3GPP TS 33.402 V8.2.0 (2008-12)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3GPP System Architecture Evolution (SAE);
Security aspects of non-3GPP accesses;
(Release 8)





The present document has been developed within the 3rd Generation Partnership Project (3GPP ™) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and reports for implementation of the 3GPP ™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords
LTE, UMTS, GSM, access, security

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2008, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TTA, TTC).
All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
LTE™ is a Trade Mark of ETSI currently being registered for the benefit of its Members and of the 3GPP Organizational Partners
GSM® and the GSM logo are registered and owned by the GSM Association

Samsung Ex. 1010, Page 2 of 41

Contents

Foreword 5
1 Scope 6
2 References 6
3 Definitions, symbols and abbreviations 7
3.1 Definitions 7
3.2 Symbols 7
3.3 Abbreviations 7
3.4 Conventions 8
4 Overview of Security Architecture for non-3GPP Accesses to EPS 8
4.1 General 8
4.2 Trusted non-3GPP Access 9
4.3 Untrusted non-3GPP Access 9
5 Security Features Provided by EPS for non-3GPP Accesses 9
5.1 User-to-Network security 9
5.1.1 User identity and device identity confidentiality 9
5.1.2 Entity authentication 9
5.2 User data and signalling data confidentiality 9
5.3 User data and signalling data integrity 10
6 Authentication and key agreement procedures 10
6.1 General 10
6.2 Authentication and key agreement for trusted access 12
6.3 Fast re-authentication procedure for trusted access 17
6.4 Authentication and key agreement for untrusted access 18
7 Establishment of security contexts in the target access system 19
7.1 General assumptions 19
7.2 Establishment of security context for Trusted non-3GPP Access 19
7.2.1 CDMA-2000 HRPD EPS Interworking 19
7.2.1.1 EPS-HRPD Architecture 19
7.2.1.2 Network Elements 20
7.2.1.2.1 E-UTRAN 20
7.2.1.2.2 MME 20
7.2.1.2.3 Gateway 20
7.2.1.2.3.1 General 20
7.2.1.2.3.2 Serving GW 20
7.2.1.2.3.3 PDN GW 21
7.2.1.2.4 PCRF 21
7.2.1.3 Reference Points 21
7.2.1.3.1 List of Reference Points 21
7.2.1.3.2 Protocol assumptions 21
7.2.1.4 Security of the initial access to EPS via HRPD 21
7.2.1.5 Security of handoff and pre-registration 21
7.2.2 WIMAX EPS Interworking 21
7.3 Establishment of security context between UE and untrusted non-3GPP Access 22
8 Establishment of security between UE and ePDG 22
8.1 General 22
8.2 Mechanisms for the set up of UE-initiated IPsec tunnels 22
8.2.1 General 22
8.2.2 Tunnel full authentication and authorization 22
8.2.3 Tunnel fast re-authentication and authorization 25
8.2.4 Security profiles 27
8.2.5 Handling of IPsec tunnels in mobility events 28
8.2.5.1 General 28

Samsung Ex. 1010, Page 3 of 41

8.2.5.2 Idle mode mobility 28
8.2.5.3 Active mode mobility 28
9 Security for IP based mobility signalling 28
9.1 General 28
9.2 Host based Mobility 28
9.2.1 MIPv4 28
9.2.1.1 General 28
9.2.1.2 Bootstrapping of MIPv4 FACoA parameters 29
9.2.1.2.1 Procedures 29
9.2.1.2.2 MIPv4 Key Derivation 30
9.2.1.2.3 Key Usage 31
9.2.1.2.4 Key Distribution for MIPv4 31
9.2.2 DS-MIPv6 31
9.2.2.1 General 31
9.2.2.2 Bootstrapping of DSMIPv6 parameters 32
9.2.2.2.1 Full Authentication 32
9.2.2.2.2 Fast Re-authentication 34
9.2.2.3 Security Profiles 36
9.3 Network based Mobility 36
9.3.1 Proxy Mobile IP 36
9.3.1.1 Introduction 36
9.3.1.2 PMIP security requirements 36
9.3.1.3 PMIP security mechanisms 37
10 Security interworking between 3GPP access networks and non-3GPP access networks 37
10.1 General 37
10.2 CDMA2000 Access Network 37
10.2.1 Idle Mode Mobility 37
10.2.1.1 E-UTRAN to HRPD Interworking 37
10.2.1.2 HRPD to E-UTRAN Interworking 37
10.2.2 Active mode mobility 38
10.2.2.1 E-UTRAN to HRPD Interworking 38
10.2.2.2 HRPD to E-UTRAN Interworking 38
11 Network Domain Security 38
12 UE-ANDSF communication security 38
12.1 UE-ANDSF communication security requirements 38
Annex A (normative): Key derivation functions 39
A.1 KDF interface and input parameter construction 39
A.2 Function for the derivation of CK', IK' from CK, IK 39
Annex B (informative): Change history 41

Samsung Ex. 1010, Page 4 of 41

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.

Samsung Ex. 1010, Page 5 of 41

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] IETF RFC 4306: "Internet Key Exchange (IKEv2) Protocol".

[4] draft-ietf-dime-mip6-split-06.txt: "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".

[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 Internet-Draft, draft-ietf-hokey-emsk-hierarchy-07: “Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)", work in Progress.

Samsung Ex. 1010, Page 6 of 41

[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; (Release 8) ".

[23] IETF Internet-Draft, draft-arkko-eap-aka-kdf-09: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA') ", work in Progress

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

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 [05].
S7a	Interface between a PCRF and a HRPD PDSN
S101	Interface between a MME and a HRPD AN
S103	Interface between a SGW and a HRPD PDSN

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
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
ESP	Encapsulating Security Payload
E-UTRAN	Evolved UTRAN
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

Samsung Ex. 1010, Page 7 of 41

NDS	Network Domain Security
NDS/IP	NDS for IP based protocols
PMIP/PMIPv6	Proxy Mobile IP version 6
SA	Security Association
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.

