so that when a AAA receives the temporary identity, it can use the corresponding key for obtaining the *Padded IMSI* (and thence the Username).

If a temporary identity is sent to a client but then the user does not initiate new authentication attempts for a long period of time, the key used for the generation of that temporary identity could eventually be removed from all the AAA servers. If the user initiates an authentication attempt after that time using that old temporary identity, the receiving AAA server will not be able to recognise the temporary identity as a valid one but it will be able to recognize the type of temporary identity (pseudonym or re-authentication identity), and it shall request the permanent user identity from the client (if the temporary identity was a re-authentication identity, the AAA server shall request first a pseudonym, and if it is not recognized, the permament user identity) Hence, in order to achieve that permanent user identities are used as little as possible, it is recommended that the encryption key is not renewed very often.

The configuration of the keys could be done via O&M, as shown in the figure below.

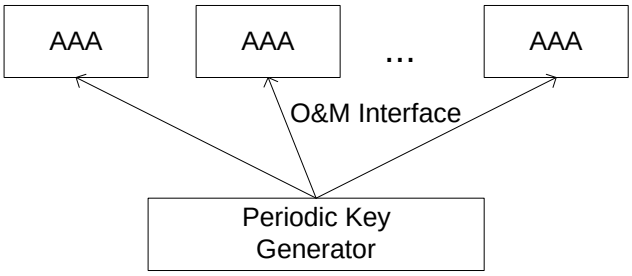

Figure14.2-1: Key configuration via O&M

Handling of these secret keys, including generation, distribution and storage, should be done in a secure way.

14.3 Impact on permanent user identities

User identities (permanent or temporary) are sent with the form of a NAI, according to the EAP EAP-AKA/EAP-AKA' specifications, and the maximum length of a NAI that we can expect to be handled correctly by standard equipment is 72 octets (see [44]). Moreover, this NAI shall be transported inside the User-Name attribute of a RADIUS Access-Request, with standard length up to 63 octets (see [45]). Therefore, it can be assumed that the maximum length of a user identity should be 63 octets (i.e. 63 characters).

Since the length of the temporary identity proposed in section 14.1 is 23 characters, the length of the realm part of any permanent user identity shall always be 40 characters or less. This applies regardless of whether the length of the username part of the permanent user identity is less than 23 characters.

NOTE: A temporary user identity is formed as a NAI with the pseudonym or re-athentication identity as the username part and the realm.

Moreover, the permanent user identities should not begin with the character resulting of the printable encoding transformation (see section 14.1) of the *Temporary identity Tag* used for EAP-AKA and EAP-AKA' pseudonyms or re-authentication identities. This is needed so that at reception of a user identity, the AAA server can determine whether it is a permanent or a temporary user identity.

14.4 Acknowledged limitations

This mechanism does not prevent forging of temporary identities generated with keys that are no longer maintained in the AAA servers. That is, an attacker may form a temporary identity by concatenating the desired *Temporary identity Tag* and 132 bits of random information, and then applying the printable encoding transformation (see clause 14.1). At reception of such temporary identity in a AAA server, the following cases are possible:

- The *Key Indicator* may not correspond to any key (active or suspended) maintained at the AAA server.
- If the *Key Indicator* corresponds to any of the keys maintained at the AAA server, then that key is used for the de-encryption of the *Encrypted IMSI*, but the sanity check over the padding, the MCC and the MNC would show that the IMSI is not correct.

In any case, the AAA server shall interpret that the received temporary identity was generated with a key that is no longer available, and therefore it shall request the permanent user identity (if the received temporary identity was a pseudonym) or the pseudonym (if the received temporary identity was a re-authentication identity) to the client.

This could be exploited to perform DoS attacks by initiating a large amount of authentication attempts presenting different forged temporary identities. Nonetheless, the consequences of this attack should not be worse than the already possible attack of initiating a large amount of authentication attempts presenting different forged permanent identities.

