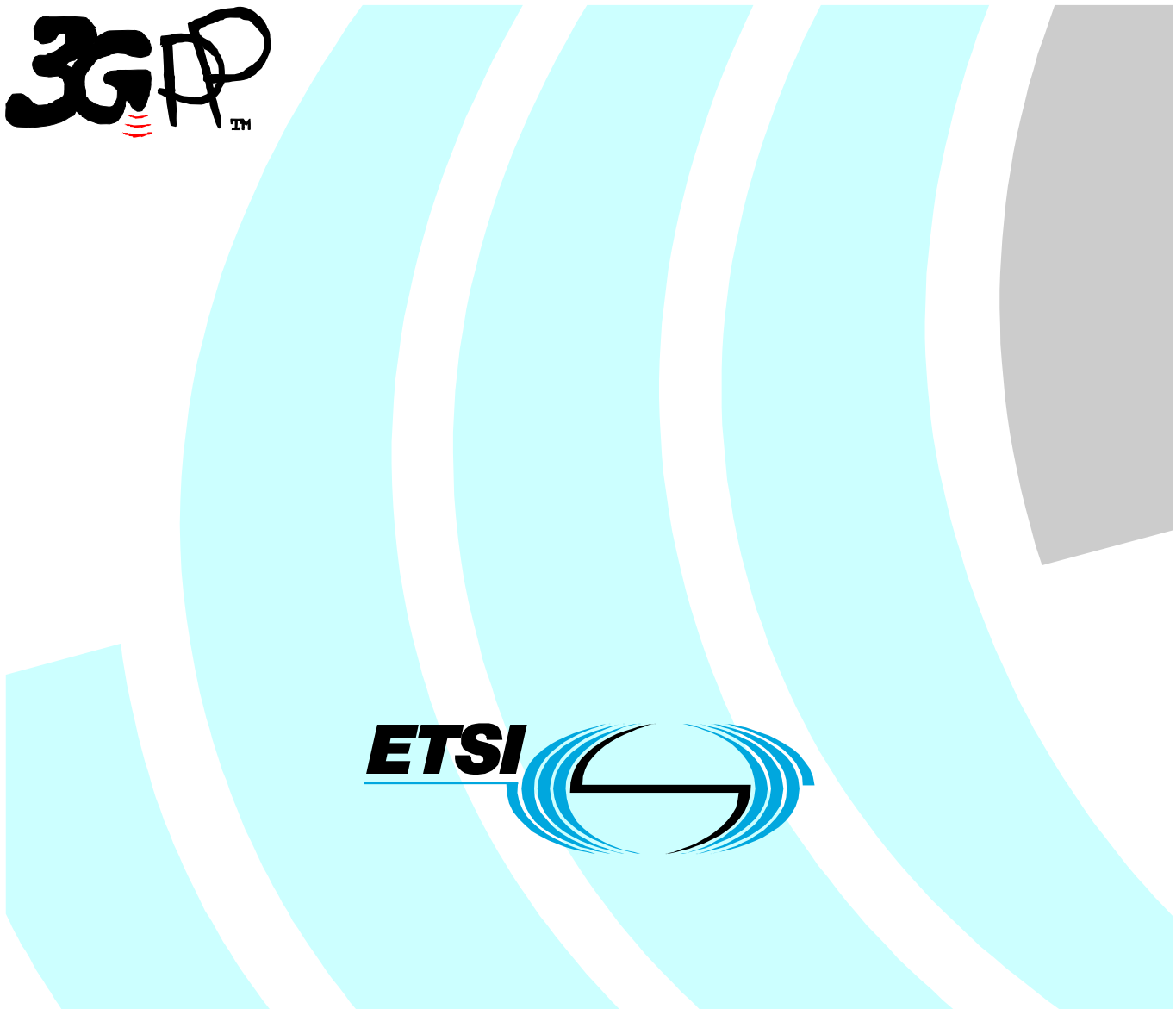
ETSI TS 133 234 V6.9.0 (2007-03)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
3G security;
Wireless Local Area Network (WLAN) interworking security
(3GPP TS 33.234 version 6.9.0 Release 6)



Reference
RTS/TSGS-0333234v690

Keywords
SECURITY, UMTS

ETSI

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

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

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

Foreword

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

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

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Contents

Foreword

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

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

Version x.y.z

where:

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

Introduction

WLAN is not a single radio technology: several different technologies fall into the category called WLAN. Existing industry standard is IEEE 802.11b operating at 2.4 GHz ISM band. New entrant for this same band is Bluetooth and technologies such as IEEE 802.11a and ETSI BRAN Hiperlan2 are being developed for the 5 GHz band.

Despite the different radio technologies, all these WLAN systems are commonly used for transportation of IP datagrams. The specific WLAN technology used in each wireless IP network is not very visible for the layers above IP.

This Technical Specification covers the models and mechanisms under which these technologies can be used to securely interwork with 3GPP networks.

1 Scope

The present document specifies the security architecture; trust model and security requirements for the interworking of the 3GPP System and WLAN Access Networks. This specification is not limited to WLAN technologies. It is also valid for other IP based Access Networks that support the same security capabilities towards the interworking system as WLAN does. These security capabilities are addressed in section 4 of this specification.

Specifications of the appropriate mechanisms for user and network authentication, key management, service authorization, confidentiality and integrity protection of user and signalling data are also provided.

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 22.934: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking".

[2] 3GPP TR 23.934: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) Interworking; Functional and architectural definition".

[3] IETF RTC 3748: "Extensible Authentication Protocol (EAP)".

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

[5] RFC 4186, January 2006: "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)".

[6] IEEE 802.11i-2004: "IEEE Standard for Information technology - Telecommunications and information exchange between systems - LAN/MAN - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications-Amendment 6: MAC Security Enhancements".

[7] RFC 2716, October 1999: "PPP EAP TLS Authentication Protocol".

[8] SHAMAN/SHA/DOC/TNO/WP1/D02/v050, 22-June-01: "Intermediate Report: Results of Review, Requirements and Reference Architecture".

[9] ETSI TS 101 761-1 v1.3.1B: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 1: Basic Data Transport".

[10] ETSI TS 101 761-2 v1.2.1C: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 2: Radio Link Control (RLC) sublayer".

[11] ETSI TS 101 761-4 v1.3.1B: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 4 Extension for Home Environment".

[12] ETSI TR 101 683 v1.1.1: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; System Overview".

[13] 3GPP TS 23.234: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) Interworking; System Description".

[14] RFC 2486, January 1999: "The Network Access Identifier". [15] RFC 2865, June 2000: "Remote Authentication Dial In User Service (RADIUS)".

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

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

[18] 3GPP TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing and identification".

[19] IEEE P802.1X/D11 June 2001: "Standards for Local Area and Metropolitan Area Networks: Standard for Port Based Network Access Control".

[20] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[21] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

[22] CAR 020 SPEC/0.95cB: "SIM Access Profile, Interoperability Specification", version 0.95VD.

[23] draft-ietf-aaa-eap-08.txt, June 2004: "Diameter Extensible Authentication Protocol (EAP) Application". IETF Work in progress

[24] RFC 3588, September 2003: "Diameter base protocol".

[25] RFC 3576, July 2003: "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)".

[26] RFC 3579, September 2003: "RADIUS (Remote Authentication Dial In User Service) Support for Extensible Authentication Protocol (EAP)".

[27] draft-ietf-eap-keying-02.txt, June 2004: "EAP Key Management Framework". IETF Work in progress

[28] E. Barkan, E. Biham, N. Keller: "Instant Ciphertext-Only Cryptoanalysis of GSM Encrypted Communication", Crypto 2003, August 2003.

[29] RFC 4306, December 2005: "Internet Key Exchange (IKEv2) Protocol".

[30] RFC 4303,December 2005: "IP Encapsulating Security Payload (ESP)".

[31] draft-ietf-ipsec-ui-suites-06.txt, April 2004: "Cryptographic Suites for IPsec". IETF Work in progress

[32] draft-ietf-ipsec-udp-encaps-09.txt, May 2004: "UDP Encapsulation of IPsec Packets". IETF Work in progress

[33] draft-ietf-ipsec-ikev2-algorithms-05.txt, April 2004: "Cryptographic Algorithms for use in the Internet Key Exchange Version 2". IETF Work in progress

[34] RFC 2104, February 1997: "HMAC: Keyed-Hashing for Message Authentication".

[35] RFC 2404, November 1998: "The Use of HMAC-SHA-1-96 within ESP and AH".

[36] RFC 2548, March 1999: " Microsoft Vendor-specific RADIUS Attributes".

[37] draft-arkko-radext-multi-service-decisions-01.txt, February 2005. " Policy Decisions for Users with Access to Multiple Services ". IETF Work in progress

[38] RFC 3279, April 2002: "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[39] RFC 3280, April 2002: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[40] 3GPP TS 27.007: "Technical Specification Group Terminals; AT command set for User Equipment (UE)".

[41] ETSI TS 102.310: "Smart Cards; Extensible Authentication Protocol support in the UICC".

[42] ETSI TS 102.221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

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

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

3GPP - WLAN Interworking: Used generically to refer to interworking between the 3GPP system and the WLAN family of standards.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

Local interface: an interface between the devices that may conform to the WLAN UE, normally one device with WLAN capabilities and one UICC or SIM card holding device.

Temporary identity: an identity given by the home network to the WLAN UE, used to identify the user temporarily, normally in one authentication process lifetime. In this TS it refers to a pseudonym or a re-authentication identity.

Tunnel: it refers to an IPsec security association used in WLAN 3GPP IP access to protect the communications from the WLAN UE to the 3GPP network. It is preceded by an IKE negotiation.

W-APN: WLAN Access Point Name – identifies an IP network and a point of interconnection to that network (Packet Data Gateway).

WLAN 3GPP IP Access: Access to an IP network via the 3GPP system.

WLAN Direct IP Access: Access to an IP network is direct from the WLAN AN.

WLAN coverage: an area where wireless local area network access services are provided for interworking by an entity in accordance with WLAN standards.

WLAN-UE: user equipment to access a WLAN interworking with the 3GPP system, including all required security functions.

3.2 Abbreviations

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

AAA	Authentication Authorisation Accounting
AKA	Authentication and Key Agreement
EAP	Extensible Authentication Protocol
IKE	Internet Key Exchange

NAT	Network Address Translation
PDG	Packet Data Gateway
WAG	WLAN Access Gateway
WLAN	Wireless Local Area Network
WLAN AN	WLAN Access Network
W-APN	WLAN APN

4 Security Requirements for 3GPP-WLAN Interworking

The reference models for WLAN interworking from TS 23.234 [13] are reproduced in the following sub-sections.

4.1.1 Non roaming WLAN interworking Reference Model

The home network is responsible for access control and tunnel establishment.

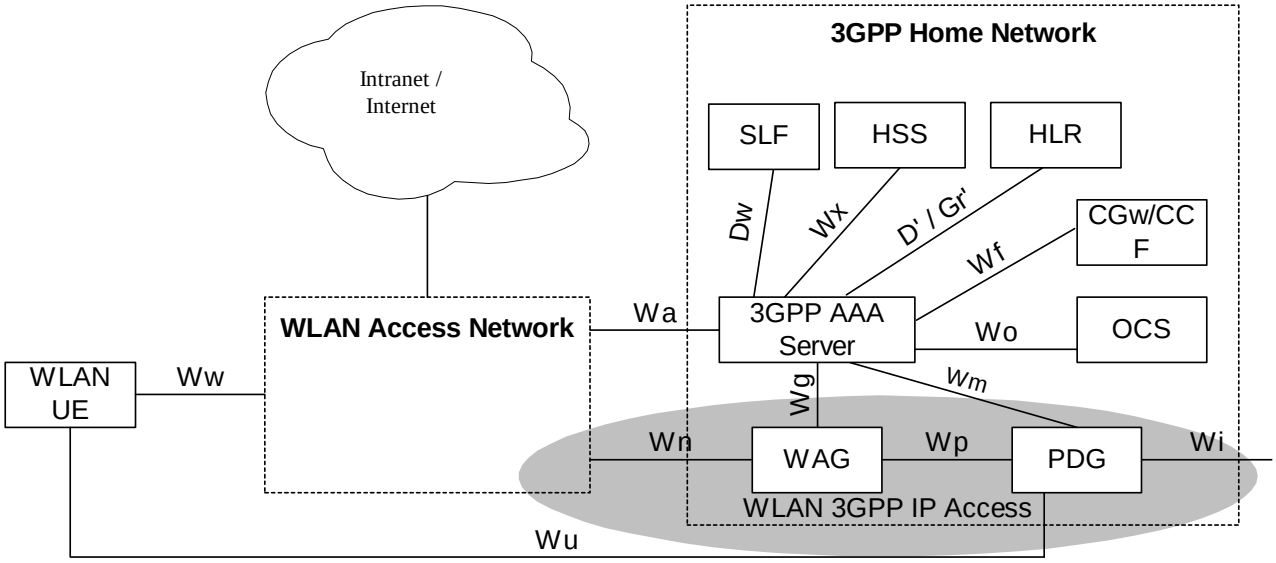


Figure 1: Non-roaming reference model (the shaded area refers to WLAN 3GPP IP Access functionality)

4.1.2 Roaming WLAN Interworking Reference Model, access to HPLMN services

The home network is responsible for access control and tunnel establishment. The traffic is routed through the visited network (using the WAG).