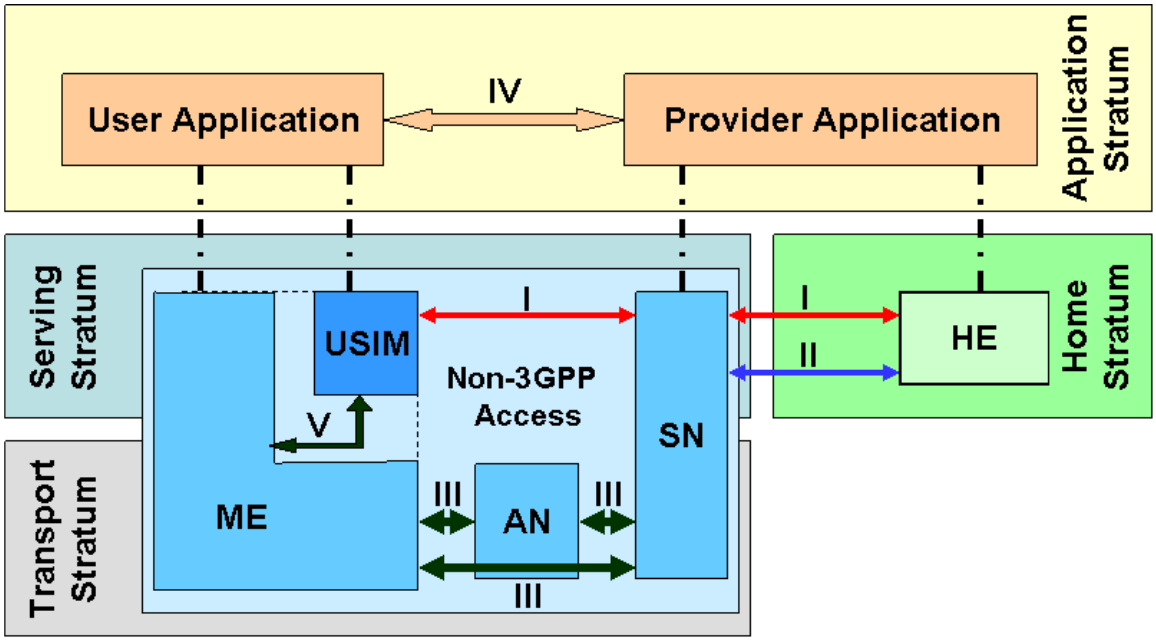


Figure 4.1-1: Security Architecture of Non-3GPP Access and 3GPP EPS

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.

Samsung Ex. 1010, Page 8 of 41

- **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.

4.2 Trusted non-3GPP Access

When all of the security feature groups are considered sufficiently secure by the home operator, the non-3GPP access is identified as a trusted non-3GPP access for that operator.

4.3 Untrusted non-3GPP Access

When one or more of the security feature groups is considered not sufficiently secure by the home operator, the non-3GPP access is identified as an untrusted non-3GPP access for that operator.

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.

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.

Samsung Ex. 1010, Page 9 of 41

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.

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 [7] or on EAP-AKA' [23]. 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.

Editor's Note: Shall the credentials used with EAP-AKA reside on the UICC for all cases in non-3GPP accesses ?.

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

Samsung Ex. 1010, Page 10 of 41

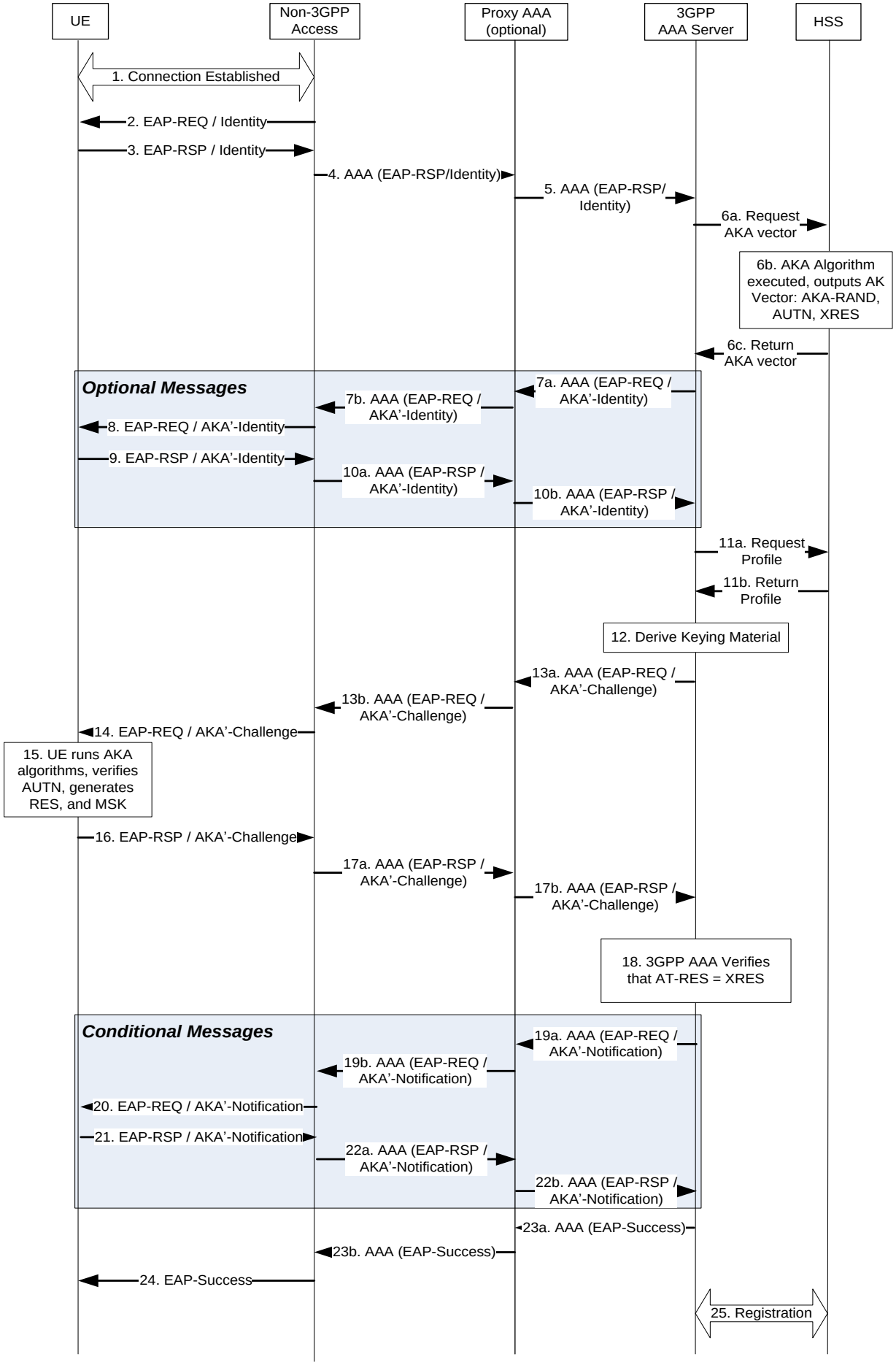
non-3GPP IP access is trusted or not. If such an indication is sent it shall be sent by the 3GPP AAA server as part of an EAP-AKA or EAP-AKA' request. If no such indication is received by the UE, and there is no pre-configured information in the UE, the UE shall consider the non-3GPP IP access as untrusted. 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.

Samsung Ex. 1010, Page 11 of 41

6.2 Authentication and key agreement for trusted access

Samsung Ex. 1010, Page 12 of 41



Samsung Ex. 1010, Page 13 of 41

Figure 6.2-1: Non-3GPP Access Authentication

EAP-AKA' as defined in [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 shall be 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 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 EAP-AKA', as defined [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_4: 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 [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', IK') = F(CK, IK, <access network identity>) where F is a key derivation function. The HSS then sends this transformed authentication vector to the 3GPP AAA server.

NOTE 5: 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.

Samsung Ex. 1010, Page 14 of 41

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.

7. 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 draft-arkko-eap-aka-kdf [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 7 through 10.