14.5 UE behaviour on receiving requests to send the IMSI-based user identity

When the 3GPP AAA server does not recognize a temporary identifier used by the UE, the 3GPP AAA server requests the UE to send the IMSI-based user identity. The UE can operate according to one of the following three alternatives.

1. Ignore the Request: This alternative may result in deadlock situations that prevent the UE from connecting to a valid network. If this alternative is implemented, then there shall be a separate mechanism available for the user to override the policy (for example to delete the stored temporary identifier, which would result in using the IMSI-based identity upon the next connection).
2. Prompt the User: In this alternative, the UE prompts the user during the EAP authentication whether to send the IMSI-based identity to the network. If the user denies sending the IMSI, then the authentication exchange is cancelled.
3. Always Send the IMSI-Based Identity: In alternative #3, the UE always sends the IMSI-based identity when requested.

The decision is UE specific and outside the scope of this specification.

Annex A (normative): Key derivation functions

A.1 KDF interface and input parameter construction

All key derivations (including input parameter encoding) shall be performed using the key derivation function (KDF) specified in TS 33.220 [8]. This clause specifies how to construct the input string, S, to the KDF (which is input together with the relevant key). For each of the distinct usages of the KDF, the input parameters S are specified below.

The FC number space used is controlled by TS 33.220 [8], FC values allocated for this specification are in range of 0x20 – 0x2F.

A.2 Function for the derivation of CK', IK' from CK, IK

When deriving CK', IK' from CK, IK and the access network identity as defined in clause 6 of this specification , the following parameters shall be used to form the input S to the KDF.

- FC = 0x20,
- P0 = value of access network identity, as defined in 3GPP TS 24.302 [22],
- L0 = length of value of access network identity (variable, depending on access network type),
- P1 = SQN ⊕ AK
- L1 = length of SQN ⊕ AK (i.e. 0x00 0x06)

If AK is not used, AK shall be treated in accordance with TS 33.102, i.e. as 000…0.

The access network identity is defined separately for each access network type. For each access network type, the access network identity is documented in TS 24.302 [22] to ensure that UE and HSS use the same access network identities as input for key derivation.

The input key shall be the concatenation CK || IK of CK and IK.

The KDF returns a 256-bit output, where the 128 most significant bits are identified with CK' and the 128 least significant bits are identified with IK'.

A.3 Function for the derivation of WLCP key from EMSK

When deriving WLCP key from the EMSK as defined in clause 7.2.3 of this specification, the following parameters shall be used to form the input S to the KDF.

- FC = 0x21,
- P0 = "wlcp-key" (i.e. 0x77 0x6C 0x63 0x70 0x2D 0x6B 0x65 0x79) ,
- L0 = length of P0 is 8 octets (i.e., (i.e. 0x00 0x08).

The input key shall be the EMSK.

A.4 Function for the derivation of MSK key for unauthenticated emergency sessions over WLAN

When deriving MSK for Unauthenticated Emergency sessions over WLAN, the following parameters shall be used to form the input S to the KDF.

- FC = 0x22,
- P0 = “unauth-emer” (i.e. 0x75 0x6E 0x61 0x75 0x74 0x68 0x65 0x6D 0x65 0x72)
- L0 = length of P0 is 11 octets (i.e., 0x00 0x0B).

The input key shall be the IMEI of the UE.

Annex B (normative): Tunnelling of UE Services over restrictive access networks

B.1 Overview

This Annex specifies a mechanism for tunnelling of UE Services over Restrictive Access Networks. Before using the mechanisms specified in this Annex, the UE shall in accordance with normal procedures attempt to use existing NAT/FW traversal mechanisms as specified in TS 23.402 [5], the main body of this document, and if applicable TS 33.203 [34]. The exact procedure depends on the UE, the access, the requested service, and operator policy.

Clause X.2 specifies a mechanism to achieve UE access to PLMN IP-based services over restrictive firewalls in non-3GPP accesses. As only the transport/encapsulation layer is changed, all protocol variants specified in TS 23.402 [5] are supported and all functionality provided by ePDG/IKE is available.

The mechanisms in this Annex are optional to implement.