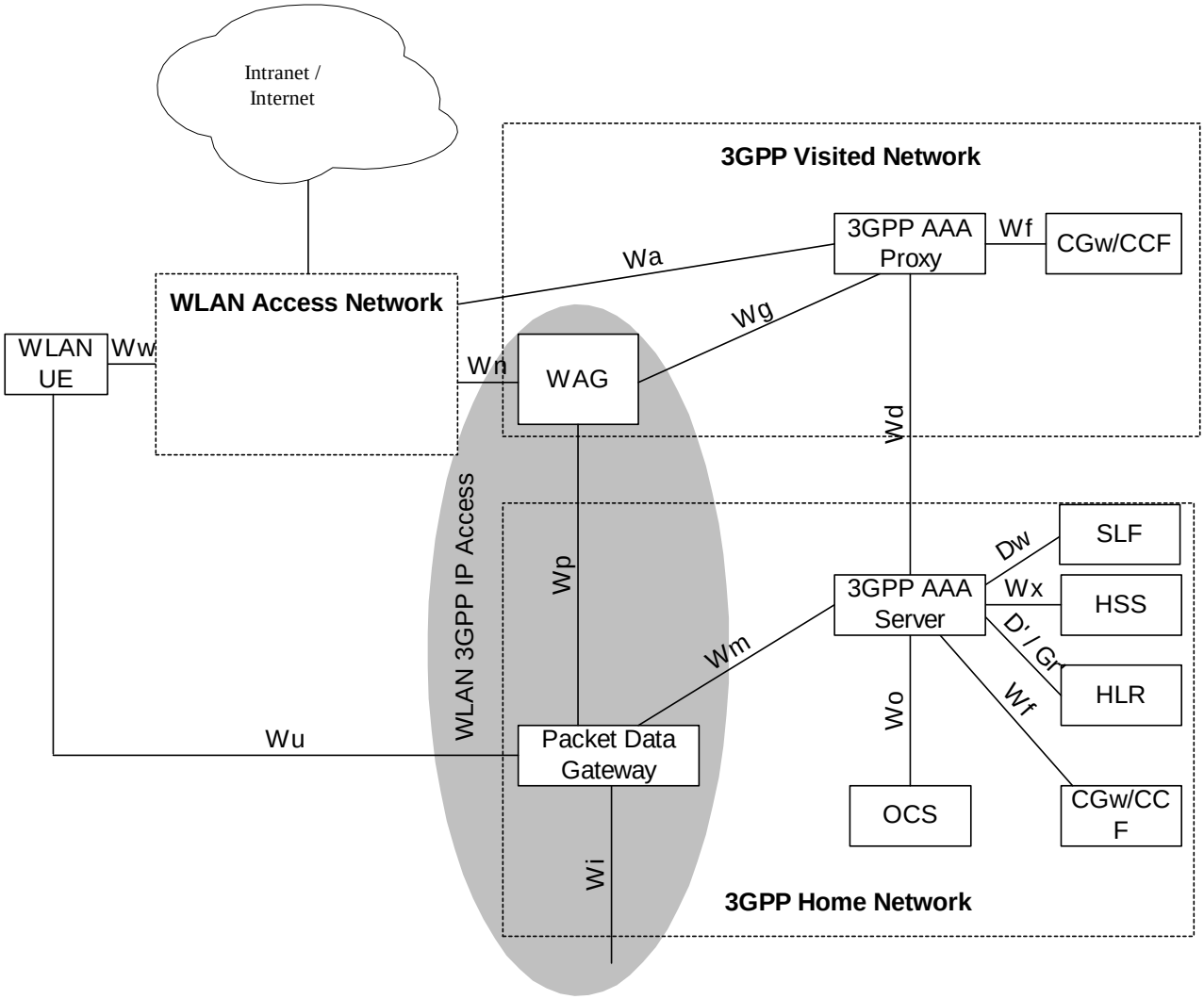


Figure 2: Roaming reference model - 3GPP PS based services provided via the 3GPP Home Network (the shaded area refers to WLAN 3GPP IP Access functionality)

4.1.3 Roaming WLAN Interworking Reference Model, access to VPLMN services

The home network is responsible for access control, but the authorization decision of tunnel establishment will be taken by the 3GPP proxy AAA based on own information plus information received from the home network. The VPLMN will take part in tunnel establishment (either the WAG or the PDG).

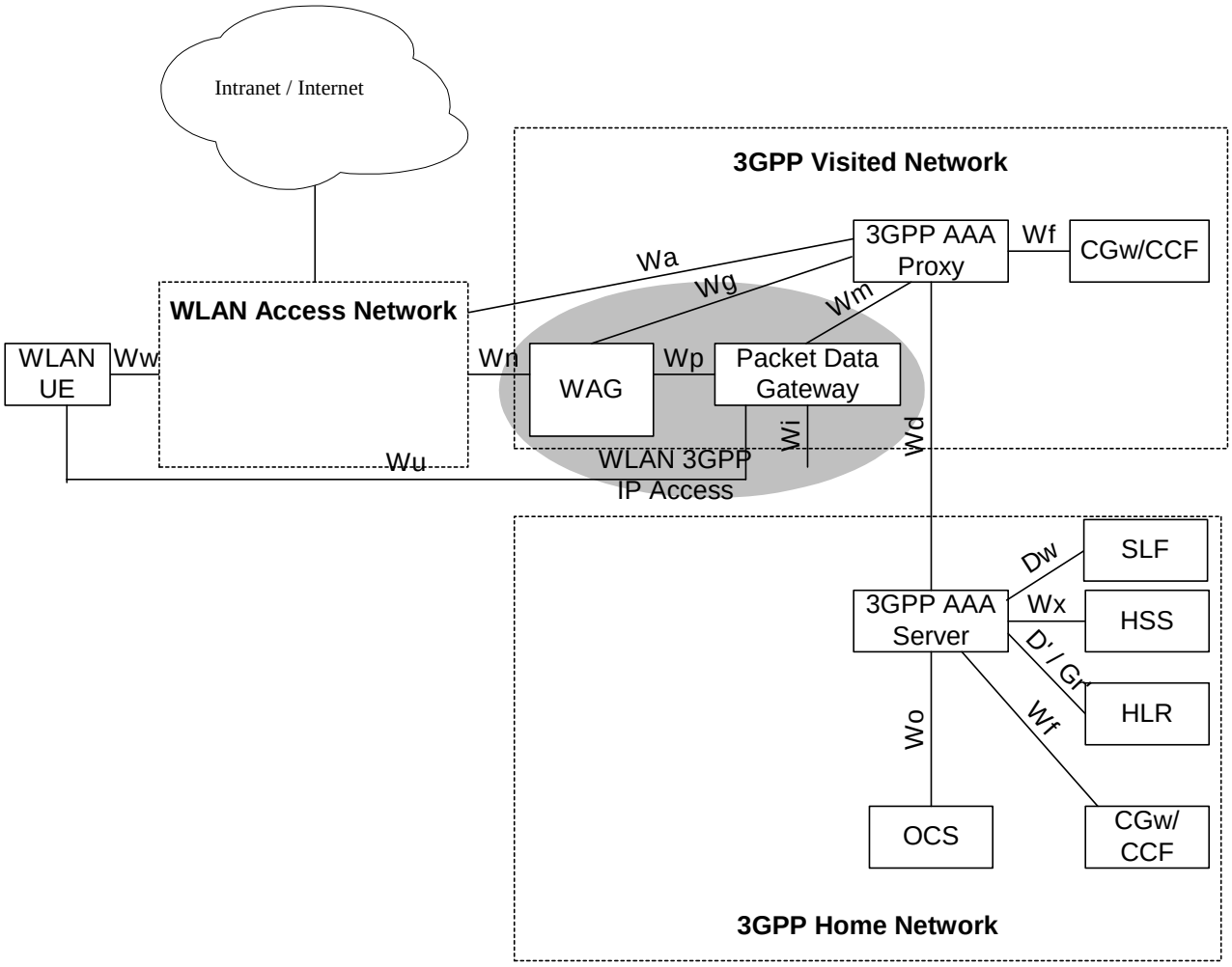


Figure 3: Roaming reference model - 3GPP PS based services provided via the 3GPP Visited Network (the shaded area refers to WLAN 3GPP IP Access functionality)

4.1.4 Network elements

The list below describes the access control related functionality in the network elements of the 3GPP-WLAN interworking Reference Model:

- The **WLAN-UE**, equipped with a UICC (or SIM card), for accessing the WLAN interworking service):
  - May be capable of WLAN access only;
  - May be capable of both WLAN and 3GPP System access;
  - May be capable of simultaneous access to both WLAN and 3GPP systems;

NOTE: Definition of simultaneous access is specified in TS 23.234 [13].

  - May be a laptop computer or PDA with a WLAN card, UICC (or SIM card) card reader, and suitable software applications;

- May be functionally split over several physical devices, that communicate over local interfaces e.g. Bluetooth, Infrared or serial cable interface;

- The **AAA proxy** represents a logical proxying functionality that may reside in any network between the WLAN and the 3GPP AAA Server. These AAA proxies are able to relay the AAA information between WLAN and the 3GPP AAA Server.
  The number of intermediate AAA proxies is not restricted by 3GPP specifications. The AAA proxy functionality can reside in a separate physical network node; it may reside in the 3GPP AAA server or any other physical network node;

- The **3GPP AAA server** is located within the 3GPP network. The 3GPP AAA server:

  - Retrieves authentication information from the HLR/HSS of the 3GPP subscriber's home 3GPP network;

  - Authenticates the 3GPP subscriber based on the authentication information retrieved from HLR/HSS. The authentication signalling may pass through AAA proxies;

  - Communicates authorisation information to the WLAN potentially via AAA proxies.

- The **Packet Data Gateway (PDG)** enforces tunnel authorization and establishment with the information received from the 3GPP AAA via the Wm interface.

NOTE: The **WLAN Access Gateway (WAG)** responsibilities for security issues are related to tunnel establishment but this decision is pending to be taken.

4.1.5 Reference points description

Wa

The reference point Wa connects the WLAN Access Network to the 3GPP Network (i.e. the 3GPP AAA Proxy in the roaming case and the 3GPP AAA server in the non-roaming case). The main purpose of the protocols implementing this interfaces is to transport authentication and keying information (WLAN UE - 3GPP network), and authorization information (WLAN AN – 3GPP network). The reference point has to accommodate also legacy WLAN Access Networks and thus should be Diameter [23], [24] or RADIUS [15], [26] based.

Wx

This reference point is located between 3GPP AAA Server and HSS. The main purpose of the protocols implementing this interface is communication between WLAN AAA infrastructure and HSS, and more specifically the retrieval of authentication vectors, e.g. for USIM authentication, and retrieval of WLAN access-related subscriber information from HSS. The protocol is either MAP or Diameter based.

D'/Gr'

This optional reference point is located between 3GPP AAA Server and pre-R6 HLR/HSS. The main purpose of the protocol implementing this interface is communication between WLAN AAA infrastructure and HLR, and more specifically the retrieval of authentication vectors, e.g. for USIM authentication, from HLR. The protocol is MAP-based.

Wn

This reference point is located between the WLAN Access Network and the WAG. This interface is to force traffic on a WLAN UE initiated tunnel to travel via the WAG. The specific method to implement this interface is subject to local agreement between the WLAN AN and the PLMN and is out of the scope of this Release of 3GPP specifications.

Wm

This reference point is located between 3GPP AAA Server and Packet Data Gateway. The functionality of this reference point is to retrieve tunnelling attributes and UE's IP configuration parameters from/via Packet Data Gateway.

Wd

The reference point Wd connects the 3GPP AAA Proxy to the 3GPP AAA Server. This interface is similar to Wa, its main purpose is to transport authentication, authorization and related information in a secure manner.

Wu

The reference point Wu is located between the WLAN UE and the Packet Data Gateway. It represents the WLAN UE-initiated tunnel between the WLAN UE and the Packet Data Gateway. On Wu interface WLAN UE and Packet Data Gateway run IKEv2 protocol to establish IPsec tunnel and protect user data packets transmitted.

4.2 Security Requirements

4.2.1 General

- The authentication scheme shall be based on a challenge response protocol.
- All long-term security credentials used for subscriber and network authentication shall be stored on UICC or SIM card.
- Long-term security credentials, which are stored on the UICC or SIM card, shall not leave the UICC or SIM card.
    - Mutual Authentication shall be supported.
    - EAP SIM and EAP AKA (both methods described in this TS) shall be supported by the AAA server and the WLAN UE

4.2.2 Signalling and user data protection

- The subscriber should have at least the same security level for WLAN access as for his current cellular access subscription.
- 3GPP systems should support authentication methods that support protected success/failure indications.
- The selected WLAN (re-) authentication mechanisms for 3GPP interworking shall provide at least the same level of security as [33.102] for USIM based access.
- The selected WLAN (re-authentication mechanism for 3GPP interworking shall provide at least the same level of security as [43.020] for SIM based access.
- Selected WLAN Authentication mechanisms for 3GPP interworking shall support agreement of session keying material.
- 3GPP systems should provide the required keying material with sufficient length and the acceptable levels of entropy as required by the WLAN subsystem.
- Selected WLAN key agreement and key distribution mechanism shall be secure against man in the middle attacks.
- Protection should be provided for WLAN authentication data and keying material on the Wa, Wd and Wx interfaces.
- The WLAN technology specific connection between the WLAN-UE and WLAN AN shall be able to utilise the generated session keying material for protecting the integrity of an authenticated connection.

4.2.3 User identity privacy

- Any secret keys used in 3G AAA servers for the generation of temporary identities should be infeasible for an attacker to recover.
- It shall be infeasible for an attacker to recover the corresponding permanent identity, given any temporary identity(s).
- It should be infeasible for an attacker to determine whether or not two temporary identities correspond to the same permanent identity.
- It shall be infeasible for an attacker to generate a valid temporary identity.

4.2.4 WLAN-UE Functional Split

4.2.4.1 General

In the case when the WLAN-UE, equipped with a UICC (or SIM card), for accessing the WLAN interworking service, is functionally split over several physical devices one device holding the card, and one device providing the WLAN access, that communicate over local interfaces e.g. Bluetooth, IR or serial cable interface, then is shall be:

- Possible to re-use existing UICC and GSM SIM cards; and
- The UE functional split shall be such that attacking the CS or PS domain of GSM or UMTS by compromising the device providing the WLAN access is at least as difficult as attacking the CS or PS domain by compromising the card holding device.

4.2.4.2 Generic security requirements on local interface

The security functionality required on the terminal side for WLAN-3G interworking may be split over several physical devices that communicate over local interfaces. The UICC or the SIM card may reside in a 3GPP UE (acting as a (U)SIM "server") and be accessed by a WLAN-UE through Bluetooth, Infrared or a USB (Universal Serial Bus) cable or some other similar wired or wireless interconnect technology (acting as the (U)SIM "client"). This would facilitate the user to get simultaneous WLAN and 3GPP access with the same (U)SIM. If this is the case, then the following requirements shall be satisfied:

1. Any local interface shall be protected against eavesdropping, attacks on security-relevant information. This protection may be provided by physical or cryptographic means. For cryptographic means, the encryption key length shall be at least 128 bits.
2. The endpoints of a local interface should be authenticated and authorised. The authorisation may be implicit in the security set-up. Keys used for local interface transport security shall not be shared across local interface links. Each local interface shall use unique keys.
3. The involved devices shall be protected against eavesdropping, undetected modification attacks on security-relevant information. This protection may be provided by physical or cryptographic means.
4. The device without (U)SIM shall not be allowed to change the status of the device with (U)SIM, i.e. to reset it, or to switch its power on or off.
5. The (U)SIM holding device shall allow the user to shut off sharing of (U)SIM feature.
6. .Whenever someone tries to remotely access a (U)SIM some sort of alert shall be sent, e.g. a message shall be displayed informing the user of the attempted access and guiding him to choose "Allow", or "Disallow". The user can then decide whether the access is authorized or not and can opt for allow or disallow the access.
7. Leakage of (U)SIM information (authentication data, session keys) to the user, or any third party over the UE Split local wireless interface (e.g. Bluetooth/WLAN) or wireline interface (USB etc.) is the major security threat. This leakage of information shall be guarded against. (Integrity and privacy of signalling between the WLAN system, the 3GPP core network, and the WLAN-UE is covered under Wa, Wd and Wx interfaces).
8. The UICC holding device shall be responsible for scheduling all (possibly concurrent) accesses to the UICC by itself, and by one additional device connected via the local interface.