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

9. The UE responds with the same identity it used in the previous EAP Response Identity message.

10. The authenticator in the access network forwards the EAP Response/AKA' Identity to the 3GPP AAA Server. The identity received in this message will be used by the 3GPP AAA Server in the rest of the authentication process. If an inconsistency is found between the identities received in the two messages (EAP Response Identity and EAP Response/AKA' Identity) so that the user profile and authentication vectors previously retrieved from HSS are not valid, these data shall be requested again to HSS (step 6 shall be repeated before continuing with step 11).

NOTE 7: In order to optimise performance, the identity re-request process (the latter four steps) should be performed before user profile and authentication vectors retrieval.

11. 3GPP AAA Server checks that it has the EPS access profile of the subscriber available. If not, the profile is retrieved from HSS. 3GPP AAA Server verifies that the subscriber is authorized to use the EPS.

NOTE 8: This step could be performed at some other point, after step 5 and before step 14.

12. New keying materials MSK and EMSK are derived from CK' and IK' according to draft-arkko-eap-aka-kdf [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 on the USIM application on UICC. The USIM application verifies that AUTN is correct and hereby authenticates the network. If AUTN is incorrect, the terminal rejects the authentication (not shown in this example). If the sequence number is out of synch, terminal initiates a synchronization procedure, c.f. draft-arkko-eap-aka-kdf [23]. If AUTN is correct, the USIM application computes RES, IK and CK.

Samsung Ex. 1010, Page 15 of 41

The UE then computes (CK', IK') = F(CK, IK, <access network identity>) in the same way as the HSS. The UE derives required additional new keying material, including the key MSK, according to draft-arkko-eap-aka-kdf [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 draft-arkko-eap-aka-kdf [23].

Draft-arkko-eap-aka-kdf [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 draft-arkko-eap-aka-kdf [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 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 draft-arkko-eap-aka-kdf [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

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 20). The 3GPP AAA Server also includes the key MSK, draft-arkko-eap-aka-kdf [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. The 3GPP AAA Server shall initiate the 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.

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: More detailed provisions may be required for particular access networks, similar to those in bullet 25 in TS 33.234 [9], subclause 6.1.1.1 for WLAN access networks.

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 draft-arkko-eap-aka-kdf [23] and an indication shall be sent to HSS.

Samsung Ex. 1010, Page 16 of 41

6.3 Fast re-authentication procedure for trusted access

Fast re-authentication for EAP-AKA' is specified in draft-arkko-eap-aka-kdf [23]. Fast re-authentication re-uses keys derived on the previous full authentication. Fast re-authentication does not involve the HSS nor the USIM application, 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 USIM application 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 draft-arkko-eap-aka-kdf [23].

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

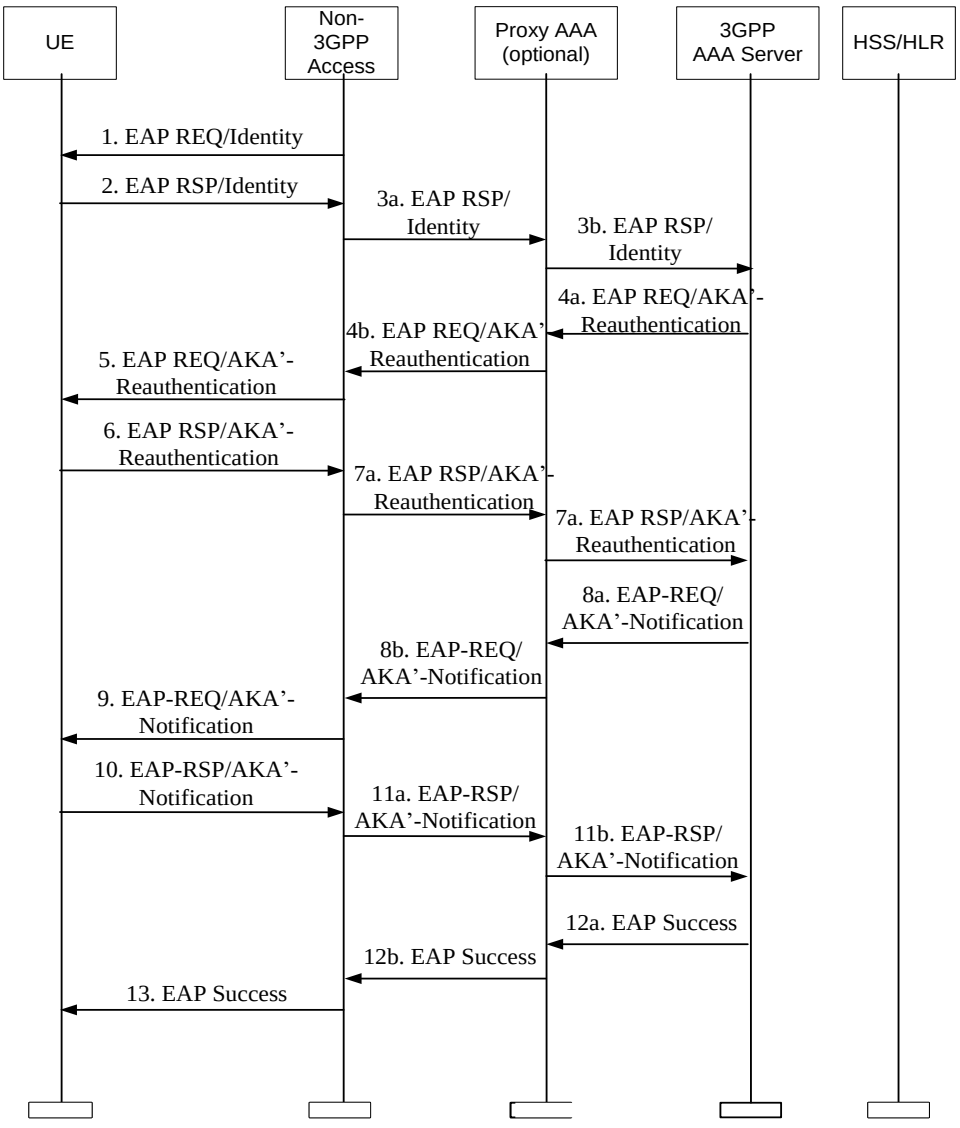


Figure 6.3-1: Non-3GPP Fast Re-authentication

Samsung Ex. 1010, Page 17 of 41

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).

   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.

   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.
5. The Non-3GPP Access Network forwards the EAP Request message to the UE.
6. 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.

   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.
7. The Non-3GPP Access Network forwards the response toward the AAA server.
8. 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.
9. The Non-3GPP Access Network forwards the EAP Request/AKA'-Notification message to the UE.
10. The UE sends the EAP Response/AKA'-Notification.
11. 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.
12. 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.
13. 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 draft-arkko-eap-aka-kdf [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

Samsung Ex. 1010, Page 18 of 41

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.

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 a USIM application 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.