Editor's note: It is FFS whether the mechanisms defined in this Annex should be standadized by IETF or 3GPP.

B.2 Service and media reachability for users over restrictive firewalls - untrusted non 3GPP access

This clause specifies a generic mechanism to achieve UE access to PLMN IP-based services over restrictive firewalls in non-3GPP accesses. The mechanism is intended to be used in the case the tunnelling mechanism from section 8.2 does not work.

The UDP encapsulation layer is replaced with a TCP/TLS encapsulation layer on port 80/443 that makes the traffic appear as HTTP/HTTPS traffic to the firewall. To traverse HTTP proxies, the TCP/TLS connection may optionally be setup with HTTP CONNECT The TLS profile as defined in TS 33.310 [12] Annex E shall be used..

All protocol variants specified in TS 23.402 (S2b with PMIPv6/GTP and S2c with DSMIPv6) are supported and all functionality provided by ePDG/IKE is available.

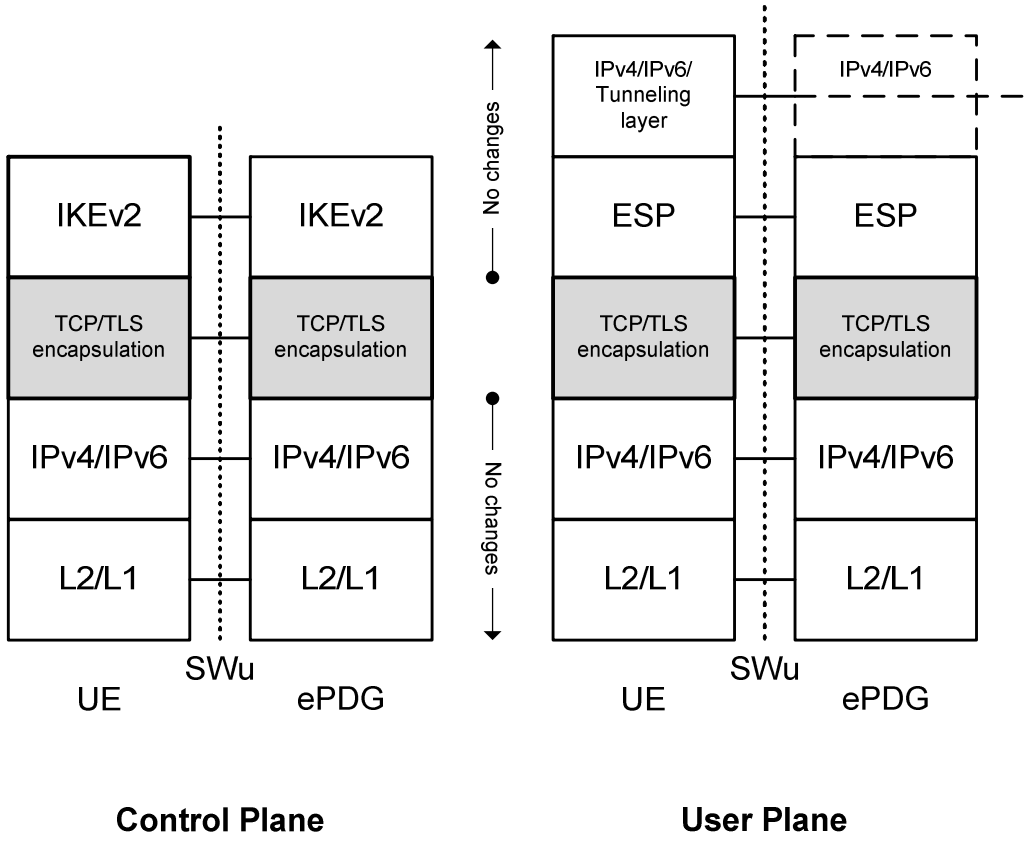

Figure B.1: Protocol stacks for firewall traversal

Legend:

- Only the transport layer is changed. Instead of UPD encapsulation, TCP/TLS encapsulation on port 80/443 is used. Packets types (IKE, ESP, NAT-Keepalive) are identified in a similar way as in IETF RFC 3948 [35].
- As before, when PMIPv6 is used the ePDG terminates some of the IPv4/IPv6 messages.