9. (U)SIM Security Reuse shall be consistent with current security arrangements and ensure that user security is not compromised.

10. Applications/Data information could be retrieved from (U)SIM, provided that the UICC (or SIM card) is inserted in a 3GPP ME. When the (U)SIM is re-used over local interfaces, further access control on the Applications/Data information shall be applied by the 3GPP ME holding the (U)SIM.

4.2.4.3 Communication over local interface via a Bluetooth link

For SIM access via a Bluetooth link, the SIM Access Profile developed in BLUETOOTH SIG forum may be used. See [22].

4.2.5 Link layer security requirements

Most WLAN technologies provide (optional) link-layer protection of user data. Since the wireless link is likely to be the most vulnerable in the entire system, 3GPP-WLAN interworking should take advantage of the link layer security provided by WLAN technologies. The native link-layer protection can also prevent against certain IP-layer attacks.

Areas in which relevant requirements are defined are:

- Confidentiality and integrity protection of user data;
- Protection of signalling;
- Key distribution, key freshness validation and key ageing.

These requirements are out of scope of 3GPP. IEEE has defined the security requirements and features for the link layer in WLAN access networks, see IEEE 802.11i [6]. Other WLAN access technologies are not excluded to be used although not described here.

4.2.5.1 Void

4.2.5.2 Void

4.2.5.3 Void

4.2.6 UE-initiated tunnelling

The security features that are expected in a tunnel from the UE to the VPLMN or HPLMN will be:

- Data origin authentication and integrity must be supported.
- Confidentiality must be supported.
- The 3GPP network has the ultimate decision to allow tunnel establishment, based on:
  - The level of trust in the WLAN AN and/or VPLMN
  - The capabilities supported in the WLAN UE
  - Whether the user is authorized or not to access the services (in the VPLMN or HPLMN) the tunnel will give access to.
- The 3GPP network, in the setup process, decides the characteristics (encryption algorithms, protocols) under which the tunnel will be established.

NOTE: Authorization for the tunnel establishment is decided by the 3GPP AAA and enforced by the PDG or WAG. Whether this authorization information is protected or not is FFS.

Working assumptions:

1. The security mechanisms used in context with the IP tunnel in WLAN 3GPP IP Access are to be independent of the link layer security in WLAN Direct IP Access.

4.2.7 Requirements on IP based Access Networks other than WLAN

Section 1 of this specification states that it is also valid for IP based Access Networks other than WLAN that support the same security capabilities towards the interworking system as WLAN does. IP based Access Networks to which this specification is applicable shall satisfy at least the following requirements:

Security for Direct IP access:

- the EAP framework as defined in [3] shall be supported;
- the EAP authenticator in the access network and the EAP peer (i.e. the UE) shall establish link layer security, based on keys derived from an EAP protocol run.

Other security functions may also be required of the access network in order for this specification to be applicable. These need to be determined for each type of access network separately.

Security for 3GPP IP access:

No security requirements specific to the access network need to be satisfied.

Note : Requirements on whether a network operator should use these mechanisms for a particular access network is out of the scope of this TS. This applies also to the case of WLAN access network.

5 Security features

5.1 Authentication of the subscriber and the network and Security Association Management

5.1.1 End to End WLAN Access Authentication (WLAN Direct IP Access)

WLAN access authentication signalling is executed between WLAN-UE and 3GPP AAA Server. This authentication signalling shall be independent on the WLAN technology utilised within WLAN Access network. WLAN authentication signalling for 3GPP-WLAN interworking shall be based on Extensible Authentication Protocol (EAP) as specified in RFC 2284 (ref. [3]).

5.1.2 Transport of authentication WLAN Access signalling over the WLAN Radio interface

WLAN authentication signalling is carried between WLAN-UE and WLAN Access Network by WLAN Access Technology specific protocols. These WLAN technology specific protocols shall be able to meet the security requirements set for WLAN Access control in 3GPP-WLAN interworking. To ensure multi-vendor interoperability these WLAN technology specific protocols shall conform to existing standards of the specific WLAN access technology. For IEEE 802.11 type of WLAN radio interfaces the WLAN radio interface shall conform to IEEE 802.11i standard (ref. [6]).

5.1.3 Transport of WLAN Access authentication signalling between the WLAN access network and the 3GPP AAA proxy server

WLAN Authentication signalling shall be transported over the Wa reference point by standard mechanisms, which are independent on the specific WLAN technology utilised within the WLAN Access network. The transport of Authentication signalling over Wa reference point shall be based on standard Diameter [23], [24] or RADIUS [15], [26] protocols.

When the Wa reference point is based on Diameter, it shall be protected with IPsec if there is no physical protection between the WLAN Access network and the 3GPP AAA proxy/server (the support of IPsec for Diameter is mandatory as stated in RFC 3588 [24]).

NOTE: In case of RADIUS based Wa reference point, protection is achieved by means of RADIUS standard procedures. In particular, the attribute MS-MPPE-Recv-Key (see RFC 2548 [36]) provides protection of the keying material derived in the 3GPP AAA server and sent to the WLAN Access network.

5.1.4 Transport of authentication signalling between the 3GPP AAA proxy server and the 3GPP AAA server

WLAN Authentication signalling shall be transported over the Wd reference point by standard mechanisms.

5.1.5 Transport of WLAN Access authentication signalling between the 3GPP AAA server and the HSS

WLAN Authentication signalling shall be transported over the Wx reference point by standard mechanisms.

5.1.6 User Identity Privacy in WLAN Access

User identity privacy (Anonymity) is used to avoid sending any cleartext permanent subscriber identification information which would compromise the subscriber's identity and location on the radio interface, or allow different communications of the same subscriber on the radio interface to be linked.

User identity privacy is based on temporary identities (pseudonyms or re-authentication identities). The procedures for distributing, using and updating temporary identities are described in ref. [4] and [5]. Support of this feature is mandatory for implementation in the network and WLAN UE. The use of this feature is optional in the network, but mandatory in the WLAN UE.

The AAA server generates and delivers the temporary identity and/or the re-authentication identity to the WLAN-UE as part of the authentication process. The WLAN-UE shall not interpret the temporary identity; it shall just store the received identifier and use it at the next authentication. Clause 6.4 describes a mechanism that allows the home network to include the user's identity (IMSI) encrypted within the temporary identity.

When the WLAN-UE receives one temporary identity issued by the AAA server, it shall use it in the next authentication. The WLAN-UE can only use the permanent identity when there is no temporary identity available in the WLAN-UE. A temporary identity is available for use when it has been received in last authentication process. Temporary identities received in earlier authentication processes have to be cleared in the WLAN-UE or marked as "deleted" after the completion of the ongoing EAP procedure (whether success or failure) so that they can only be used for one EAP procedure. If during the ongoing EAP procedure an EAP-REQUEST/AKA-identity or EAP-REQUEST/SIM-start is received by the WLAN UE, the same identity that has been used in the EAP/Response/Identity message shall be used as specified in the clauses 6.1.1.1 and clause 6.1.2.1. If the WLAN-UE does not receive any new temporary identity during a re-authentication procedure, the WLAN-UE shall use a previously unused pseudonym, if available, for the next full re-authentication attempt.

If the WLAN-UE receives from the AAA server more than one temporary identity (a pseudonym and a re-authentication identity), in the next authentication procedure, it will use the re-authentication identity, so that the AAA server is able to decide either to go on with a fast re-authentication or to fallback to a full re-authentication (by requesting the pseudonym to the WLAN-UE). This capability of decision by the AAA server is not possible if the WLAN-UE sends the pseudonym, since the AAA server is not able to request the re-authentication identity if it decides to change to fast re-authentication.

For tunnel establishment in WLAN 3GPP IP Access, fast re-authentication may be used for speed up the procedure. In this case, the WLAN-UE shall use the fast re-authentication identities (as long as the re-authentication identity has been received in the last authentication process).

If identity privacy support is not activated by the home network, the communication of the user identity (IMSI) in WLAN 3GPP IP access is more secure than in WLAN direct IP access. In WLAN 3GPP IP access, the authentication exchange is performed in a protected tunnel which provides encryption and integrity protection, as well as replay protection. Nevertheless, if identity privacy support is used by the home network and the WLAN UE received a temporary identity in a previous authentication, it shall use it in the tunnel authentication process.

NOTE: There exist the following risks when sending the IMSI in the tunnel set-up procedure:

- the protected tunnel is encrypted but not authenticated at the moment of receiving the user identity (IMSI). The IKEv2 messages, when using EAP, are authenticated at the end of the EAP exchange. So in case of a man-in-the-middle attack the attacker could be able to see the IMSI in clear text, although the attack would eventually fail at the moment of the authentication;
- the IMSI would be visible for the PDG, which in roaming situations may be in the VPLMN. This is not a significant problem if the home network operator trusts the PDGs owned by the visited network operators.

To avoid user traceability, the user should not be identified for a long period by means of the same temporary identity. On the other hand, the AAA server should be ready to accept at least two different temporary identities, in case the WLAN-UE fails to receive the new one issued from the AAA server. The mechanism described in Clause 6.4 also includes facilities to maintain more than one allowed temporary identities.

If identity privacy is used but the AAA server fails to identify the user by its temporary identity, the AAA server shall request the next one following the order 1.Fast re-authentication id., 2.Pseudonym, 3.Permanent id. For example, if the WLAN UE is using the previously issued re-authentication identity but the AAA server cannot identify the user by its re-authentication identity, the AAA server shall request the WLAN UE to send its pseudonym. If the AAA server still does not recognize the pseudonym, it shall request the WLAN UE to send its permanent identity. This represents a breach in the provision of user identity privacy. It is a matter of the operator's security policy whether to allow clients to accept requests from the network to send the cleartext permanent identity. If the client rejects a legitimate request from the AAA server, it shall be denied access to the service.

5.1.7 Re-authentication in WLAN Access

A re-authentication maybe full or fast. Full re-authentication means that a new full authentication procedure shall take place as the initial authentication procedure where new keys are generated in the (U)SIM card and in the network. A fast re-authentication implies a new authentication in which some keys are not generated in (U)SIM and in the network, but reused from the previous authentication process.

NOTE 1: The use of fast re-authentication implies the advantage of saving processing time in the WLAN UE and the AAA server and saving power consumption, mainly in the WLAN UE. However, it has the disadvantage that the continuous re-use of keys maybe risky if the user is accessing a low trusted WLAN AN. In this case the keys should be refreshed and hence full re-authentication should be used. The use of fast re-authentication should be left for situations in which the user is accessing a high trusted WLAN AN.

WLAN 802.1x/AAA re-authentication is performed between WLAN-UE and AAA server, through Wd and Wa interfaces.

NOTE 2: The WLAN-AN may initiate the 802.1x/AAA re-authentication process periodically. The frequency of the 802.1x/AAA re-authentications is determined by a timer which normally is set by O&M procedures in the WLAN-AN but it may be sent to the WLAN-AN by the AAA server in a RADIUS or Diameter message (in the attribute RADIUS Session Timeout or Diameter AVP Authorization-Lifetime).

The WLAN UE may initiate the 802.1x/AAA re-authentication process for example upon moving to a new access point. The WLAN UE may also initiate the 802.1x/AAA re-authentication periodically; however it is out of the scope how the WLAN UE determines the frequency of periodic 802.1x/AAA re-authentications.

The 3GPP AAA server may initiate the 802.1x/AAA re-authentication process upon some event (for example the amount of data reported in accounting messages exceeds some limit), or periodically, alternatively to the usage of the Session Timeout/Authorization-Lifetime. The frequency of periodic 802.1x/AAA re-authentications is determined by a timer, which is normally set by O&M procedures in the 3GPP AAA server.

NOTE 3: If several elements (UE, WLAN AN, 3GPP AAA server) maintain timers for periodic 802.1x/AAA re-authentications, then the element that has the shortest timer shall determine the frequency of periodic 802.1x/AAA re-authentications, because each element is able to initiate an 802.1x/AAA re-authentication.

At reception of the Session Timeout attribute, or the Authorization-Lifetime AVP, the WLAN-AN may substitute the previously set counter by the received one. Nevertheless, the 3GPP network does not have the certainty that the counter sent by the AAA server is enforced by the WLAN AN, since the latter may not support this feature (the reception and acceptance of this attribute or AVP). In this case, the WLAN AN shall discard it and trigger the re-authentications in the period set by O&M procedures as mentioned before.

The 802.1x/AAA re-authentication process shall be performed either with an EAP SIM/AKA full authentication process or with an EAP SIM/AKA fast re-authentication process. Both processes are described in this TS.

The EAP SIM/AKA re-authentication process shall be implemented together with the full authentication procedure in the network and the WLAN UE, although use of EAP/SIM/AKA for fast re-authentication is optional in the network and depends on operator's policies. The decision of using the fast re-authentication process is taken by the home network (i.e. the AAA server) and indicated to the WLAN UE by means of sending the re-authentication identity to the WLAN UE in any authentication process. When a re-authentication process is initiated by the network, the WLAN UE shall reply with the re-authentication identity if it is available (it was received in the previous successful authentication), and it shall be the home network (AAA server), when receiving this re-authentication identity the ultimate point of decision of whether to continue with a fast re-authentication or to defer to a full re-authentication. This decision of using fast re-authentication depends on operator's policies.

NOTE 4: These policies depend on the level of trust of the 3GPP operator and the WLAN AN, and the possible threats detected by an operator, which may require a periodic refresh of keys. The full process description can be found in ref. [4] and [5].

Since HSS will maintain the registration status of the user in WLAN, any change to that status shall be communicated to HSS. When a re-authentication (full or fast) process fails, for any reason, the AAA server shall inform HSS about the event. The reason for this mechanism is that the home network may use re-authentication not only to authenticate the user periodically but also as a heartbeat mechanism (to track user's activity). The HSS will mark the user as registered when he/she first authenticates in WLAN. If for example the user removes the (U)SIM card, the next re-authentication will fail, and the HSS shall be informed.

5.1.8 Security Association Management for UE-initiated tunnels (WLAN 3GPP IP Access)

The tunnel endpoints, the UE and the PDG, are mutually authenticated when setting up the tunnel.

The tunnel set-up procedure results in security associations, which are used to provide confidentiality and integrity protection, as required according to sections 5.2 and 5.3, for data transmitted through the tunnel.