Samsung Ex. 1010, Page 19 of 41

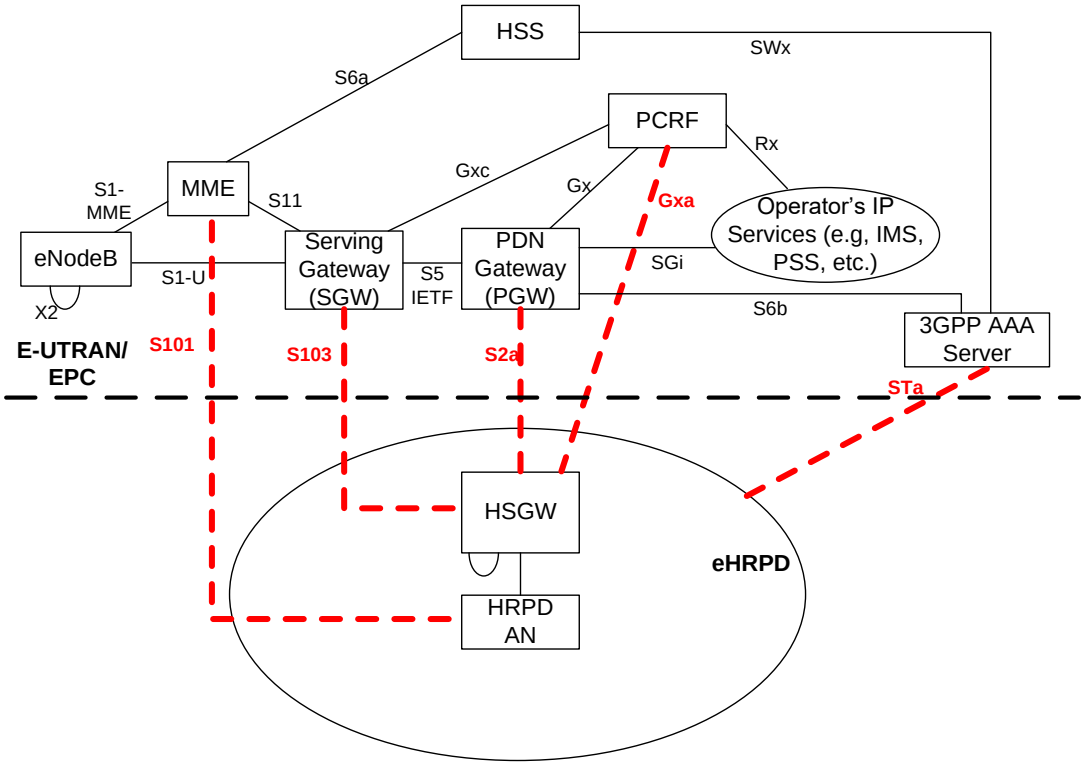


Figure 7.2.1.1-1: Basic non-roaming architecture for HRPD-LTE Interworking. Interworking reference points are highlighted.

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 33.abc [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 33.abc [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].

Samsung Ex. 1010, Page 20 of 41

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. draft-arkko-eap-aka-kdf [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 1: Initial access to the EPS via HRPD is described in the TS 23.402 [5].

NOTE 2: TS 23.402 [5] requires access authentication for trusted non-3GPP systems to be based on EAP-AKA'.

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

Editor's Note: General Concepts for Interworking between E-UTRAN and WIMAX are described in TS 23.402 [5] Section 4.1.2.

Samsung Ex. 1010, Page 21 of 41

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 4306 [3],in order to establish IPSec security associations.
- Public key signature based authentication with certificates, as specified in RFC 4306 [3], 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 4306 [3], shall be used to authenticate UEs.
- For profile for IKEv2, IPsec ESP and certificate contents and processing refer to subclause 8.2.4.

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 4306 [3]. 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.

Samsung Ex. 1010, Page 22 of 41

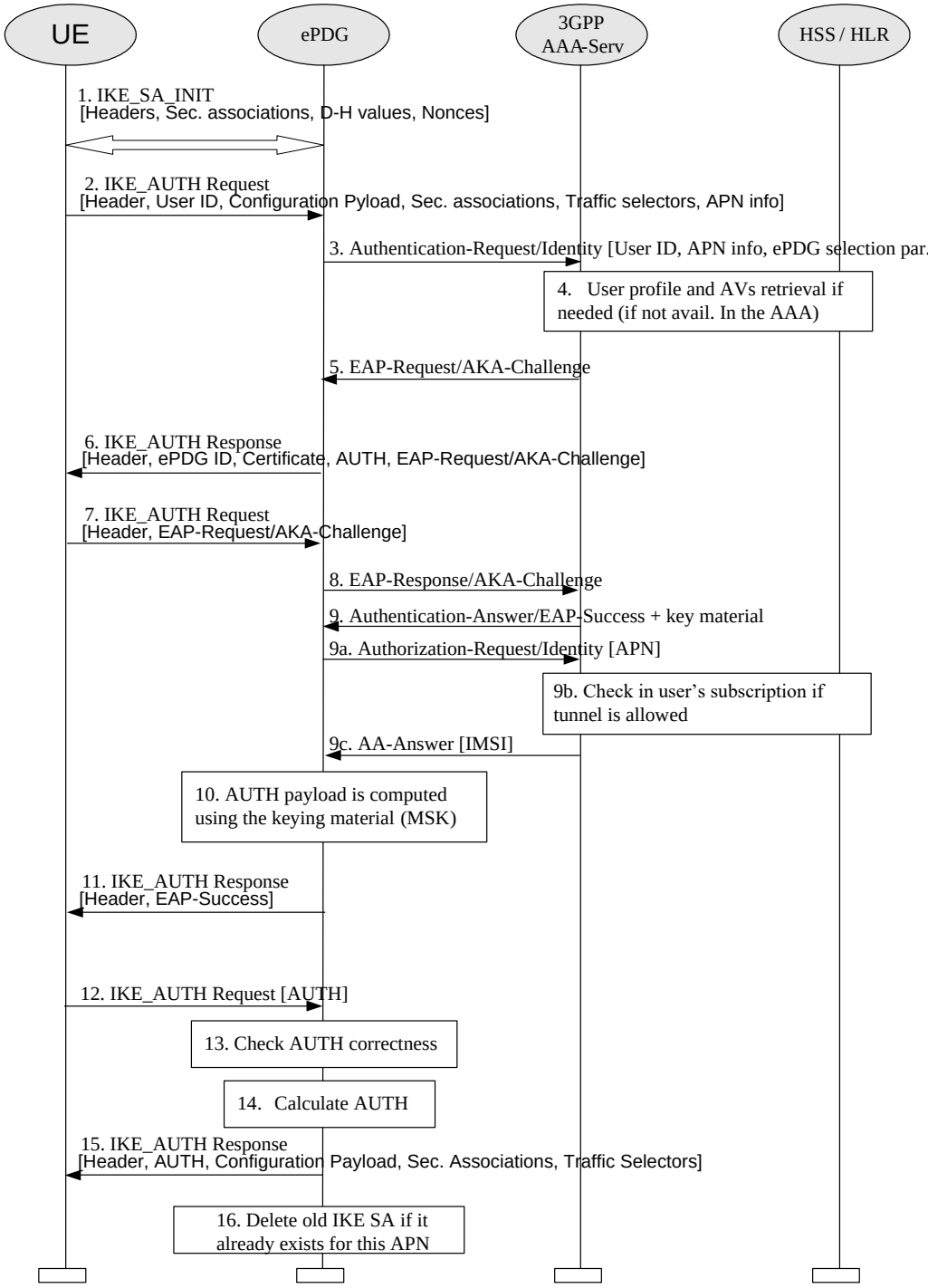


Figure 8.2.2-1: Tunnel full authentication and authorization

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

Samsung Ex. 1010, Page 23 of 41

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 a remote IP Address.