Authentication, integrity protection, and confidentiality are provided by the IKEv2/ESP layer. TLS is strictly used for firewall traversal (making the traffic look like HTTPS) and shall not be used to provide security instead of the IKEv2/ESP layer.

NOTE: The exact details of the TCP/TLS encapsulation layer are defined in the corresponding stage 3 specification.

If the establishment of the TCP/TLS connection fails, this may be caused by the presence of an HTTP proxy between the UE and the ePDG. The UE should try to establish a TCP connection to the ePDG by using the HTTP CONNECT method (IETF RFC 2616 [36]). How the UE gets the address of the HTTP proxy (manual or automatic configuration) is out of scope of 3GPP.

Annex C (informative): List of 3GPP-vendor specific EAP-methods

Table C-1 specifies semantics for code points of the Vendor-Type ID field of the Expanded Type EAP method when the Vendor-Id field is set to the 3GPP Vendor-Id 10415 (decimal).

Table C-1: Vendor-Type ID

Vendor-Type ID	Semantic
1	EAP-LWA, defined in TS 33.401 [16], Annex G.3
2	EAP-3GPP-LimitedService, defined in clause 13.4 of this document.
3	EAP-5G, defined in TS 24.502 [48], clause 9.2

Annex D (informative): Security aspects of DNS and ICMP

D.1 General

The security measures specified in Annex P of TS 33.501 [49] can be used to protect the DNS and ICMP messages that are carried over the user plane.