5.2 Confidentiality protection

5.2.1 Confidentiality protection in WLAN Direct IP Access

Confidentiality protection in the WLAN AN link layer is required. The specification of this feature is, however, out of scope of 3GPP. When the WLAN link layer is according to IEEE 802.11 then the confidentiality protection shall be as specified in ref. [6].

The home network (AAA server) has to be able to send key material to the WLAN AN, as input for the encryption procedure, in a confidential and integrity protected way (for detailed requirements cf. [27]).

5.2.2 Confidentiality protection in WLAN 3GPP IP Access

It shall be possible to protect the confidentiality of IP packets sent through a tunnel between the UE and the PDG.

5.3 Integrity protection

5.3.1 Integrity protection in WLAN Direct IP Access

Integrity protection in the WLAN AN link layer is required. The specification of this feature is, however, out of scope of 3GPP. When the WLAN link layer is according to IEEE 802.11 then the integrity protection shall be as specified in ref. [6].

The home network (AAA server) has to be able to send key material to the WLAN AN, as input for the integrity protection mechanism, in a confidential and integrity protected way (for detailed requirements cf. [27]).

5.3.2 Integrity protection in WLAN 3GPP IP Access

The integrity of IP packets sent through a tunnel between the UE and the PDG shall be protected.

5.4 Void

5.5 Immediate Service Termination

The AAA server initiates immediate service termination when some events may require stopping user's activity (end of subscription, expiration of charging account, etc.). This process can be initiated at any time by the AAA server with the Diameter command Diameter-Abort-Session-Request and Diameter-Abort-Session-Answer (the Wd interface is implemented with Diameter protocol) as specified in [24]. The AAA proxy shall just forward this procedure to the WLAN AN through Wa interface if the latter supports Diameter. If it supports appropriate RADIUS extensions, the AAA proxy shall map the procedure to the RADIUS messages Disconnect-Request and Disconnect-Response as specified in [25].

5.6 WLAN UE functionality split

The WLAN UE may consist of several devices. When there is more than one, it will be typically a WLAN Terminal Equipment (e.g. a laptop) and a Mobile Terminal (e.g. a mobile phone) equipped with a UICC or SIM card.

The WLAN TE provides WLAN access, while the MT or UICC implements the authentication as the EAP termination, which includes key derivation and identity handling. The termination point of EAP shall always be the MT or UICC. When any authentication process is finished (in the MT or UICC), the resulting keys can be retrieved by the WLAN TE in order to be used for link layer security in the WLAN access.

5.7 Simultaneous access control

The home network operator needs to be aware of how the user is accessing the WLAN network. If the user is making the SIM or UICC card available for several devices that have WLAN access capabilities, the home network operator may decide, at any time, to allow or bar t he access of two or more network devices simultaneously.

WLAN direct IP access

The control of simultaneous sessions in WLAN direct IP access can be performed, under some circumstances, using the MAC address of the user''s device. After a number of successful authentications, if a subsequent authentication attempt is being performed by another device, the MAC address will be different and the AAA server will be able to detect it. However, this mechanism has some limitations. One of them is that if the two devices are accessing two different WLAN access points (assuming that a WLAN access point has a independent control of MAC address space), the MAC address of one of them can be spoofed and made equal to the other one. This is a fraud situation the home network should avoid. However, it may happen that the user is accessing other WLAN access point and a pre-authentication is performed in this new access point. In this case there is no fraud attempt. Then, in this situation (same MAC addresses, different WLAN radio networks) the AAA server will not be able to distinguish between a legal and a fraud situation and shall not reject the authentication process.

WLAN 3GPP IP access

The control of simultaneous sessions in WLAN 3GPP IP access has to be performed in a different way than in WLAN direct IP access as in this case the MAC addresses cannot be trusted by the home network and may not be available.

The user gets connected to the 3GPP network using the W-APNs. When a W-APN is activated by the user, an IKEv2 exchange will be initiated and, if successful, an IKE SA and an IPsec SA will be established.

The IKEv2 procedure is authenticated using EAP SIM or EAP AKA, so the AAA server has to be contacted in order to perform this authentication. Then the AAA server will be aware of the fact that a new W-APN is going to be activated.

The mechanism to control simultaneous sessions is to limit the number of W-APNs to be activated by the user and control the number of IKEv2 security associations per W-APN. The home operator shall configure, by subscription, the Maximum Number of IKE SAs per W-APN. With this mechanism, it is ensured that only as many devices as defined by the Maximum Number make use of the same subscription to access the 3GPP network, because each device will have to activate a W-APN (and use a different IKE SA and IPsec SA).

According to the IKEv2 protocol, one IKE SA allows to establish multiple IPsec SAs. Operators shall be able to configure the maximum value for the number of IPsec SAs per IKE SA at PDG. To avoid session interruptions when the first IPsec SA reaches the end of its lifetime, re-keying is needed. Implementations shall correctly handle this re-keying, even though this may temporarily raise the number of IPsec SAs to 2 if there is only one IPsec SA per IKE SA.

6 Security mechanisms

6.1 Authentication and key agreement

The WLAN UE and AAA server shall support both EAP AKA and EAP SIM methods. A WLAN UE with either a USIM or a SIM inserted shall request the authentication method corresponding to the type of smart card it holds (i.e. the user's subscription type). The procedure to select the method is:

1) The WLAN UE shall send an identity (whatever it is: permanent, pseudonym, etc.) to the AAA server. In the first authentication, the identity shall be an IMSI and the message containing the identity shall also contain an indication of the authentication method to be used. In subsequent authentications, the identity shall be a temporary identity for which the AAA server has already an indication of the associated authentication method. The associated authentication method indication shall not be modified by the WLAN UE.

2) If the AAA server recognizes the EAP method but not the user identity (for example an obsolete pseudonym), it shall request a new identity using the EAP method indicated by the WLAN UE.

3) If the AAA server recognizes the user identity (and hence the EAP method), it shall fetch AVs from HSS. If they don't match the EAP method received (e.g. the EAP method received is EAP AKA and triplets are received from HSS), the user's subscription shall prevail (in the previous example EAP SIM shall be used).

4) If the user identity is not recognized, the AAA server shall decide which method to use (there may exist a default method ONLY in this situation). If this default method does not match user's subscription (e.g. EAP AKA for a SIM user), the WLAN UE shall respond a NACK to the AAA server and then the AAA shall try with the other EAP method until a recognised identity is received.

The authentication and key agreement shall be dedicated for WLAN access only, thus the keys provided by the SIM (Kc) or USIM (CK, IK) during authentication and key agreement shall be stored in the ME's volatile memory.

6.1.1 USIM-based WLAN Access Authentication

USIM based authentication is a proven solution that satisfies the authentication requirements from clause 4.2. This form of authentication shall be based on EAP-AKA (ref. [4]), as described in clause 6.1.1.1. For the case of WLAN-UE Functional Split, see clause 4.2.4.

6.1.1.1 EAP/AKA Procedure

The EAP-AKA authentication mechanism is specified in ref. [4]. The present section describes how this mechanism is used in the WLAN-3GPP interworking scenario.

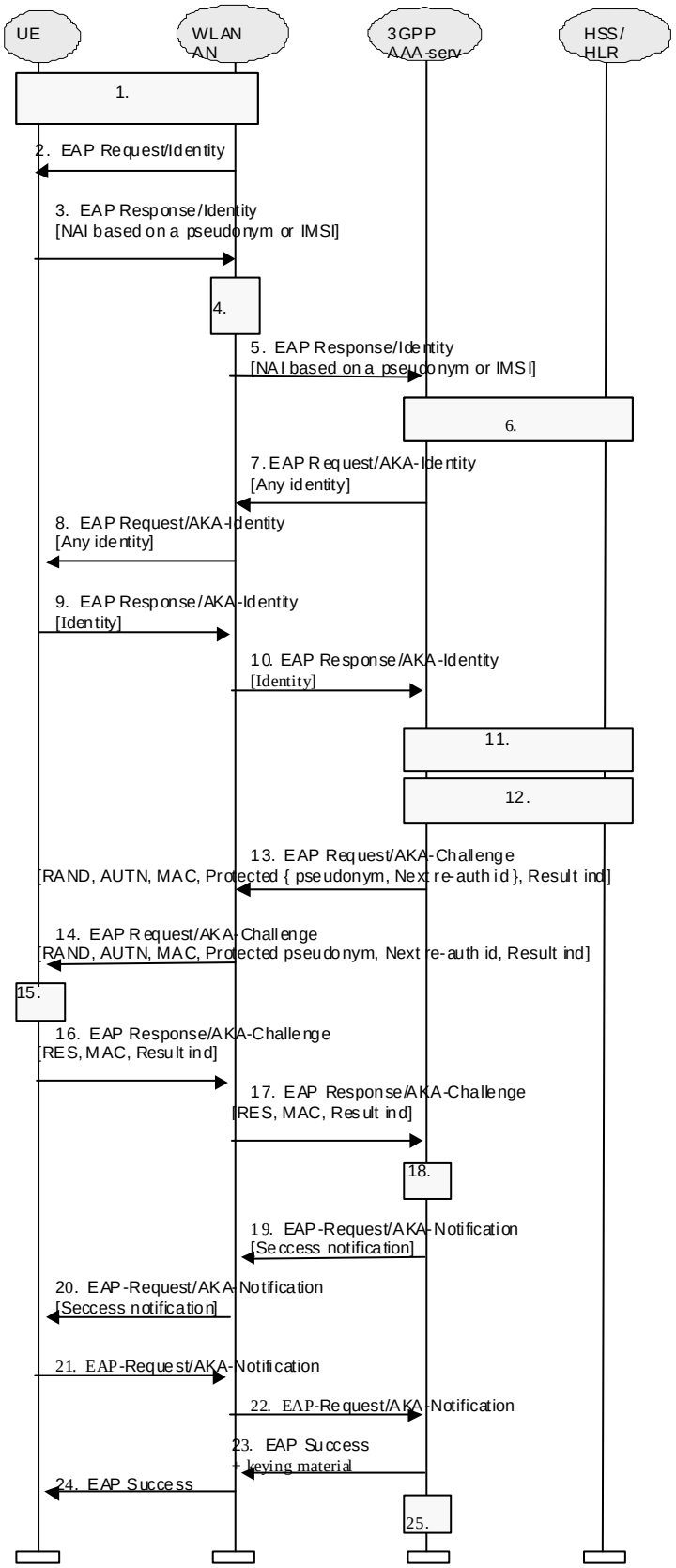


Figure 4: Authentication based on EAP AKA scheme

1. A connection is established between the WLAN UE and the WLAN AN, using a Wireless LAN technology specific procedure (out of scope for this specification).

2. The WLAN AN sends an EAP Request/Identity to the WLAN UE.

   EAP packets are transported over the Wireless LAN interface encapsulated within a Wireless LAN technology specific protocol.

3. The WLAN UE sends an EAP Response/Identity message. The WLAN UE sends its identity complying with Network Access Identifier (NAI) format specified in 3GPP TS 23.003 [18]. NAI contains either a pseudonym allocated to the WLAN UE in previous authentication or, in the case of first authentication, the IMSI.

NOTE 1: Generating an identity conforming to NAI format from IMSI is defined in 3GPP TS 23.003 [18].

4. The message is routed towards the proper 3GPP AAA Server based on the realm part of the NAI. The routing path may include one or several AAA proxies (not shown in the figure).

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

5. The 3GPP AAA Server receives the EAP Response/Identity packet that contains the subscriber identity. The identifier of the WLAN radio network, VPLMN Identity and the MAC address of the WLAN UE shall also be received by the 3GPP AAA Server in the same message.

6. 3GPP AAA Server identifies the subscriber as a candidate for authentication with EAP-AKA, based on the received identity. The 3GPP AAA Server then checks that it has an unused authentication vector available for that subscriber. If not, a set of new authentication vectors is retrieved from HSS/HLR. A mapping from the temporary identifier to the IMSI may be required. In addition, 3GPP AAA Server shall retrieve authentication vectors from HLR/HSS when it detects that the VPLMN selected by a user has changed. This can happen, for example, when a user is performing a VPLMN re-selection procedure and is initiating a new authentication procedure via a new VPLMN.

   The HSS/HLR shall check if there is a 3GPP AAA Server already registered to serve for this subscriber In case the HSS/HLR 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 AAA proxy or the WLAN AN, or the current 3GPP AAA Server acts as a AAA proxy and forwards the authentication message to the previously registered 3GPP AAA Server.

NOTE 3: It could also be the case that the 3GPP AAA Server first obtains an unused authentication vector for the subscriber and, based on the type of authenticator vector received (i.e. if a UMTS authentication vector is received), it regards the subscriber as a candidate for authentication with EAP-AKA.

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 ref. [4]. However, this new request of the user identity can be omitted by the home operator if there exist the certainty that the user identity could not be changed or modifies by any means in the EAP Response Identity message.

8. The WLAN AN forwards the EAP Request/AKA Identity message to the WLAN UE.

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

10. The WLAN AN 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/HLR are not valid, these data shall be requested again to HSS/HLR (step 6 shall be repeated before continuing with step 11).

NOTE 4: In order to optimise performance, the identity re-request process (the latter four steps) should be performed when the 3GPP AAA Server has enough information to identify the user as an EAP-AKA user, and before user profile and authentication vectors retrieval, although protocol design in Wx interface may not allow to perform these four steps until the whole user profile has been downloaded to the 3GPP AAA Server.

11. 3GPP AAA Server checks that it has the WLAN 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 WLAN service.

    Although this step is presented after step 6 in this example, it could be performed at some other point, however before step 14. (This will be specified as part of the Wx interface.)

12. New keying material is derived from IK and CK., cf. [4]. This keying material is required by EAP-AKA, and some extra keying material may also be generated for WLAN technology specific confidentiality and/or integrity protection.

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

13. 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 WLAN AN in EAP Request/AKA-Challenge message. 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 WLAN UE, 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 WLAN AN sends the EAP Request/AKA-Challenge message to the WLAN UE.

15. The WLAN UE runs UMTS algorithm on the USIM. The USIM 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. [4]. If AUTN is correct, the USIM computes RES, IK and CK.

    The WLAN UE derives required additional new keying material from the new computed IK and CK from the USIM, checks the received MAC with the new derived keying material.

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

16. The WLAN UE calculates a new MAC value covering the EAP message with the new keying material. WLAN UE sends EAP Response/AKA-Challenge containing calculated RES and the new calculated MAC value to WLAN AN.

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

17. WLAN AN 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 requested previously to use protected successful result indications. This message is MAC protected.

20. The WLAN AN forwards the message to the WLAN UE.

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

22. The WLAN AN 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 WLAN AN (perhaps preceded by an EAP Notification, as explained in step 20). If some extra keying material was generated for WLAN technology specific confidentiality and/or integrity protection then the 3GPP AAA Server includes this keying material in the underlying AAA protocol message (i.e. not at the EAP level). The WLAN AN stores the keying material to be used in communication with the authenticated WLAN UE.