3. The ePDG sends the Authentication Request message with an empty EAP AVP to the 3GPP AAA Server, containing the user identity and APN. The ePDG shall include a parameter indicating that the authentication is being performed for tunnel establishment with an ePDG (and not an I-WLAN PDG as defined in TS 33.234 [9]). This will help the 3GPP AAA Server distinguish among authentications for 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).

4. 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 3 indicating that the authentication is being performed for tunnel establishment with an ePDG 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.

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

6. The ePDG responds 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). It completes the negotiation of the child security associations as well. 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 only payload (apart from the header) in the IKEv2 message is the EAP message.

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

9. When all checks are successful, the 3GPP AAA Server sends the Authentication Answer including 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 parameter, as defined in RFC 4072 [10].

9a. The ePDG sends the Authorization Request message with an empty EAP AVP to the 3GPP AAA Server, containing APN.

9b. The 3GPP AAA Server checks in user's subscription if he/she is authorized to establish the tunnel.

The counter of IKE SAs for that APN is stepped up. If the maximum number of IKE SAs for that APN is exceeded, the 3GPP AAA Server shall send an indication to the ePDG that established the oldest active IKE SA (it could be the same ePDG or a different one) to delete the oldest established IKE SA. The 3GPP AAA Server shall update accordingly the information of IKE SAs active for the APN.

9c. The 3GPP AAA Server sends the AA-Answer to the ePDG. The 3GPP AAA Server shall send the IMSI within the AA-Answer, if the Authorization Request message (9a) contains the temporary identity, i.e. if the AAR does not contain the IMSI.

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 4306 [3]. These two first messages had not been authenticated before as there was no key material available yet. According to RFC 4306 [3], 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.

Samsung Ex. 1010, Page 24 of 41

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.

16. If the ePDG detects that an old IKE SA for that APN already exists, it will delete the IKE SA and send the UE an INFORMATIONAL exchange with a Delete payload, as specified in RFC 4306 [3], in order to delete the old IKE SA in UE.

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 USIM application, 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.

NOTE: The ePDG cannot indicate to the UE that fast re-authentication for EAP-AKA be used by sending a re-authentication identity to the UE as the EAP Request/AKA Identity messages is omitted, cf. step 5 in subclause 8.2.2 of the present document. This is a difference to the use of EAP in clause 6.

The security level of fast re-authentication for EAP-AKA is lower as it does not prove the presence of the USIM application 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.

Samsung Ex. 1010, Page 25 of 41

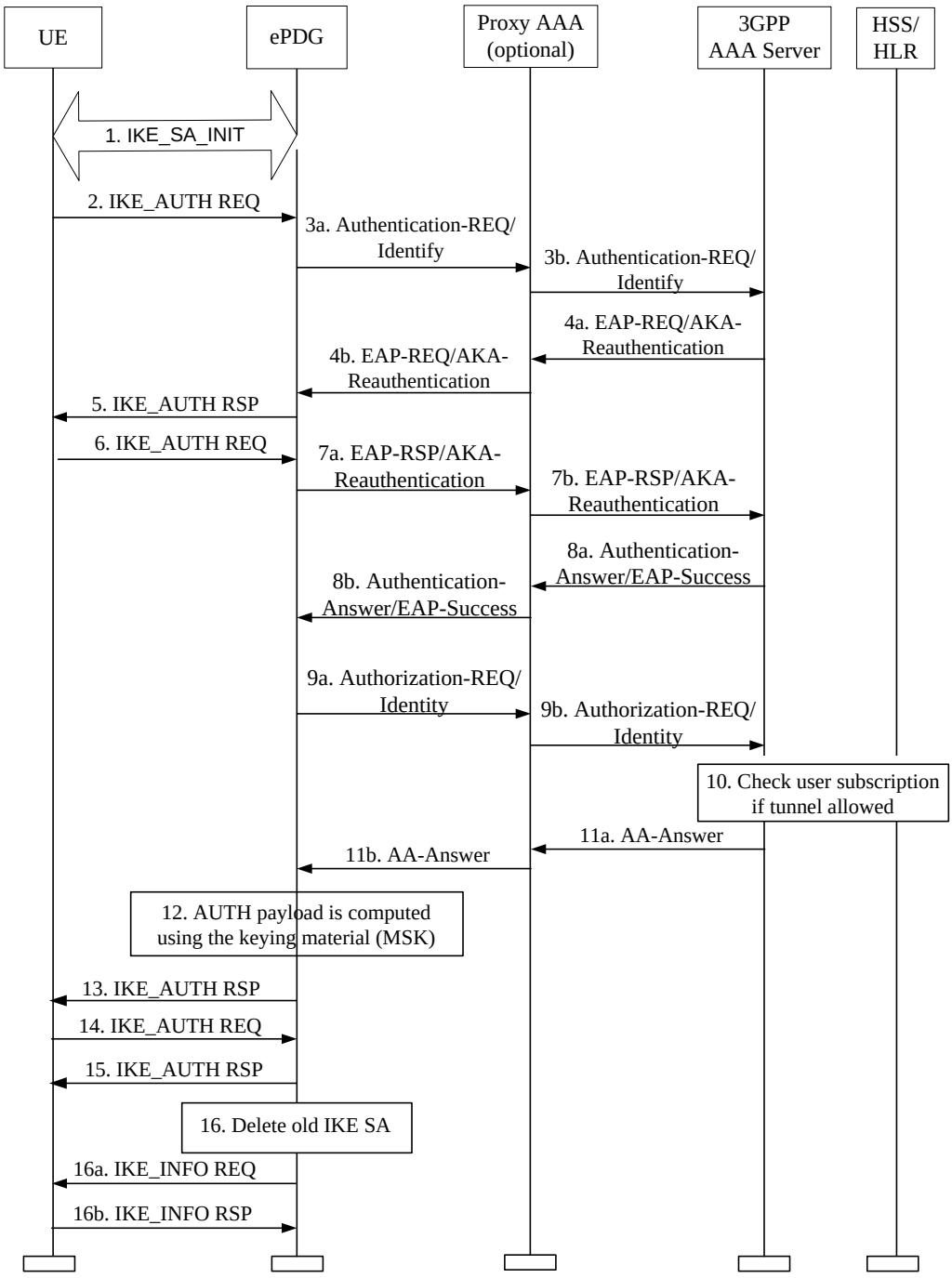


Figure 8.2.3-1: Untrusted Tunnel - Fast Re-authentication

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 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 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.

Samsung Ex. 1010, Page 26 of 41

3. The ePDG sends the Authentication Request message with an EAP AVP toward the 3GPP AAA Server, containing the re-authentication identity. The ePDG shall include a parameter indicating that the authentication is being performed for tunnel establishment with an ePDG (and not an I-WLAN PDG as defined in TS 33.234 [9]). This will help the 3GPP AAA Server distinguish among authentications for 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).

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). It completes the negotiation of the child security associations as well. 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 only payload (apart from the header) in the IKEv2 message is the EAP message.