Annex E (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2007-05					Initial version contains commented Table of Contents with references to TR 33.922 and TR 33.821	-	0.0.0
2007-12	SA3#49bis				Additions based on S3a070978, S3a070981, S3a071028	0.0.0	0.1.0
2008-02	SA3#50				Additions based on S3-080062; S3-080084; S3-080101; S3-080102; S3-080103; S3-080105; S3-080162; S3-080175	0.1.0	0.2.0
2008-03	SA#39				Presented for information at SA	0.2.0	1.0.0
2008-04	SA3#51				Additions based on S3-080428,474, 427, 449, 423, 334, 337, 338, 476, 473, 446, 450, 430, 485, 475, 426, 477, 339, 340, 439, 494	1.0.0	1.1.0
2008-05					MCC preparation for approval	1.1.0	2.0.0
2008-06	SA#40	SP-080258			SA approval	2.0.0	8.0.0
2008-09	SA#41	SP-080488	017	-	Resolution of Ed notes on use of EAP-AKA in IKEv2	8.0.0	8.1.0
2008-09	SA#41	SP-080488	004	1	Resolution of the Ed Notes under clause 8.2.5, TS33.402	8.0.0	8.1.0
2008-09	SA#41	SP-080488	0023	2	Resolution of 2nd And 3rd Editor's Notes in 8.2.2	8.0.0	8.1.0
2008-09	SA#41	SP-080488	02	-	Resolution of 1st Ed Note in Clause 6.1 TS33.402	8.0.0	8.1.0
2008-09	SA#41	SP-080488	0006	1	MIPv4 Signalling protection between PDN-GW and FA	8.0.0	8.1.0
2008-09	SA#41	SP-080488	012	-	correction of 33.402	8.0.0	8.1.0
2008-09	SA#41	SP-080488	013	-	Clarification of text on access network identities	8.0.0	8.1.0
2008-09	SA#41	SP-080488	014	-	Clarification of use of AMF separation bit with EAP-AKA access authentication	8.0.0	8.1.0
2008-09	SA#41	SP-080488	015	-	Clarification on handling of authentication vectors in the 3GPP AAA server	8.0.0	8.1.0
2008-09	SA#41	SP-080488	007	1	Resolution of Ed notes on MIPv4 Root key generation	8.0.0	8.1.0
2008-09	SA#41	SP-080488	016	2	update of S3-080756 Resolution of EditorÆs notes regarding parameter exchange in access authentication	8.0.0	8.1.0
2008-09	SA#41	SP-080488	018	-	Removing the restriction on AKA for Trusted Access	8.0.0	8.1.0
2008-09	SA#41	SP-080488	022	1	Methods to avoid impersonation attacks on S2c	8.0.0	8.1.0
2008-09	SA#41	SP-080488	024	-	Note on SNID IP binding	8.0.0	8.1.0
2008-09	SA#41	SP-080488	005	1	CR on UE-ANDSF security	8.0.0	8.1.0
2008-09	SA#41	SP-080641	025	1	CR on EAP AKA (relaxation scenario)	8.0.0	8.1.0
2008-12	SA#42	SP-080739	026	-	Change on some names of interfaces in 33.402 and an editorial modification	8.1.1	8.2.0
2008-12	SA#42	SP-080739	027	-	MIPv4 SPI Collision Avoidance	8.1.1	8.2.0
2008-12	SA#42	SP-080739	028	-	MN-HA Key generation during initial attach or additional PDN connectivity	8.1.1	8.2.0
2008-12	SA#42	SP-080739	029	-	Handling of Mobility Keys during Re-authentication	8.1.1	8.2.0
2008-12	SA#42	SP-080739	030	2	Aligment of TS 33.402 to draft-arkko-eap-aka-kdf and clarification of indication of type of authentication from AAA to HSS	8.1.1	8.2.0
2008-12	SA#42	SP-080739	031	-	Resolution of Editor's note on tunnel fast re-authentication	8.1.1	8.2.0
2008-12	SA#42	SP-080739	032	1	Clarifications to security procedures for DSMIPv6	8.1.1	8.2.0
2008-12	SA#42	SP-080739	035	-	Adding EMSK derivation in clause 6.2	8.1.1	8.2.0
2008-12	SA#42	SP-080739	036	1	Fast re-authentications for DSMIPv6	8.1.1	8.2.0
2008-12	SA#42	SP-080739	037	-	AMF separation bit for untrusted non-3gpp access for S2c	8.1.1	8.2.0
2008-12	SA#42	SP-080739	038	-	Finalising the PMIP security requirements	8.1.1	8.2.0
2008-12	SA#42	SP-080739	039	-	Key Derivation Function to derive CK', IK' from CK, IK for non-3GPP access to EPC	8.1.1	8.2.0
2008-12	SA#42	SP-080739	040	-	Change on some names of interfaces in 33.402 and some corrections	8.1.1	8.2.0
2008-12	SA#42	SP-080739	041	-	Removing editor's note on legacy UEs	8.1.1	8.2.0
2008-12	SA#42	SP-080739	042	-	Correction of text on access authentication for untrusted access	8.1.1	8.2.0
2008-12	SA#42	SP-080739	043	-	Correction of text on access authentication for untrusted access	8.1.1	8.2.0
2008-12	SA#42	SP-080739	044	-	Clarification of indication of type of authentication from AAA to HSS and on access network authorization in AAA server	8.1.1	8.2.0
2008-12	SA#42	SP-080739	045	-	Modification of the MIPv4 bootstrapping	8.1.1	8.2.0
2008-12	SA#42	SP-080739	046	-	ANDSF security	8.1.1	8.2.0
2008-12	SA#42	SP-080739	034	-	MIPv4 support for Additional PDN connectivity	8.1.1	8.2.0
2008-12	--	--	--	-	MCC editorial correction	8.2.0	8.2.1
2009-03	SA#43	SP-090130	049	-	Trust Indication by Visited Network	8.2.1	8.3.0
2009-03	SA#43	SP-090130	048	2	Editorial corrections for 33.402	8.2.1	8.3.0
2009-03	SA#43	SP-090130	051	1	Clarifications on MIPv4 procedure	8.2.1	8.3.0
2009-03	SA#43	SP-090130	047	1	Corrections of DS-MIPv6 bootstrapping	8.2.1	8.3.0
2009-03	--	--	--	--	Editorial modifications	8.3.0	8.3.1
2009-06	SA#44	SP-090269	052	-	Editorial corrections to security context establishment clause	8.3.1	8.4.0
2009-06	SA#44	SP-090269	055	1	Authorization for ANDSF	8.3.1	8.4.0
2009-06	SA#44	SP-090269	057	2	Clarifications for Annex A and References	8.3.1	8.4.0
2009-06	SA#44	SP-090269	056	2	Change in the Clause 6.2. Removal of explicit CK'/IK' function.	8.3.1	8.4.0
2009-06	SA#44	SP-090269	065	-	Correction of KDF definition	8.3.1	8.4.0
2009-06	SA#44	SP-090269	062	-	Combination of authentication and authorization procedures	8.3.1	8.4.0
2009-06	SA#44	SP-090269	067	-	Clarification of order for identity request , identity for EAP-AKA' and AVs fetching	8.3.1	8.4.0