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

25. If there is no other ongoing WLAN Access session for the subscriber detected by the 3GPP AAA Server, and the WLAN registration for this subscriber is not performed previously, then the 3GPP AAA Server shall initiate the WLAN registration to the HSS/HLR. Otherwise, the 3GPP AAA Server shall compare the MAC address, VPLMN Identity and the WLAN access network information of the authentication exchange with the same information of the ongoing sessions. If the information is the same as with an ongoing session, then the authentication exchange is related to the ongoing session, so there is no need to do anything for old sessions. If it is the same subscriber but with a different MAC address, or with a different VPLMN identity or with different radio network information that is received than in any ongoing session, the 3GPP AAA Server then considers that the authentication exchange is related to a new WLAN Access session. It shall terminate an old WLAN Access session after the successful authentication of the new WLAN Access session, based on the policy whether simultaneous sessions are not allowed, or whether the number of allowed sessions has been exceeded. When the MAC addresses (the old one and the new one) are equal and the WLAN radio network information received is different from the old one, it is up to home operator local policies to interpret this fact as a fraud or a legal situation, and then proceed either deleting the old session or allowing both (the old and the new one)

The authentication process may fail at any moment, for example because of unsuccessful checking of MACs or no response from the WLAN UE after a network request. In that case, the EAP AKA process will be terminated as specified in ref. [4] and an indication shall be sent to HSS/HLR.

6.1.2 GSM SIM based WLAN Access authentication

SIM based authentication is useful for GSM subscribers that do not have a UICC with a USIM application. This form of authentication shall be based on EAP-SIM (ref. [5]), as described in clause 6.1.2.1. This authentication method satisfies the authentication requirements from clause 4.2, without the need for a UICC with a USIM application. For the case of WLAN-UE Functional Split, see clause 4.2.4.

6.1.2.1 EAP SIM procedure

The EAP-SIM authentication mechanism is specified in ref. [5]. The present section describes how this mechanism is used in the WLAN-3GPP interworking scenario.

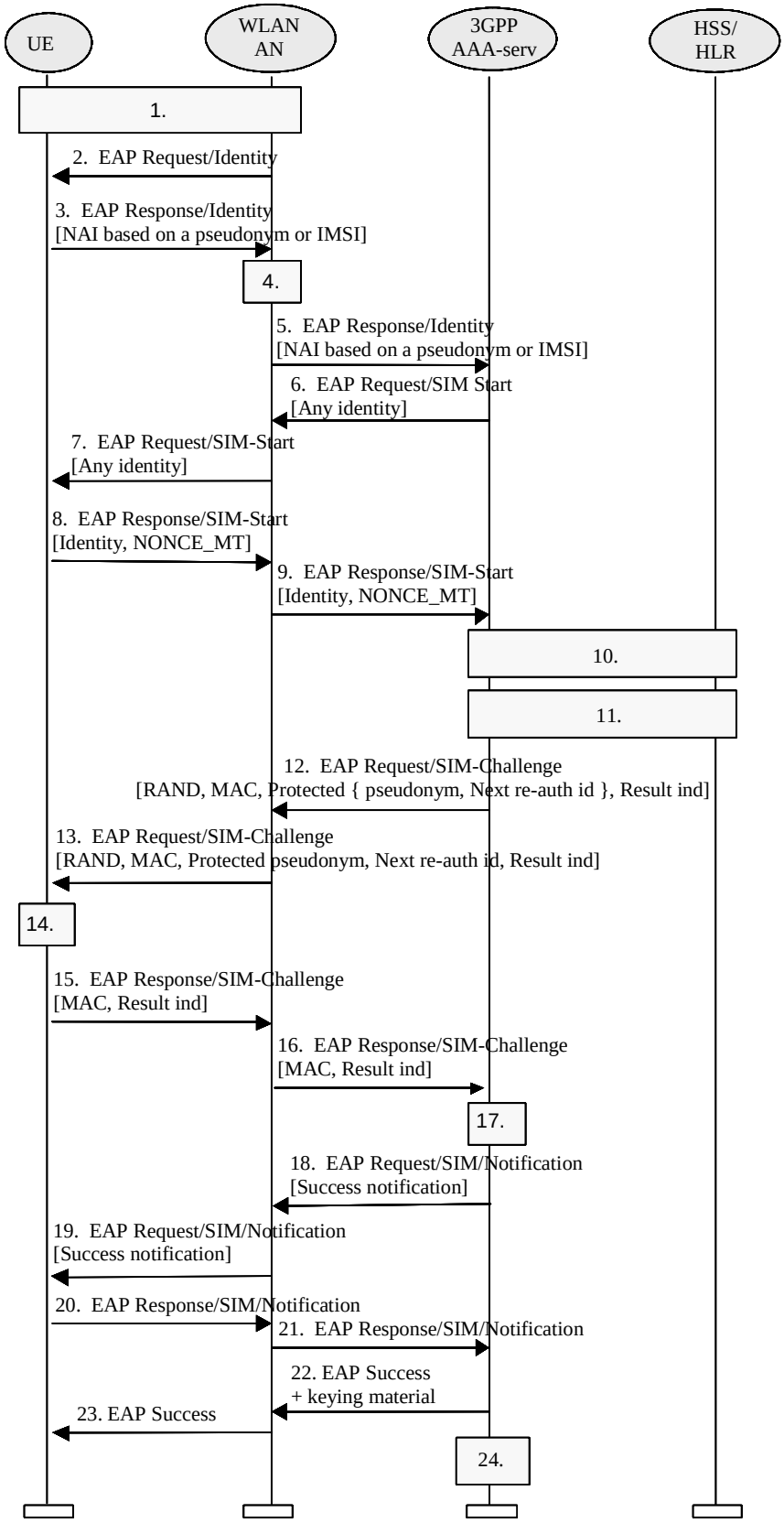


Figure 5: Authentication based on EAP SIM scheme

1. A connection is established between the WLAN UE and the WLAN AN, using a Wireless LAN technology specific procedure (out of scope for this specification).

2. The WLA AN sends an EAP Request/Identity to the WLAN UE.

   EAP packets are transported over the Wireless LAN interface encapsulated within a Wireless LAN technology specific protocol.

3. The WLAN UE sends an EAP Response/Identity message. The WLAN UE sends its identity complying with the Network Access Identifier (NAI) format specified in 3GPP TS 23.003 [18]. NAI contains either a pseudonym allocated to WLAN UE in previous authentication or, in the case of first authentication, the IMSI.

NOTE 1: Generating an identity conforming to NAI format from IMSI is defined in 3GPP TS 23.003 [18].

4. The message is routed towards the proper 3GPP AAA Server based on the realm part of the NAI. The routing path may include one or several AAA proxies (not shown in the figure).

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

5. The 3GPP AAA Server receives the EAP Response/Identity packet that contains the subscriber identity. The identifier of the WLAN radio network, VPLMN Identity and the MAC address of the WLAN UE shall also be received by the 3GPP AAA Server in the same message.

6. The 3GPP AAA Server, identifies the subscriber as a candidate for authentication with EAP-SIM, based on the received identity, and then it sends the EAP Request/SIM-Start packet to WLAN AN. The 3GPP AAA Server requests again the user identity. 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 ref. [5]. However, this new request of the user identity can be omitted by the home operator if there exist the certainty that the user identity could not be changed or modified by any means in the EAP Response Identity message.

NOTE 3: It could also be the case that the 3GPP AAA Server first obtains an authentication vector for the subscriber and, based on the type of authenticator vector received (i.e. if a GSM authentication vector is received), it regards the subscriber as a candidate for authentication with EAP-SIM.

7. WLAN AN sends the EAP Request/SIM-Start packet to WLAN UE

8. The WLAN UE chooses a fresh random number NONCE_MT. The random number is used in network authentication. The WLAN UE includes the same user identity it used in the EAP Response Identity message.

   The WLAN UE sends the EAP Response/SIM-Start packet, containing NONCE_MT and the user identity, to WLAN AN.

9. WLAN AN sends the EAP Response/SIM-Start packet to 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/SIM Start) so that any user data retrieved previously from HSS/HLR are not valid, these data shall be requested again to HSS/HLR.

10. The 3GPP AAA Server checks that it has available N unused authentication vectors for the subscriber. Several GSM authentication vectors are required in order to generate keying material with effective length equivalent to EAP-AKA. If N authentication vectors are not available, a set of authentication vectors is retrieved from HSS/HLR. A mapping from the temporary identifier to the IMSI may be required. In addition, 3GPP AAA Server shall retrieve authentication vectors from HLR/HSS when it detects that the VPLMN selected by a user has changed. This can happen, for example, when a user is performing a VPLMN re-selection procedure and is initiating a new authentication procedure via a new VPLMN.

    Although this step is presented after step 9 in this example, it could be performed at some other point, for example after step 5, however before step 12. (This will be specified as part of the Wx interface).

    The HSS/HLR shall check if there is a 3GPP AAA Server already registered to serve for this subscriber. In case the HSS/HLR 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 WLAN AN, or the current 3GPP AAA Server acts as a AAA proxy and forwards the authentication message to the previously registered 3GPP AAA Server.

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

    Although this step is presented after step 10 in this example, it could be performed at some other point, however before step 18. (This will be the specified as part of the Wx interface).

12. New keying material is derived from NONCE_MT and N Kc keys. This keying material is required by EAP-SIM, and some extra keying material may also be generated for WLAN technology specific confidentiality and/or integrity protection.

    A new pseudonym and/or a re-authentication identity may be chosen and protected (i.e. encrypted and integrity protected) using EAP-SIM generated keying material.

    A message authentication code (MAC) is calculated over the EAP message using an EAP-SIM derived key. This MAC is used as a network authentication value.

    3GPP AAA Server sends RAND, MAC, protected pseudonym and protected re-authentication identity (the two latter in case they were generated) to WLAN AN in EAP Request/SIM-Challenge message. 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 WLAN UE, 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.

13. The WLAN AN sends the EAP Request/SIM-Challenge message to the WLAN UE.

14. WLAN UE runs N times the GSM A3/A8 algorithms in the SIM, once for each received RAND.

    This computing gives N SRES and Kc values.

    The WLAN UE derives additional keying material from N Kc keys and NONCE_MT.

    The WLAN UE calculates its copy of the network authentication MAC with the newly derived keying material and checks that it is equal with the received MAC. If the MAC is incorrect, the network authentication has failed and the WLAN UE cancels the authentication (not shown in this example). The WLAN UE continues the authentication exchange only if the MAC is correct.

    The WLAN UE calculates a new MAC with the new keying material covering the EAP message concatenated to the N SRES responses.

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

15. WLAN UE sends EAP Response/SIM-Challenge containing calculated MAC to WLAN AN.

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

16. WLAN AN sends the EAP Response/SIM-Challenge packet to 3GPP AAA Server.

17. 3GPP AAA Server compares its copy of the response MAC with the received MAC.

18. Once the comparison in step 17 is successful, the 3GPP AAA Server shall send the message EAP Request/SIM/Notification, previous to the EAP Success message, if the 3GPP AAA Server requested previously to use protected success result indications. The message EAP Request/SIM/Notification is MAC protected.

19. The WLAN AN forwards the message to the WLAN UE.

20. The WLAN UE sends the EAP Response/SIM/Notification.

21. The WLAN AN forwards the EAP Response/SIM/Notification message to the 3GPP AAA Server. The 3GPP AAA Server shall ignore the contents of this message.

22. The 3GPP AAA Server sends the EAP Success message to WLAN AN (perhaps preceded by an EAP Notification, as explained in step 20). If some extra keying material was generated for WLAN technology 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 WLAN AN stores the keying material to be used in communication with the authenticated WLAN UE.

23. WLAN AN informs the WLAN UE about the successful authentication with the EAP Success message. Now the EAP SIM exchange has been successfully completed, and the WLAN UE and the WLAN AN may share keying material derived during that exchange.

24. If there is no other ongoing WLAN Access session for the subscriber detected by the 3GPP AAA Server, and the WLAN registration for this subscriber is not performed previously, then the 3GPP AAA Server shall initiate the WLAN registration to the HSS/HLR. Otherwise, the 3GPP AAA Server shall compare the MAC address, VPLMN Identity and the WLAN access network information of the authentication exchange with the same information of the ongoing sessions. If the information is the same as with an ongoing session, then the authentication exchange is related to the ongoing session, so there is no need to do anything for old sessions. If it is the same subscriber but with a different MAC address, or with a different VPLMN identity or with different radio network information that is received than in any ongoing session, the 3GPP AAA Server then considers that the authentication exchange is related to a new WLAN Access session. It shall terminate an old WLAN Access session after the successful authentication of the new WLAN Access session, based on the policy whether simultaneous sessions are not allowed, or whether the number of allowed sessions has been exceeded. When the MAC addresses (the old one and the new one) are equal and the WLAN radio network information received is different from the old one, it is up to home operator local policies to interpret this fact as a fraud or a legal situation, and then proceed either deleting the old session or allowing both (the old and the new one)

NOTE 4: The derivation of the value of N is for further study.

The authentication process may fail at any moment, for example because of unsuccessful checking of MACs or no response from the WLAN UE after a network request. In that case, the EAP SIM process will be terminated as specified in ref. [5] and an indication shall be sent to HSS/HLR.

6.1.3 EAP support in Smart Cards

6.1.3.1 EAP-AKA procedure

It shall be possible as an implementation option to have the termination of EAP in the UICC. For this purpose, all steps of the EAP-AKA authentication mechanism described in clause 6.1.1.1 apply with the exception of step 15 that shall be replaced with the following:

> The WLAN-UE runs EAP authentication method (see ETSI TS 102.310 [41]) on the UICC. The USIM verifies that AUTN is correct and hereby authenticates the network. If AUTN is incorrect, the UICC rejects the authentication (not shown in this example). If the sequence number is out of synch, UICC initiates a synchronization procedure, see reference [4]. If AUTN is correct, the UICC computes the Master Session Key and Extended Master Session Key and checks the received MAC with the new derived keying material.
>
> If a temporary identity (pseudonym and/or re-authentication identities) is received, then the UICC stores the temporary identity for the next full or fast authentications. This temporary identity shall be deleted after the next authentication procedure.

6.1.3.2 EAP-SIM procedure

It shall be possible as an implementation option to have the termination of EAP in the UICC. To handle EAP-SIM the UICC uses GSM AKA by applying conversion functions c2 and c3 (as defined in TS 33.102 [21]). For this purpose, all steps of the EAP-SIM authentication mechanism described in clause 6.1.2.1 apply with the exception of step 14 that shall be replaced with the following:

> The WLAN-UE runs EAP authentication method (see ETSI TS 102.310 [41]) on the UICC. The WLAN-UE continues the authentication exchange only if the MAC is correct.