7. The ePDG 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 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 parameter, as defined in RFC 4072 [10].

9. The ePDG sends the Authorization Request message towards the 3GPP AAA Server serving the APN containing an empty EAP AVP.

10. The 3GPP AAA Server checks in user's subscription for authorization to establish the tunnel.

    The counter of IKE SAs for that APN is stepped up. If the maximum number of IKE SAs for that APN is exceeded, the 3GPP AAA Server shall send an indication to the ePDG that established the oldest active IKE SA (it could be the same ePDG or a different one) to delete the oldest established IKE SA. The 3GPP AAA Server shall update accordingly the information of IKE SAs active for the APN.

11. The 3GPP AAA Server sends the AA-Answer toward the ePDG. The 3GPP AAA Server shall send the IMSI within the AA-Answer.

12. 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 4306 [3]. These two first messages had not been authenticated before as there were no key material available yet. According to RFC 4306 [3], the shared secret generated in an EAP exchange (the MSK), when used over IKEv2, shall be used to generated the AUTH parameters.

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

14. 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.

15. 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.

16. If the ePDG detects that an old IKE SA for that APN already exists, it will delete the IKE SA and send to the UE an INFORMATIONAL exchange with a Delete payload, as specified in RFC 4306 [3], in order to delete the old IKE SA in UE.

8.2.4 Security profiles

The profiles for IKEv2 and IPsec ESP as defined in TS 33.234 [9] shall be used.

For ePDG certificates, the certificate profiles as defined in TS 33.234 [9] shall be used.

Samsung Ex. 1010, Page 27 of 41

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 4306, 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].

Samsung Ex. 1010, Page 28 of 41

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

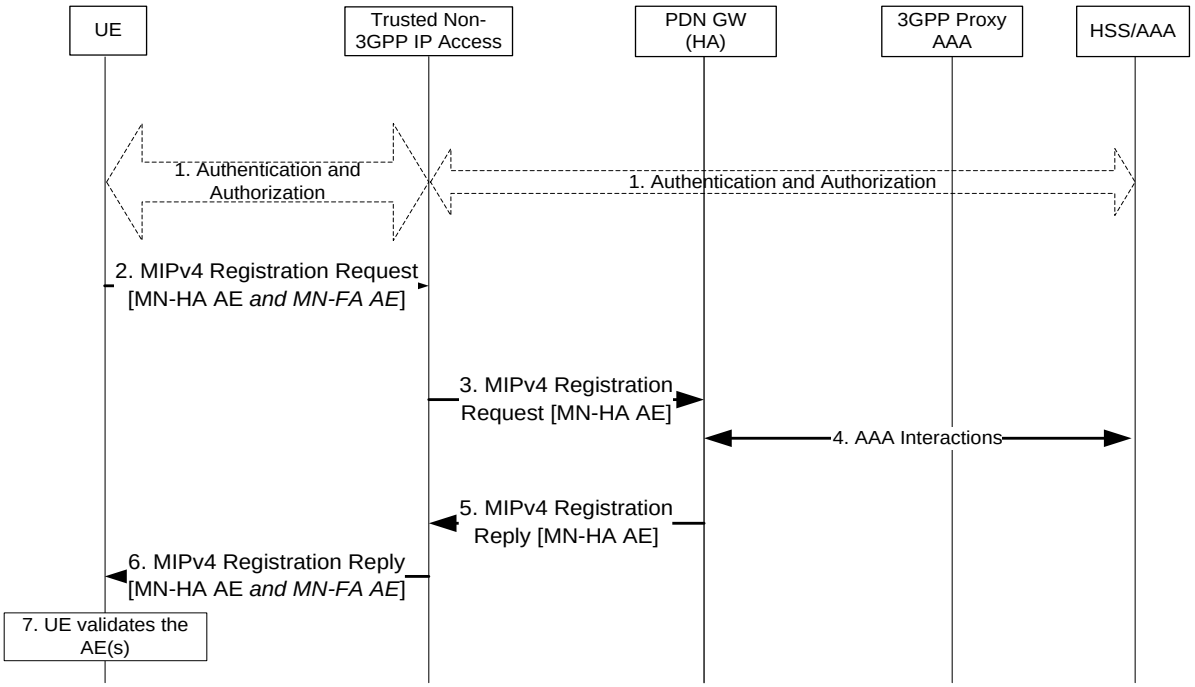


Figure 9.2.1.2.1-1: MIPv4 bootstrapping

The event that triggers Authentication and Authorization in step 1 or in step 3 between the Trusted Non-3GPP IP Access and the EAP Server 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.

Samsung Ex. 1010, Page 29 of 41

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 using the following formula:

MIP-RK = KDF (EMSK, “Mobile IP Root Key” | "\0" | length)

Where:

"\0" is a NULL octet (0x00 in hex)

length is a 2 octet unsigned integer in network byte order

KDF in this clause is as specified in [19]

Editor’s Note: The label “Mobile IP Root Key” is to be registered with IANA.

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 Mobile IP Root Key "| APN))

The MIP-SPI is derived at the UE and at the 3GPP AAA server. If the generated SPI value is smaller than 256, then this value is increased by 256. The AAA and the UE checks whether this SPI value is already in use for the given UE, if so, the SPI value is incremented by 1 until there is no collision. 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,"MIP4 MN HA Key" | 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.

Samsung Ex. 1010, Page 30 of 41

Editors Note: If the HA IP address is not determine in step 1 of subclause 9.2.2, then the MN-HA-MIP4 key derivation procedure is FFS.

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 and the HA-RK 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 RFC4877 [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 RFC4306, in order to establish IPsec security associations.

Samsung Ex. 1010, Page 31 of 41

- Public key signature based authentication with certificates, as specified in RFC 4306 [3], 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 RFC4877 [2] and RFC 4306 [3], is used to authenticate UEs, which contain a USIM.

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.

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

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 Address through the Configuration Payload in the IKE_AUTH exchange by including an INTERNAL_IP6_ADDRESS attribute.

When the Home Agent processes the message, it allocates a HoA and sends it a CFG_REPLY message.

The IPv6 Home Address 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.