2009-06	SA#44	SP-090269	078	2	HA switch consideration for DSMIPv6 bootstrap	8.3.1	8.4.0
2009-06	SA#44	SP-090269	74	-	Clarification for network domain security and PMIP security	8.3.1	8.4.0
2009-06	SA#44	SP-090269	071	1	Add a NOTE to clarify the security for S101	8.3.1	8.4.0
2009-06	SA#44	SP-090269	054	1	Clarification on use of USIM/UICC in non-3GPP accesses	8.3.1	8.4.0
2009-06	SA#44	SP-090269	075	-	Corrections to clause 7	8.3.1	8.4.0
2009-06	SA#44	SP-090269	64	1	Generation of pseudonyms and re-authentication identities	8.3.1	8.4.0
2009-06	SA#44	SP-090279	058	1	Addition of the Emergency Calling Clause	8.4.0	9.0.0
2009-06	SA#44	SP-090418	055	3	Authorization for ANDSF	8.4.0	9.0.0
2009-09	SA#45	SP-090519	081	-	Updating reference to EAP-AKA' RFC	9.0.0	9.1.0
2009-12	SA#46	SP-090813	082	-	Correction of CMIPv4 Key derivation and SPI calculation for WiMAX interworking	9.1.0	9.2.0
2009-12	SA#46	SP-090813	084	1	Replacing KDF definition with a reference	9.1.0	9.2.0
2009-12	SA#46	SP-090814	086	-	Deletion of erroneous notes relating to fast re-authentication	9.1.0	9.2.0
2010-03	SA#47	SP-100103	088	-	Use of identities in EAP-AKA'	9.2.0	9.3.0
2010-06	SA#48	SP-100383	089	1	Addition of emergency call handling for non-3GPP access	9.3.0	9.4.0
2010-10	SA#49	SP-100483	090	1	Adding reference to RFC5295	9.4.0	9.5.0
2010-12	SA#50	SP-100723	093	--	Correction of reference draft-ietf-dime-mip6-split to point to RFC 5778	9.5.0	9.6.0
2010-12	SA#50	SP-100722	094	1	Enhanced Security support for DS-MIPv6	9.6.0	10.0.0
2011-03	SA#51	SP-110020	095	1	IPsec alignment	10.0.0	11.0.0
2011-09	SA#53	SP-110564	101	1	Removal of last step in tunnel authentications	11.0.0	11.1.0
2011-12	SA#54	SP-110694	098	3	Authentication with external networks over S2b	11.1.0	11.2.0
2011-12	SA#54	SP-110694	098	3	Authentication with external networks over S2b	11.1.0	11.2.0
2012-03	SA#55	SP-120113	103a	-	Correction of references	11.2.0	11.3.0
		SP-120038	104	-	Corrections to IKEv2 procedure	11.3.0	
		SP-120037	106	1	Correction to length of MIP-RK		11.3.1
2012-06	SA#56	SP-120344	109	1	SaMOG 33.402 Changes	11.3.1	11.4.0
2012-06	SA#56	SP-120341	110	1	Clarification of trusted and untrusted definition	11.3.1	11.4.0
2013-06	SA#60	SP-130254	113	-	Specification of Tunnelling of UE Services over Restrictive Access Networks	11.4.0	12.0.0
2013-09	SA#61	SP-130407	114	1	Correction of the editorial errors and the incorrect description	12.0.0	12.1.0
2013-12	SA#62	SP-130667	115	1	User profile fetching before authentication in non3GPP access	12.1.0	12.2.0
2014-03	SA#63	SP-140024	117	1	Correction of reference	12.2.0	12.3.0
2014-09	SA#65	SP-140592	119	1	Introduction of WLCP security	12.3.0	12.4.0
2014-12	SA#66	SP-140829	120	-	Correction of WLCP security	12.4.0	12.5.0
			121	-	Derivation of WLCP key in the UE		
			122	-	WLCP security first editor's note		
2015-09	SA#69	SP-150477	127	-	Adding TLS Reference in TS 33.402 Annex B	12.5.0	12.6.0
		SP-150478	123	2	Allowing for additional payloads in the IKE_AUTH request step of the full authentication procedure for un-trusted WLAN.	12.6.0	13.0.0
			124	1	IKE_AUTH showing wrong EAP message type in step 7 of Figure 8.2.2.1		
			125	1	Clarification that EAP-SIM is forbidden		