If a temporary identity (pseudonym and/or re-authentication identities) is received, then the UICC stores the temporary identity for the next full or fast authentications. This temporary identity shall be deleted after the next authentication procedure.

6.1.4 Fast re-authentication mechanisms in WLAN Access

When authentication processes have to be performed frequently, it can lead to a high network load especially when the number of connected users is high. Then it is more efficient to perform fast re-authentications. Thus the re-authentication process allows the WLAN-AN to authenticate a certain user in a lighter process than a full authentication, thanks to the re-use of the keys derived on the previous full authentication.

The re-use of keys from previous authentication process shall be performed as follows: the "old" Master Key is fed into a pseudo-random function (as in full authentication) to generate a new Master Session Key (MSK) and a new Extended MSK. In this process, new Transient EAP Keys (TEKs) are generated but shall be discarded. The TEKs, needed to protect the EAP packets, shall be the "old" ones. So the EAP packets shall be protected with the same keys as in the previous full authentication process but the link layer key in the WLAN access network are renewed as the MSK (from which the link layer key is extracted) is generated again.

This process implies that the AAA server, after a full authentication process when a re-authentication identity has been issued, shall store the keys needed in case the next authentication is fast re-authentication: MK, TEKs and Counter (in case there has been previous fast-authentications). When the WLAN UE has completed a full authentication where it has received the re-authentication identity, it shall store the same data in order to be prepared for fast re-authentication.

6.1.4.1 EAP/AKA procedure

The implementation of EAP/AKA must include the fast re-authentication mechanism described in this chapter, although its use is optional and depends on operator's policies, which shall be enforced by the AAA server by means of sending the re-authentication identity in any authentication process. The complete procedure is defined in ref [4]. In this section it is described how the process works for WLAN-3GPP interworking.

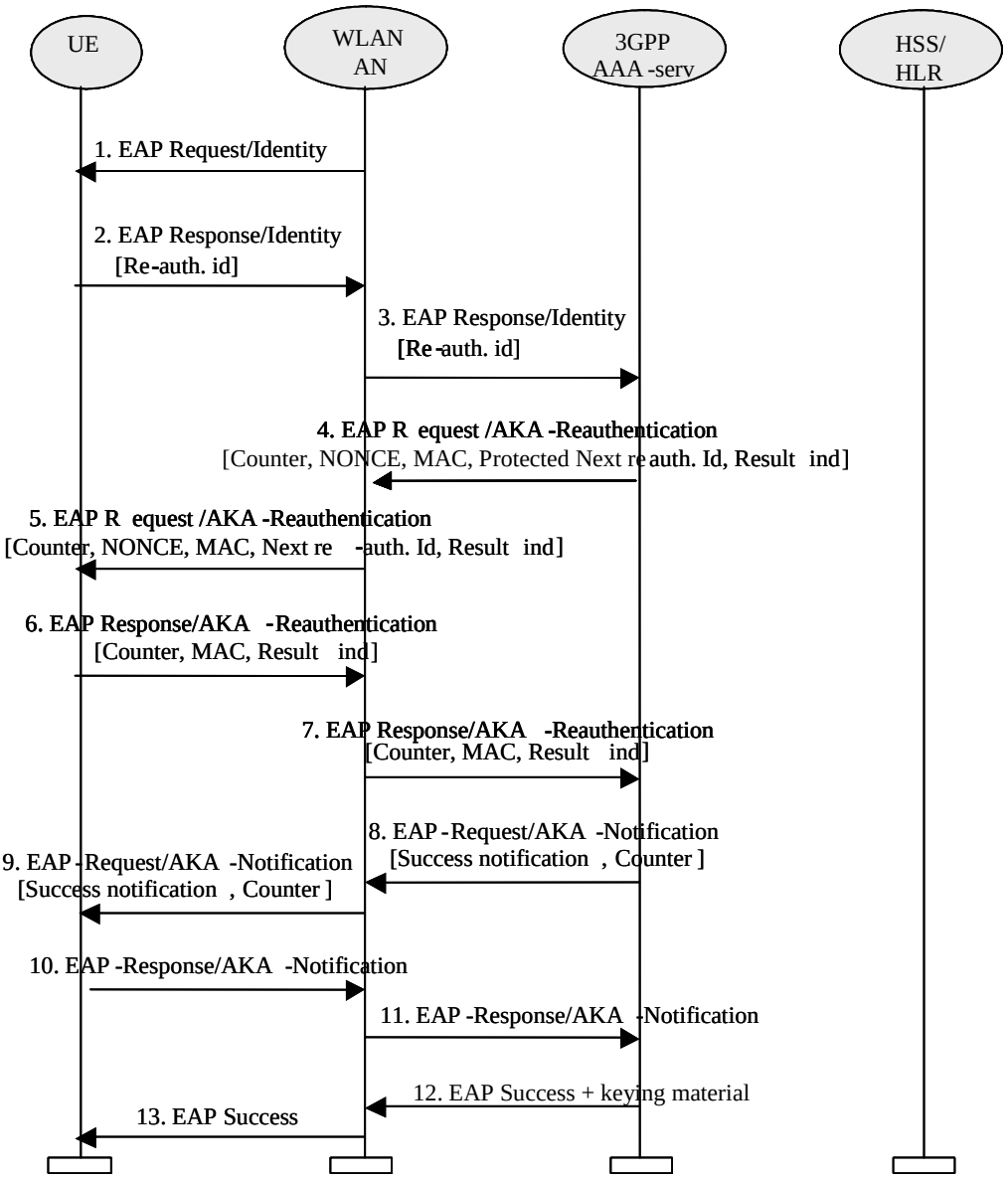


Figure 6: EAP AKA fast re-authentication

1. WLAN-AN sends an EAP Request/Identity to the WLAN-UE.

2. WLAN-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 WLAN-AN forwards the EAP Response/Identity to the AAA server.

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 WLAN-UE shall force a full-authentication (to avoid the use of the re-authentication identity more than once).

   The 3GPP AAA Server may send as well a result indication to the WLAN-UE, 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.

   The 3GPP AAA server may fail to recognize the identy 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 authnetication. This should however only be used in case the server fails to recognize the identity, as otherwise the purpose of fast re-authenticaion is defeated.

5. The WLAN-AN forwards the EAP Request message to the WLAN-UE.

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

7. The WLAN-AN forwards the response to 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 WLAN AN forwards the EAP Request/AKA-Notification message to the WLAN-UE.

10. The WLAN-UE sends the EAP Response/AKA-Notification.

11. The WLAN AN forwards the EAP Response/AKA-Notification message to 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 WLAN technology 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 WLAN-AN stores the keying material to be used in communication with the authenticated WLAN-UE.

13. The EAP Success message is forwarded to the WLAN-UE.

The re-authentication process may fail at any moment, for example because of unsuccessful checking of MACs or no response from the WLAN-UE after a network request. In that case, the EAP AKA process will be terminated as specified in ref. [4] and an indication shall be sent to HSS/HLR.

6.1.4.2 EAP/SIM procedure

The implementation of EAP/SIM must include the fast re-authentication mechanism described in this chapter, although its use is optional and depends on operator's policies, which shall be enforced by the AAA server by means of sending the re-authentication identity in any authentication process. The complete procedure is defined in ref [4]. In this section it is described how the process works for WLAN-3GPP interworking.

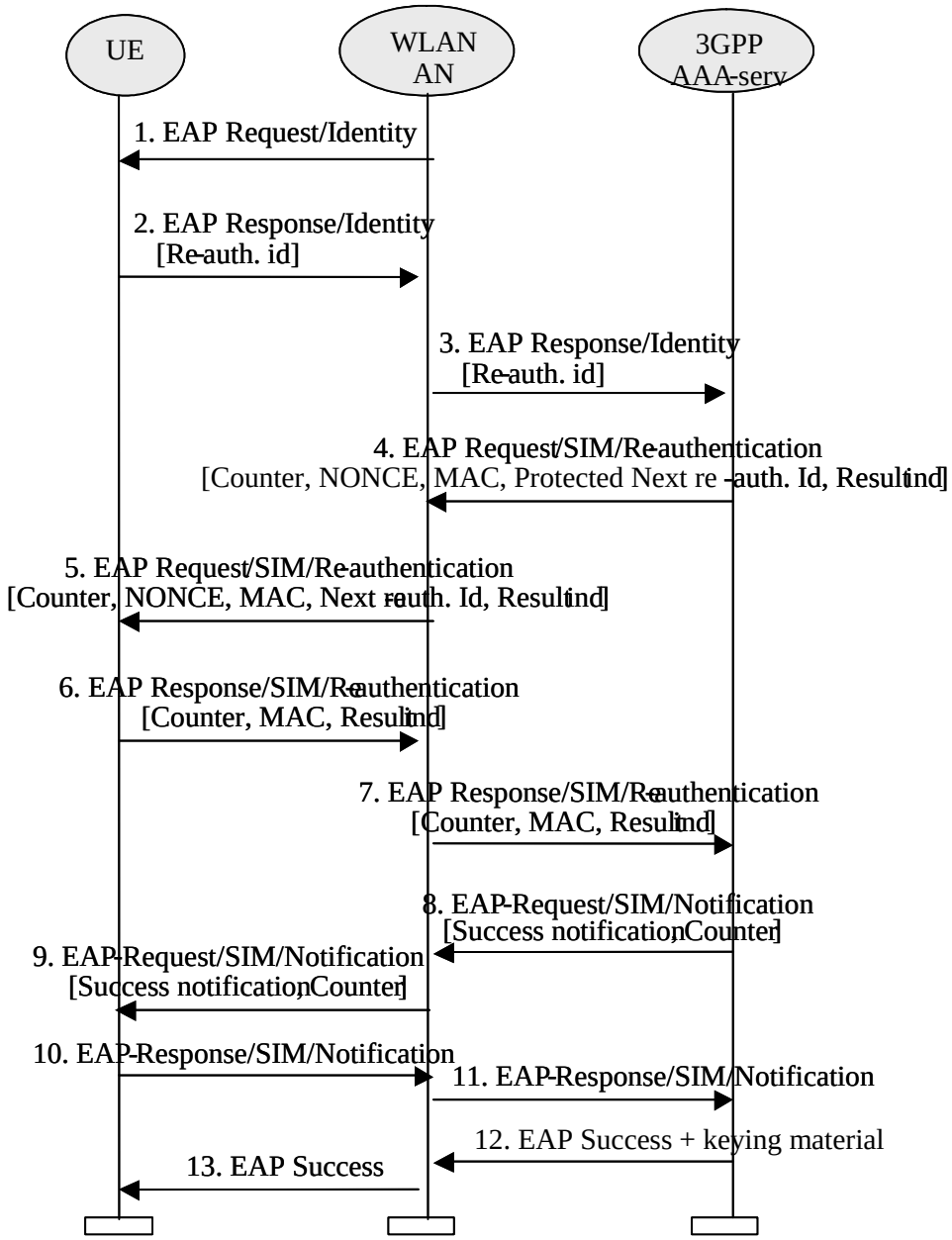


Figure 7: EAP SIM Fast re-authentication

1. WLAN-AN sends an EAP Request/Identity to the WLAN-UE.

2. WLAN-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 WLAN-AN forwards the EAP Response/Identity to the AAA server.

4. The AAA server initiates the Counter (which was initialised 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 WLAN-UE shall force a full-authentication (to avoid the use of the re-authentication identity more than once).

   The 3GPP AAA Server may send as well a result indication to the WLAN-UE, 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.

   The 3GPP AAA server may fail to recognize the identy 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 SIM method specific

identity request, i.e. "EAP-Request/SIM Start [Any identity]" in order to obtain a more reliable identity, in analogy of step 6 of the full EAP SIM authnetication. This should however only be used in case the server fails to recognize the identity, as otherwise the purpose of fast re-authenticaion is defeated.

5. The WLAN-AN forwards the EAP Request message to the WLAN-UE.
6. The WLAN-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 WLAN-UE shall include in this message the result indication if it received the same indication from the 3GPP AAA server. Otherwise, the WLAN-UE shall omit this indication.
7. The WLAN-AN forwards the response to 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/SIM/Notification, previous to the EAP Success message, if the 3GPP AAA Server requested previously to use protected success result indications. The message EAP Request/SIM/Notification is MAC protected, and includes an encrypted copy the Counter used in the present re-authentication process.
9. The WLAN AN forwards the EAP Request/AKA-Notification message to the WLAN-UE.
10. The WLAN-UE sends the EAP Response/SIM/Notification.
11. The WLAN AN forwards the EAP Response/SIM/Notification message to 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 WLAN technology 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 WLAN-AN stores the keying material to be used in communication with the authenticated WLAN-UE.
13. The EAP Success message is forwarded to the WLAN-UE.

The re-authentication process may fail at any moment, for example because of unsuccessful checking of MACs or no response from the WLAN-UE after a network request. In that case, the EAP SIM process will be terminated as specified in ref. [5] and an indication shall be sent to HSS/HLR.

6.1.4.3 Fallback to full authentication from fast re-authentication

In the EAP SIM/AKA processes for full authentication, the 3GPP AAA server sends to the WLAN UE the temporary identities to be used in the next authentication process. This next authentication process may be either a full authentication process or a fast re-authentication process, depending on the type of temporary identity received by the WLAN UE. If the WLAN UE receives a fast re-authentication identity, it shall use it in the next authentication, thus indicating to the AAA server that a fast re-authentication must be performed. If the WLAN UE receives only a pseudonym, the WLAN UE shall use it in the next authentication process and hence a full authentication will be started.

Whenever a fast re-authentication identity is received by the WLAN UE, this shall be the temporary identity used in the next authentication process, regardless if a pseudonym was received as well. The full authentication EAP Request/SIM Challenge and EAP Request/AKA Challenge messages allow both types of identity to be sent. However, in the messages EAP Request/AKA Re-authentication and EAP Request/SIM Re-authentication it is possible to send only re-authentication identities, according to references [4] and [5].

If the home network decides to initiate fast re-authentications, it shall indicate it to the WLAN UE by means of including the fast re-authentication identity in a full authentication process. If, later on, the home network decides to perform again full authentication, the 3GPP AAA server shall indicate it to the WLAN UE requesting a pseudonym after reception of the re-authentication identity. For this reason, whenever the AAA server sends a fast re-authentication identity to the WLAN UE, it shall include as well a pseudonym, so that the WLAN UE keeps it in case of fallback to full authentication, requested by the AAA server.

In case of EAP AKA, the AAA server, when it decides to perform full authentication again, shall use the message EAP Request/AKA Identity with the parameter AT_FULLAUTH_ID_REQ. The WLAN UE shall then return the pseudonym according to reference [4].