Samsung Ex. 1010, Page 32 of 41

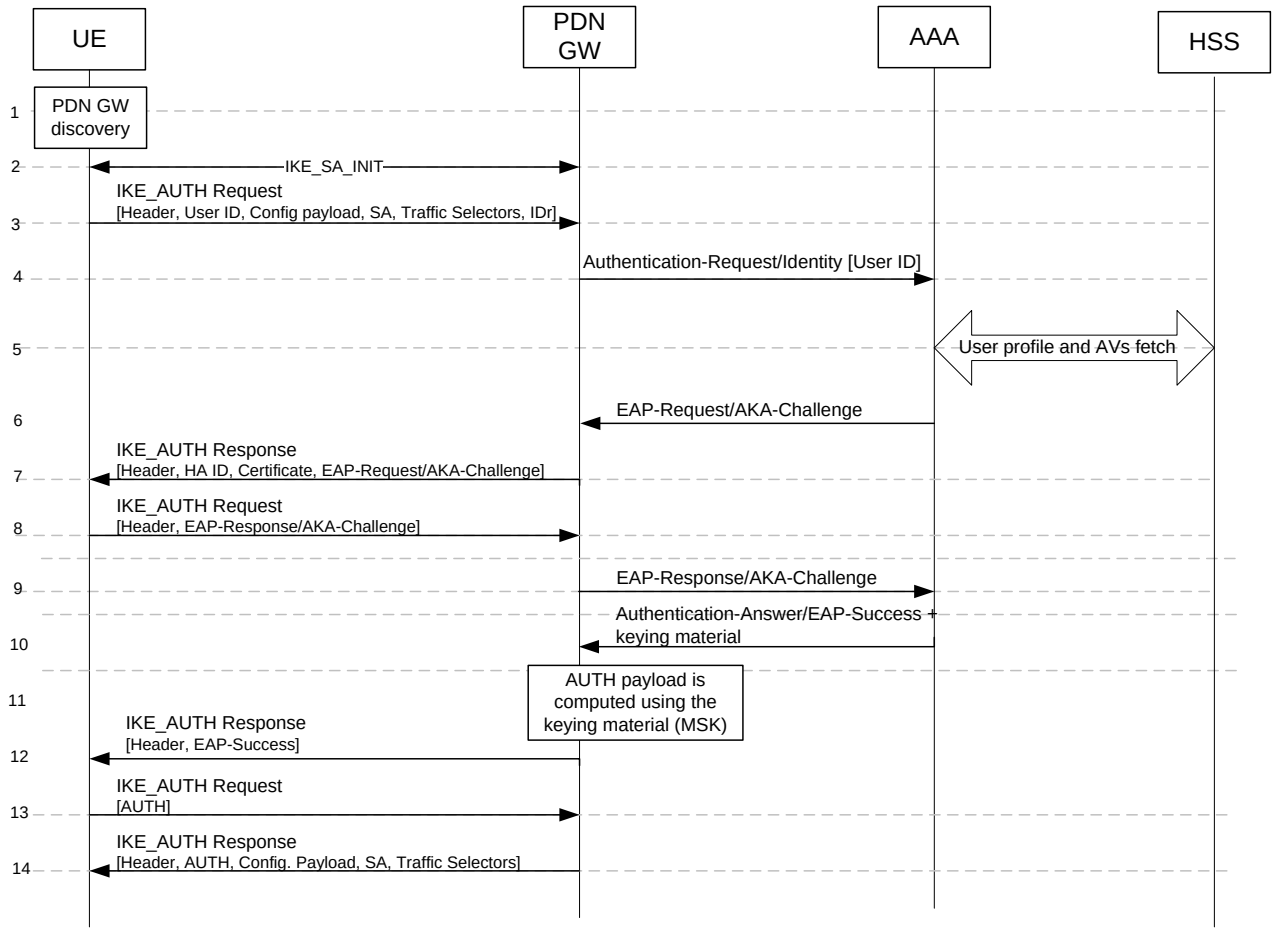


Figure 9.2.2.2.1-1: DS-MIPv6 bootstrapping based on IKEv2

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.

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.

Samsung Ex. 1010, Page 33 of 41

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) RAND and AUTN are passed to the USIM, which checks 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 only payload (apart from the header) in the IKEv2 message is the EAP message which contains the AKA response, RES.

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.

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]. 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.

9.2.2.2.2 Fast Re-authentication

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 USIM application, 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.

NOTE: The PDN GW cannot indicate to the UE that fast re-authentication for EAP-AKA be used by sending a re-authentication identity to the UE as the EAP Request/AKA Identity messages is omitted, cf. step 5 in subclause 8.2.2 of the present document. This is a difference to the use of EAP in clause 6.

The security level of fast re-authentication for EAP-AKA is lower as it does not prove the presence of the USIM application 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.

Samsung Ex. 1010, Page 34 of 41

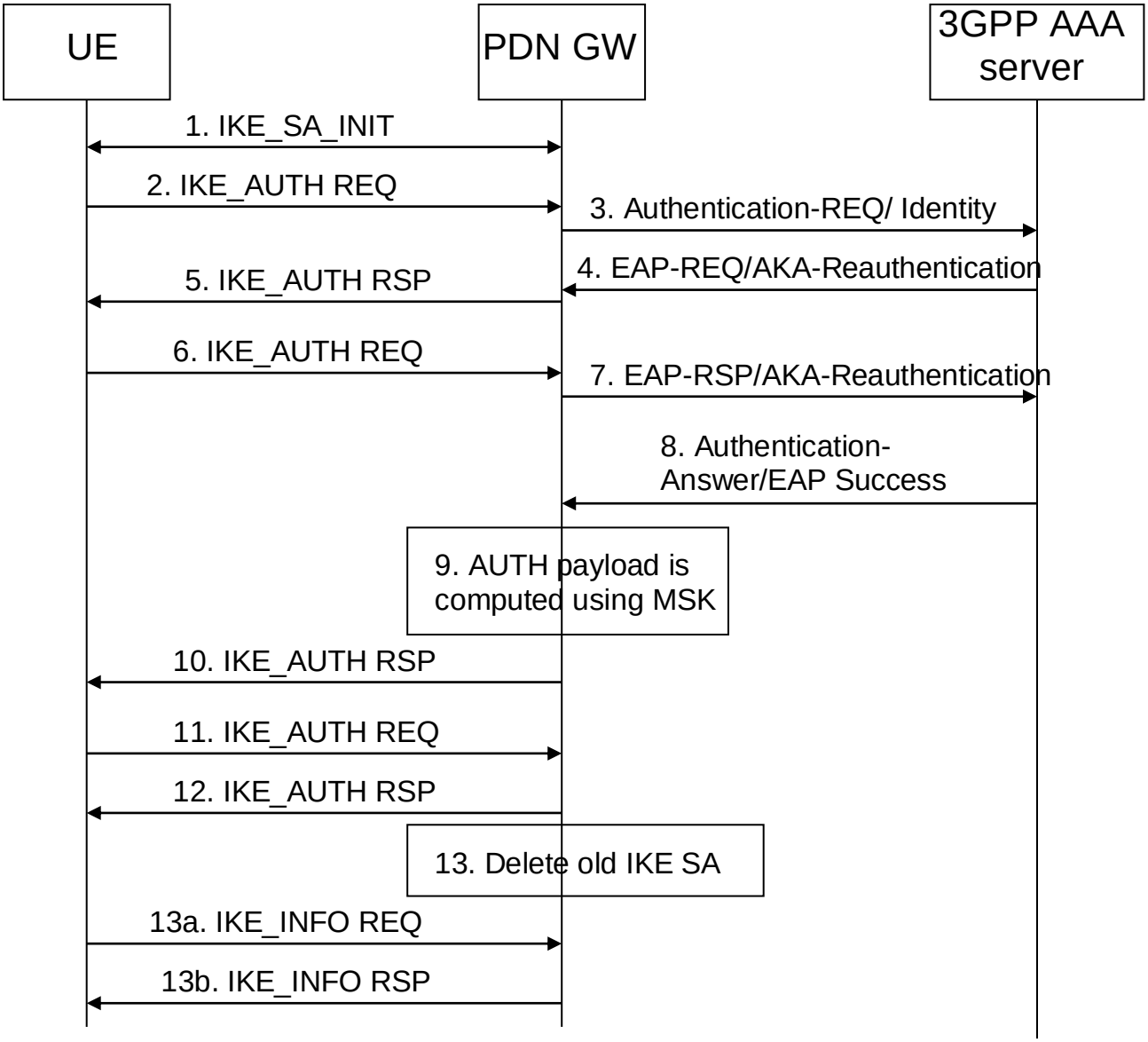


Figure 9.2.2.2.2-1: Fast Re-authentication for DSMIPv6

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 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).