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2016-12	SA#74	SP-160787	0131	1	C	Alignment according to withdrawal of I-WLAN feature	13.1.0
2016-12	SA#74	SP-160784	0129	1	B	Adding support of EAP Re-Authentication Protocol for WLAN Interworking (TWAN)	14.0.0
2016-12	SA#74	SP-160788	0132	1	B	Unauthenticated Emergency services over trusted WLAN	14.0.0
2016-12	SA#74	SP-160788	0133	1	B	Unauthenticated Emergency services over untrusted WLAN	14.0.0
2016-12	SA#74	SP-160788	0134	-	B	KDF for Unauthenticated emergency services over WLAN	14.0.0
2017-03	SA#75	SP-170099	0135	1	F	Parameter transport for unauthenticated emergency calls over trusted WLAN, using vendor-specific EAP-method	14.1.0
2017-03	SA#75	SP-170099	0136	-	F	List of 3GPP vendor-specific EAP methods	14.1.0
2017-03	SA#75	SP-170102	0137	-	F	Remove Editor's Note related to ERP information in the HSS	14.1.0
2017-06	SA#76	SP-170425	0138	1	F	Alignment of 3GPP-vendor specific EAP method name with TS 24.302	14.2.0
2017-06	SA#76	SP-170429	0141	1	F	Remove support of ERP Explicit Boostrapping	14.2.0
2017-06	SA#76	SP-170425	0142	-	F	Align with CT1 TS 24.302 for obtaining IMEI using Mobile Equipment Identity signalling	14.2.0
2017-09	SA#77	SP-170638	0143	-	F	Clarification on Unauthenticated Emergency services over untrusted WLAN	14.3.0
2018-03	SA#79	SP-180049	0144	-	B	Addition of EAP-5G method ID	15.0.0
2018-06	SA#80	SP-180449	0145	1	F	Clarifying the condition when the ePDG sends its certificate to the UE during untrusted non 3gpp access authentication (8.2.2)	15.1.0
2020-07	-	-	-	-	-	Update to Rel-16 version (MCC)	16.0.0
2022-03	-	-	-	-	-	Update to Rel-17 version (MCC)	17.0.0
2023-03	SA#99	SP-230143	0148	1	F	Aligning DNS and ICMP security for non-3GPP access with 3GPP access	18.0.0
2024-06	SA#104	SP-240656	0150	1	F	Clarification on the condition for provisioning of the ePDG identity to the UE	18.1.0
2025-10	-	-	-	-	-	Update to Rel-19 version (MCC)	**19.0.0**

History

Document history		
V19.0.0	October 2025	Publication