In case of EAP SIM, the AAA server, when it decides to perform full authentication again, shall use the message EAP Request/SIM/Start with the parameter AT_FULLAUTH_ID_REQ. The WLAN UE shall then return the pseudonym, according to reference [5].

6.1.5 Mechanisms for the set up of UE-initiated tunnels (WLAN 3GPP IP Access)

- The WLAN UE and the PDG use IKEv2, as specified in [ikev2], in order to establish IPSec security associations.
- Public key signature based authentication with certificates, as specified in [ikev2], is used to authenticate the PDG. The PDG shall authenticate itself to the WLAN UE with an identity. This identity shall be the same as the FQDN of the PDG if the PDG is found through the mechanism defined in [13]. Otherwise the PDG"s identity shall be one of the PDG identities pre-configured in the UE. This identity shall be contained in the IKEv2 ID_FQDN payload and shall match a dNSName SubjectAltName component in the PDG's certificate. A profile for certificate contents and processing is defined in clause 6.6A.
- EAP-AKA within IKEv2, as specified in [ikev2, section 2.16], is used to authenticate WLAN UEs, which contain a USIM.
- EAP-SIM within IKEv2, as specified in [ikev2, section 2.16], is used to authenticate WLAN UEs, which contain a SIM and no USIM.
- A profile for IKEv2 is defined in section 6.5.

6.1.5.1 Tunnel full authentication and authorization

The tunnel end point in the network is the PDG. As part of the tunnel establishment attempt the use of a certain W-APN is requested. When a new attempt for tunnel establishment is performed by the WLAN UE, the WLAN UE shall use IKEv2 as specified in ref. [29]. The EAP messages carried over IKEv2 shall be terminated in the 3GPP AAA Server, which communicates with the PDG via Wm interface, implemented with Diameter. Then the PDG shall extract the EAP messages received from the WLAN UE over IKEv2, and send them to the 3GPP AAA Server over Diameter (the opposite for messages sent from the 3GPP AAA Server). The WLAN UE shall use the Configuration Payload of IKEv2 to obtain the Remote IP address.

The sequence diagram is shown in figure 7A. The EAP message parameters and procedures regarding authentication are omitted since they are already described in this technical specification. Only decisions and processes relevant to this EAP-IKEv2 procedure are explained.

As the WLAN UE and PDG generated nonces are used as input to derive the encryption and authentication keys in IKEv2, replay protection is implemented as well. For this reason, there is no need for the 3GPP AAA Server to request the user identity again using the EAP AKA or EAP SIM specific methods (as specified in ref. [4] and ref. [5]), because the 3GPP AAA Server is certain that no intermediate node has modified or changed the user identity.

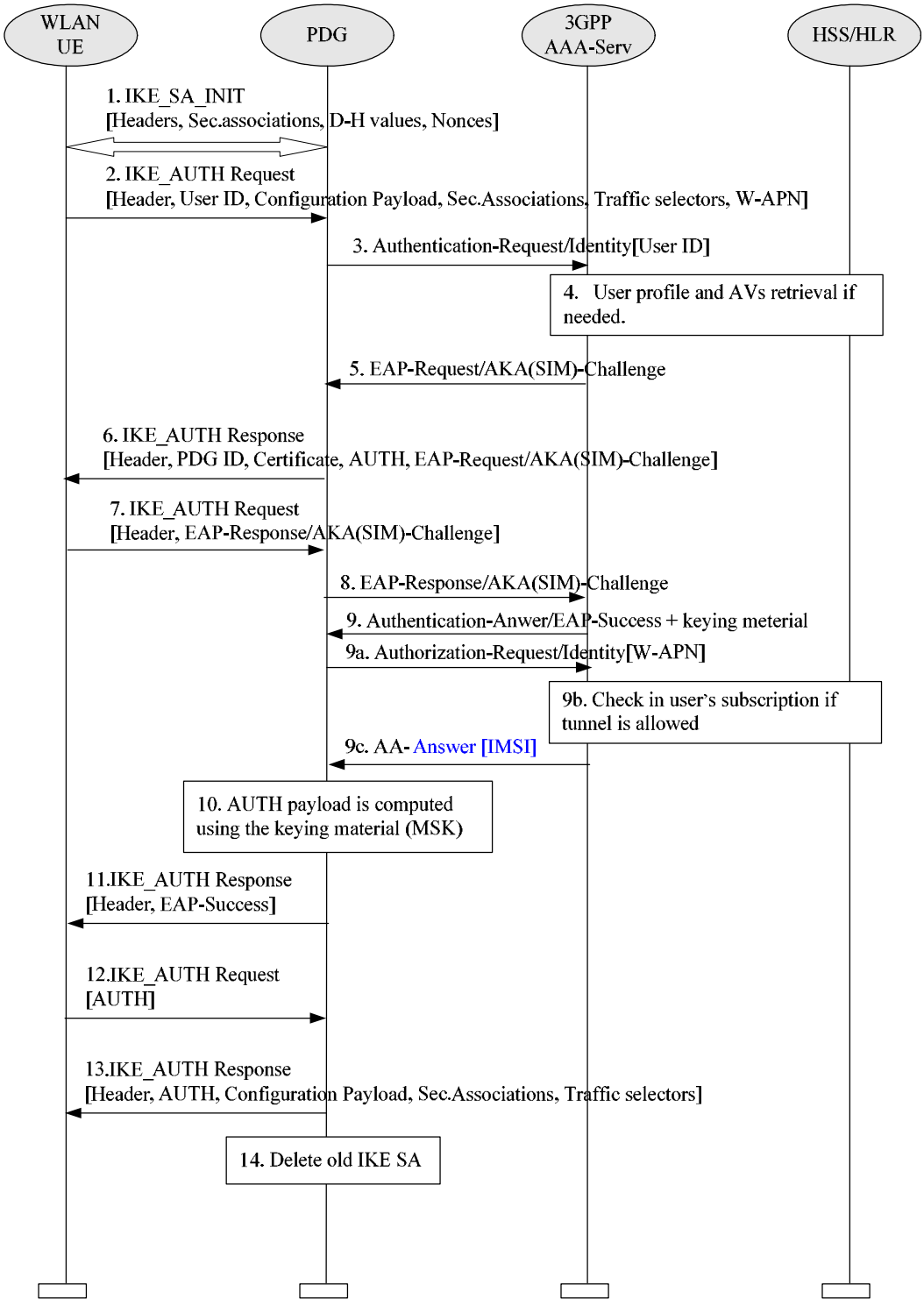


Figure 7A: Tunnel full authentication and authorization

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

2. The WLAN UE sends the user identity (in the Idi payload) and the W-APN information (in the Idr payload) in this first message of the IKE_AUTH phase, and begins negotiation of child security associations. The WLAN UE omits the AUTH parameter in order to indicate to the PDG that it wants to use EAP over IKEv2. The user identity shall be compliant with Network Access Identifier (NAI) format specified in RFC 2486 [14], containing the IMSI or the pseudonym. The identity in NAI format generated from the IMSI is described in ref. [4] and

ref. [5], depending on the type of EAP method to be used (EAP SIM or EAP AKA). If the WLAN UE"s Remote IP address needs to be configured dynamically, then the WLAN UE shall send the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to obtain a Remote IP Address.

3. The PDG sends the Authentication Request message with an empty EAP AVP to the 3GPP AAA Server, containing the user identity. The PDG shall include a parameter indicating that the authentication is being performed for tunnel establishment, as indicated in reference [37]. This will help the 3GPP AAA Server to distinguish between authentications for WLAN access and authentications for tunnel setup.

4. The3GPP AAA Server shall fetch the user profile and authentication vectors from HSS/HLR (if these parameters are not available in the 3GPP AAA Server) and determines the EAP method (SIM or AKA) to be used, according to the user subscription and/or the indication received from the WLAN UE. In addition, 3GPP AAA Server shall retrieve authentication vectors from HLR/HSS when it detects that the VPLMN selected by a user has changed. This can happen, for example, when a user is performing a VPLMN re-selection procedure and is initiating a new authentication procedure via a new VPLMN.

5. The 3GPP AAA Server initiates the authentication challenge. The user identity is not requested again, as in a normal authentication process, because there is the certainty that the user identity received in the EAP Identity Response message has not been modified or replaced by any intermediate node. The reason is that the user identity was received via an IKEv2 secure channel which can only be decrypted and authenticated by the end points (the PDG and the WLAN UE).

6. The PDG responds with its identity, a certificate, and sends the AUTH parameter to protect the previous message it sent to the WLAN 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 or EAP-Request/SIM-Challenge) is included in order to start the EAP procedure over IKEv2.

7. The WLAN 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 PDG forwards the EAP-Response/AKA-Challenge message or EAP-Response/SIM-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 PDG. This key material shall consist of the MSK generated during the authentication process. When the Wm interface (PDG-3GPP AAA Server) is implemented using Diameter, the MSK shall be encapsulated in the EAP-Master-Session-Key parameter, as defined in ref. [23].

9a. The PDG sends the Authorization Request message with an empty EAP AVP to the 3GPP AAA Server, containing W-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 W-APN is stepped up. If the maximum number of IKE SAs for that W-APN is exceeded, the 3GPP AAA Server shall send an indication to the PDG that established the oldest active IKE SA (it could be the same PDG 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 W-APN.

9c. The 3GPP AAA Server sends the AA-Answer to the PDG. 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. The MSK shall be used by the PDG to generate the AUTH parameters in order to authenticate the IKE_SA_INIT phase messages, as specified in ref. [29]. These two first messages had not been authenticated before as there were no key material available yet. According to ref. [29], the shared secret generated in an EAP exchange (the MSK), when used over IKEv2, shall be used to generated the AUTH parameters.

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

12. The WLAN 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 PDG.

13. The PDG checks the correctness of the AUTH received from the WLAN UE and calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. The PDG shall send the assigned Remote IP address in the configuration payload (CFG_REPLY), if the WLAN UE requested for a Remote IP address through the

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

14. If the PDG detects that and old IKE SA for that W-APN already exists, it will delete the IKE SA and send the WLAN UE an INFORMATIONAL exchange with a Delete payload, as specified in reference [29], in order to delete the old IKE SA in WLAN UE.

6.1.5.2 Tunnel fast re-authentication and authorization

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

The sequence diagram is shown in figure 7B. The EAP message parameters and procedures regarding fast re-authentication are omitted since they are already described in this technical specification. Only decisions and processes relevant to this EAP-IKEv2 procedure are explained.

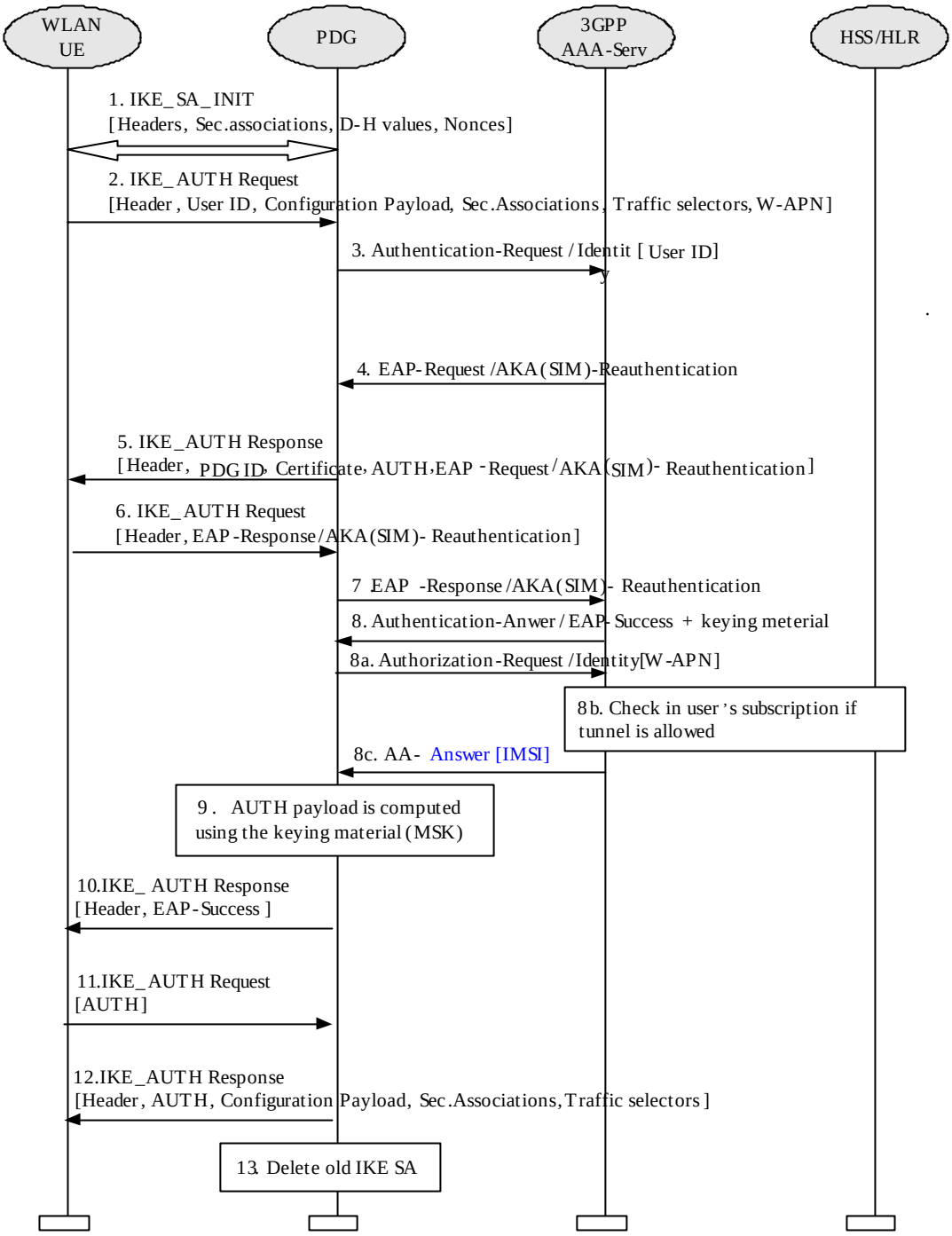


Figure 7B: Tunnel fast re-authentication and authorization

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

2. The WLAN UE sends the re-authentication identity (in the Idi payload) and the W-APN information (in the Idr payload) in this first message of the IKE_AUTH phase, and begins negotiation of child security associations. The WLAN UE omits the AUTH parameter in order to indicate to the PDG that it wants to use EAP over IKEv2. The re-authentication identity used by the WLAN UE shall be the one received in the previous authentication process. If the WLAN UE"s Remote IP address needs to be configured dynamically, then the WLAN UE shall

send the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to obtain a Remote IP Address.