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). It

Samsung Ex. 1010, Page 35 of 41

completes the negotiation of the child security associations as well. 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 only payload (apart from the header) in the IKEv2 message is the EAP message.

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 4306 [3]. These two first messages had not been authenticated before as there was no key material available yet. According to RFC 4306 [3], 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.

13. If the PDN GW detects that and old IKE SA for that APN already exists, it will delete the IKE SA and send to the UE an INFORMATIONAL exchange with a Delete payload, as specified in RFC 4306 [3], in order to delete the old IKE SA in UE.

9.2.2.3 Security Profiles

The profiles for IKEv2 and IPsec ESP as defined in TS 33.234 [9] shall be used with the exception that ESP in transport mode shall be used.

For PDN GW certificates, the certificate profiles as defined in TS 33.234 [9] 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 S8b (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 S8b:

Samsung Ex. 1010, Page 36 of 41

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 S8b. TS 33.310 [12] may be applied regarding the use of certificates with the security mechanisms of TS 33.210 [6].

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 HRPD PDSN 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 is secure as described in clause 11.

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.

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].

Samsung Ex. 1010, Page 37 of 41

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.

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: 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].

NOTE: The above security solution protects the pull based ANDSF solution only. It can also protect the push based ANDSF solution if the UE has previously used pull based ANDSF solution and the corresponding TLS connection is still available. However, it can be noted that 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.

Samsung Ex. 1010, Page 38 of 41

Annex A (normative): Key derivation functions

A.1 KDF interface and input parameter construction

The input parameters and their lengths shall be concatenated into a string S as follows:

1. The length of each input parameter in octets shall be encoded into two-octet string:

   a) express the number of octets in input parameter Pi as a number k in the range [0, 65535];

   b) Li is then a two-octet representation of the number k, with the most significant bit of the first octet of Li equal to the most significant bit of k, and the least significant bit of the second octet of Li equal to the least significant bit of k.

EXAMPLE: If Pi contains 258 octets then Li will be the two-octet string 0x01 0x02.

2. String S shall be constructed from n input parameters as follows:

   S = FC || P0 || L0 || P1 || L1 || P2 || L2 || P3 || L3 ||... || Pn || Ln

   where:

   FC is single octet used to distinguish between different instances of the algorithm,

   P0 ... Pn are the n input parameters, and

   L0 ... Ln are the two-octet representations of the length of the corresponding input parameters.

3. The final output, i.e. the derived key is equal to the KDF computed on the string S using the key Key. The present document defines the following KDF:

   derived key = HMAC-SHA-256 (Key, S),

as specified in [10] and [11], which has the KDF identity 1.

NOTE 1: Various values for parameter FC are used by TS 33.220 [8] and TS 33.401 [16], so the numbering starts at 0x20 in the present document to ensure that no input collisions will occur.

A character string shall be encoded to an octet string according to the encoding rules as specified in 3GPP TS 24.302 [22].

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.

Samsung Ex. 1010, Page 39 of 41

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'.

Samsung Ex. 1010, Page 40 of 41

Annex B (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	17	-	Resolution of Ed notes on use of EAP-AKA in IKEv2	8.0.0	8.1.0
2008-09	SA#41	SP-080488	0004	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	0002	-	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	0012	-	correction of 33.402	8.0.0	8.1.0
2008-09	SA#41	SP-080488	0013	-	Clarification of text on access network identities	8.0.0	8.1.0
2008-09	SA#41	SP-080488	0014	-	Clarification of use of AMF separation bit with EAP-AKA access authentication	8.0.0	8.1.0
2008-09	SA#41	SP-080488	0015	-	Clarification on handling of authentication vectors in the 3GPP AAA server	8.0.0	8.1.0
2008-09	SA#41	SP-080488	0007	1	Resolution of Ed notes on MIPv4 Root key generation	8.0.0	8.1.0
2008-09	SA#41	SP-080488	0016	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	0018	-	Removing the restriction on AKA for Trusted Access	8.0.0	8.1.0
2008-09	SA#41	SP-080488	0022	1	Methods to avoid impersonation attacks on S2c	8.0.0	8.1.0
2008-09	SA#41	SP-080488	0024	-	Note on SNID IP binding	8.0.0	8.1.0
2008-09	SA#41	SP-080488	0005	1	CR on UE-ANDSF security	8.0.0	8.1.0
2008-09	SA#41	SP-080641	0025	1	CR on EAP AKA (relaxation scenario)	8.0.0	8.1.0
2008-12	SA#42	SP-080739	26	-	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	27	-	MIPv4 SPI Collision Avoidance	8.1.1	8.2.0
2008-12	SA#42	SP-080739	28	-	MN-HA Key generation during initial attach or additional PDN connectivity	8.1.1	8.2.0
2008-12	SA#42	SP-080739	29	-	Handling of Mobility Keys during Re-authentication	8.1.1	8.2.0
2008-12	SA#42	SP-080739	30	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	31	-	Resolution of Editor's note on tunnel fast re-authentication	8.1.1	8.2.0
2008-12	SA#42	SP-080739	32	1	Clarifications to security procedures for DSMIPv6	8.1.1	8.2.0
2008-12	SA#42	SP-080739	35	-	Adding EMSK derivation in clause 6.2	8.1.1	8.2.0
2008-12	SA#42	SP-080739	36	1	Fast re-authentications for DSMIPv6	8.1.1	8.2.0
2008-12	SA#42	SP-080739	37	-	AMF separation bit for untrusted non-3gpp access for S2c	8.1.1	8.2.0
2008-12	SA#42	SP-080739	38	-	Finalising the PMIP security requirements	8.1.1	8.2.0
2008-12	SA#42	SP-080739	39	-	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	40	-	Change on some names of interfaces in 33.402 and some corrections	8.1.1	8.2.0
2008-12	SA#42	SP-080739	41	-	Removing editor's note on legacy UEs	8.1.1	8.2.0
2008-12	SA#42	SP-080739	42	-	Correction of text on access authentication for untrusted access	8.1.1	8.2.0
2008-12	SA#42	SP-080739	43	-	Correction of text on access authentication for untrusted access	8.1.1	8.2.0
2008-12	SA#42	SP-080739	44	-	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	45	-	Modification of the MIPv4 bootstrapping	8.1.1	8.2.0
2008-12	SA#42	SP-080739	46	-	ANDSF security	8.1.1	8.2.0
2008-12	SA#42	SP-080739	34	-	MIPv4 support for Additional PDN connectivity	8.1.1	8.2.0

Samsung Ex. 1010, Page 41 of 41