3. The PDG sends the Authentication Request message with an empty EAP AVP to the AAA server, containing the re-authentication identity. The PDG shall include a parameter indicating that the authentication is being performed for tunnel establishment, as indicated in ref. [37]. This will help the AAA server to distinguish between authentications for WLAN access and authentications for tunnel setup.

4. The AAA server initiates the fast re-authentication challenge.

5. The PDG responds with its identity, a certificate, and sends the AUTH parameter to protect the previous message it sent to the WLAN UE (in the IKE_SA_INIT exchange). It completes the negotiation of the child security associations as well. The EAP message received from the AAA server (EAP-Request/AKA-Reauthentication or EAP-Request/SIM-Reauthentication) is included in order to start the EAP procedure over IKEv2.

6. The WLAN 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 PDG forwards the EAP-Response/AKA-Reauthentication message or EAP-Response/SIM-Reauthentication message to the AAA server.

8. When all checks are successful, the AAA server sends the Authentication Answer including an EAP success and the key material to the PDG. This key material shall consist of the MSK generated during the fast re-authentication process. When the Wm interface (PDG-AAA server) is implemented using Diameter, the MSK shall be encapsulated in the EAP-Master-Session-Key parameter, as defined in ref. [23].

8a. The PDG sends the Authorization Request message with an empty EAP AVP to the AAA server, containing W-APN.

8b. The AAA server checks in user"s subscription if he/she is authorized to establish the tunnel.

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

8c. The AAA server sends the AA-Answer to the PDG. The AAA server shall send the IMSI within the AA-Answer.

9. The MSK shall be used by the PDG to generate the AUTH parameters in order to authenticate the IKE_SA_INIT phase messages, as specified in ref. [29]. These two first messages had not been authenticated before as there were no key material available yet. According to ref. [29], 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 WLAN UE over IKEv2.

11. The WLAN 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 PDG.

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

13. If the PDG detects that and old IKE SA for that W-APN already exists, it will delete the IKE SA and send to the WLAN UE an INFORMATIONAL exchange with a Delete payload, as specified in reference [29], in order to delete the old IKE SA in WLAN UE.

6.1.6 Void

6.2 Confidentiality mechanisms

6.2.1 Confidentiality mechanisms in WLAN Direct IP Access

The link layer confidentiality mechanisms are outside the scope of 3GPP. When the WLAN link layer is according to IEEE 802.11 then the confidentiality mechanisms of IEEE 802.11i [6] shall be used. It is specified in ref. [4] and [5] how the key material required for the link layer confidentiality mechanism is obtained from the master session key MSK. The generation of MSK is defined in ref. [4] and [5] as well. The use of ref. [4] and [5] in the context of 3GPP is specified in section 6.1 of this document.

When the key derivation is finished in the AAA server, the key material shall be sent to the WLAN AN via the Wa and Wd (in case of roaming) interfaces.

6.2.2 Confidentiality mechanisms in WLAN 3GPP IP Access

The confidentiality of IP packets sent through a tunnel between the UE and the PDG, if required, shall be protected by IPSec ESP (RFC 2406 [30]). A profile for IPSec ESP is defined in section 6.6.

6.3 Integrity mechanisms

6.3.1 Integrity mechanisms in WLAN Direct IP Access

The link layer integrity mechanisms are outside the scope of 3GPP. When the WLAN link layer is according to IEEE 802.11 then the integrity mechanisms of IEEE 802.11i [6] shall be used. It is specified in ref. [4] and [5] how the key material required for the link layer integrity mechanism is obtained from the master session key MSK. The generation of MSK is defined in ref. [4] and [5] as well. The use of ref. [4] and [5] in the context of 3GPP is specified in section 6.1 of this document.

When the key derivation is finished in the AAA server, the key material shall be sent to the WLAN AN via the Wa and Wd (in case of roaming) interfaces.

6.3.2 Integrity mechanisms in WLAN 3GPP IP Access

The integrity of IP packets sent through a tunnel between the UE and the PDG shall be protected by IPSec ESP (RFC 2406 [30]). A profile for IPSec ESP is defined in section 6.6.

6.4 Temporary identity management

6.4.1 Temporary Identity Generation

Temporary Identities (Pseudonyms or re-authentication identities) are generated as some form of encrypted IMSI. Advanced Encryption Standard (AES) (see ref. [17]) in Electronic Codebook (ECB) mode of operation with 128-bit keys is used for this purpose.

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

1. A *Compressed IMSI* is created utilising 4 bits to represent each digit of the IMSI. According to TS 23.003 [18], the length of the IMSI is not more than 15 digits (numerical characters, 0 through 9). The length of the *Compressed IMSI* shall be 64 bits (8 octets), and the most significant bits shall be padded by setting all the bits to 1.

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

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

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

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

A 128-bit secret key, Kpseu, is used for the encryption. The same secret key must be configured at all the WLAN AAA servers in the operator network so that any WLAN AAA server can obtain the permanent identity from atemporary identity generated at any other WLAN AAA server (see section 6.4.2).

Figure 8 summarises how the *Encrypted IMSI* is obtained.

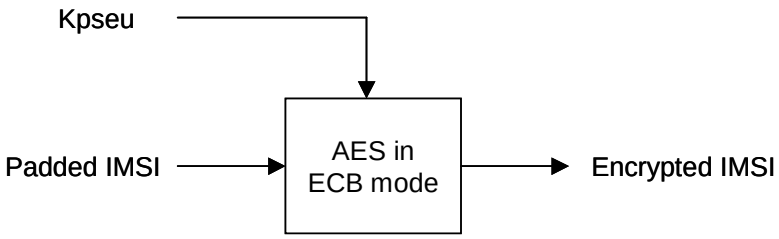


Figure 8: Encrypted IMSI generation

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

- *Encrypted IMSI*, so that a AAA server can later obtain the IMSI from the temporary identity.
- *Key Indicator*, so that the AAA server that receives the temporary identity can locate the appropriate key to de-encrypt the Encrypted IMSI (see section 6.4.2).
- *Temporary identity Tag*, used to mark the identity as temporary pseudonym or re-authentication identity. The tag should be different for identities generated for EAP-SIM and for EAP-AKA.

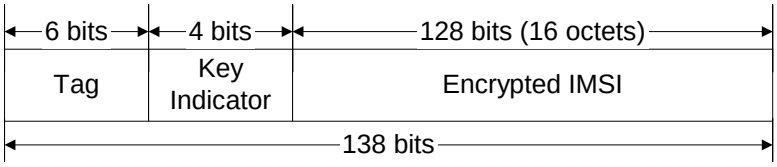


Figure 9

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

The last step in the generation of the temporary identities consists on converting the concatenation above to a printable string using the BASE64 method described in section 4.3.2.4 of RFC 1421 [16]. With this mechanism, each 6-bit group is used as an index into an array of 64 printable characters. As the length of the concatenation is 138 bits, the length of the resulting temporary identity is 23 characters, and no padding is necessary. Observe that the length of the Temporary identity*Tag* has been chosen to be 6 bits, so that it directly translates into one printable character after applying the transformation. Therefore, at reception of a user identity, the AAA server can recognise that it is a temporary identity for EAP-SIM or a temporary identity for EAP-AKA without performing any reverse transformation (i.e. without translating any printable character into the corresponding 6 bits).

6.4.2 Key Management

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

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

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

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

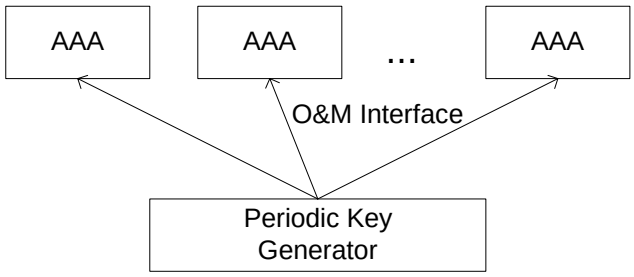


Figure 10: Key configuration via O&M

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

6.4.3 Impact on Permanent User Identities

User identities (permanent or temporary) are sent with the form of a NAI, according to the EAP-SIM/AKA specifications, and the maximum length of a NAI that we can expect to be handled correctly by standard equipment is 72 octets (see RFC 2486 [14]). Moreover, this NAI shall be transported inside the User-Name attribute of a RADIUS Access-Request, with standard length up to 63 octets (see RFC 2865 [15]). Therefore, it can be assumed that the maximum length of a WLAN user identity should be 63 octets (i.e. 63 characters).
Since the length of the temporary identity proposed in section 6.4.1 is 23 characters, the length of the realm part of any WLAN permanent user identity must always be 40 characters or less. This applies regardless of whether the length of the username part of the permanent user identity is less than 23 characters.

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

Moreover, the WLAN permanent user identities should not begin with the character resulting of the printable encoding transformation (see section 6.4.1) of the *Temporary identity Tag* used for EAP-SIM and EAP-AKA pseudonyms or re-authentication identities. This is needed so that at reception of a WLAN user identity, the AAA server can determine whether it is a permanent or a temporary user identity.

6.4.4 Acknowledged Limitations

This mechanism does not prevent forging of temporary identities generated with keys that are no longer maintained in the AAA servers. That is, an attacker may form a temporary identity by concatenating the desired *Temporary identity*

Tag and 132 bits of random information, and then applying the printable encoding transformation (see section 6.4.1). At reception of such temporary identity in a AAA server, the following cases are possible:

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

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

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

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

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

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

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

6.5 Profile of IKEv2

IKEv2, as specified in ref. [29], contains a number of options, where some are not needed for the purposes of this specification and others are required. IKEv2 is therefore profiled in this section. When IKEv2 is used in the context of this specification the profile specified in this section shall be supported.

Access to services offered by the HPLMN (WLAN 3GPP IP Access) follows a VPN-like approach. In ref. [31] it can be found a set of recommendations of IKEv2 profiles, suitable for VPN-like solutions. On the other hand, ref. [33] sets rules and recommendations for individual algorithms support. Following recommendation from both papers, the below two profiles shall be supported by the PDG and the WLAN-UE:

First cryptographic suite:

- Confidentiality: 3DES in CBC mode;
- Pseudo-random function: HMAC-SHA1;
- Integrity: HMAC-SHA1-96;
- Diffie-Hellman group 2 (1024-bit MODP), mandatory for IKEv2 according to ref. [33].

Second cryptographic suite:

- Confidentiality: AES with fixed key length in CBC mode. The key length is set to 128 bits;
- Pseudo-random function: AES-XCBC-PRF-128;

- Integrity: AES-XCBC-MAC-96.
- Diffie-Hellman group 2 (1024-bit MODP), mandatory for IKEv2 according to ref. [33]

For NAT traversal, the NAT support of IKEv2 shall be supported as specified in section 2.23 of [29]. Re-keying of IPsec SAs and IKE SAs shall be supported as specified in [29].

6.6 Profile of IPSec ESP

IPSec ESP, as specified in RFC 2406 [30], contains a number of options and extensions, where some are not needed for the purposes of this specification and others are required. IPSec ESP is therefore profiled in this section. When IPSec ESP is used in the context of this specification the profile specified in this section shall be supported. Rules and recommendations in ref. [31] and [33] have been followed, as in case of IKEv2.

First cryptographic suite:

- Confidentiality: 3DES in CBC mode;
- Integrity: HMAC-SHA1-96. The key length is 160 bits, according to RFC 2104 [34] and RFC 2404 [35];
- Tunnel mode must be used.

Second cryptographic suite:

- Confidentiality: AES with 128-bit keys in CBC mode. The key length is set to 128 bits;
- Integrity: AES-XCBC-MAC-96;
- Tunnel mode must be used.

It shall be possible to turn off confidentiality protection in the tunnel. This means that the transform IDs for encryption ENCR_NULL shall be allowed to negotiate, as specified in reference [29]. Integrity protection shall always be used, i.e. the authentication algorithm in reference [30] shall not be NULL.

For NAT traversal, the UDP encapsulation for ESP tunnel mode specified in reference [32] shall be supported.

6.6A Profile for PDG certificates

Certificates used for authentication of the PDG shall meet the following profile of RFC 3280 [39].

a) The certificate shall be encoded in DER format.

b) The version shall be 2 ("v3").

c) The certificate serial number shall meet the requirements in RFC 3280 [39], section 4.1.2.2.

d) The signature algorithm shall be "sha1WithRSAEncryption" [38], and the RSA public key used for signing shall not be longer than 2048 bits.

e) The issuer name shall not be empty.

f) The validity period shall meet the requirements in RFC 3280 [39], section 4.1.2.5.

f) The subject name may be empty in PDG certificates and shall not be empty in CA certificates.

g) The subject public key shall use algorithm "rsaEncryption" (RFC 3279 [38]), and the RSA public key shall not be longer than 2048 bits.

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

i) The SubjectAltName extension shall be present if this is a PDG certificate, and shall contain at least one dNSName component.

j) The BasicConstraints extension shall be present if this is a CA certificates with "CA" flag asserted. The pathLenConstraint may be present.

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

l) The KeyUsage extension shall be present in all certificates. The keyCertSign bit shall be set in CA certificates, and digitalSignature bit shall be set in PDG certificates.

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

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

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

p) The total length of a certificate shall not exceed 2000 bytes.

Certificate processing requirements:

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

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

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

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

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

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

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

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

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

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

k) UE may check the validity of the certificates using CRLs or OCSP [43]. Support for CRLs is optional. Support for OCSP is mandatory.

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

6.7 WLAN UE split interworking

EAP-AKA/SIM procedures terminate in the UICC or MT, so the TE shall contact the MT via protected local interface (e.g. Bluetooth, IrDa, RS232, USB, etc.) at any authentication or re-authentication process, using the AT commands +CUAD, +CEAP and +CERP, as defined in TS 27.007 [40]. The local interface acts as a transparent carrier of the EAP methods; the TE just forwards messages from the MT or UICC to the network (or in the opposite direction) and does not take active part in the authentication process. The TE is not able to handle any key except the MSK and/or the EMSK when it receives them at the end of the authentication process. The MT shall forbid the transfer of RUN GSM ALGO command, and the AUTHENTICATE command in GSM/UMTS security context, from any TE involved in WLAN-UE split interworking. The EAP peer at the network side is any node in the WLAN AN, the VPLMN or the home network. Since the interworking to be described here is at the WLAN UE side, it is not relevant which node is sending/receiving any message in the network side.

6.7.1 Full authentication with EAP AKA

The procedures specified in clauses 6.7.1.1 and 6.7.1.2 have in common that, prior to the exchange of EAP messages, the appropriate USIM application on the UICC needs to be selected. For this purpose, the TE runs the AT command +CUAD to discover what applications are available for selection on the UICC, so that the user can be prompted, if necessary, to perform the selection, as specified in ETSI TS 102.221 [42].

6.7.1.1 Termination in the UICC

The process is shown in figure 11.

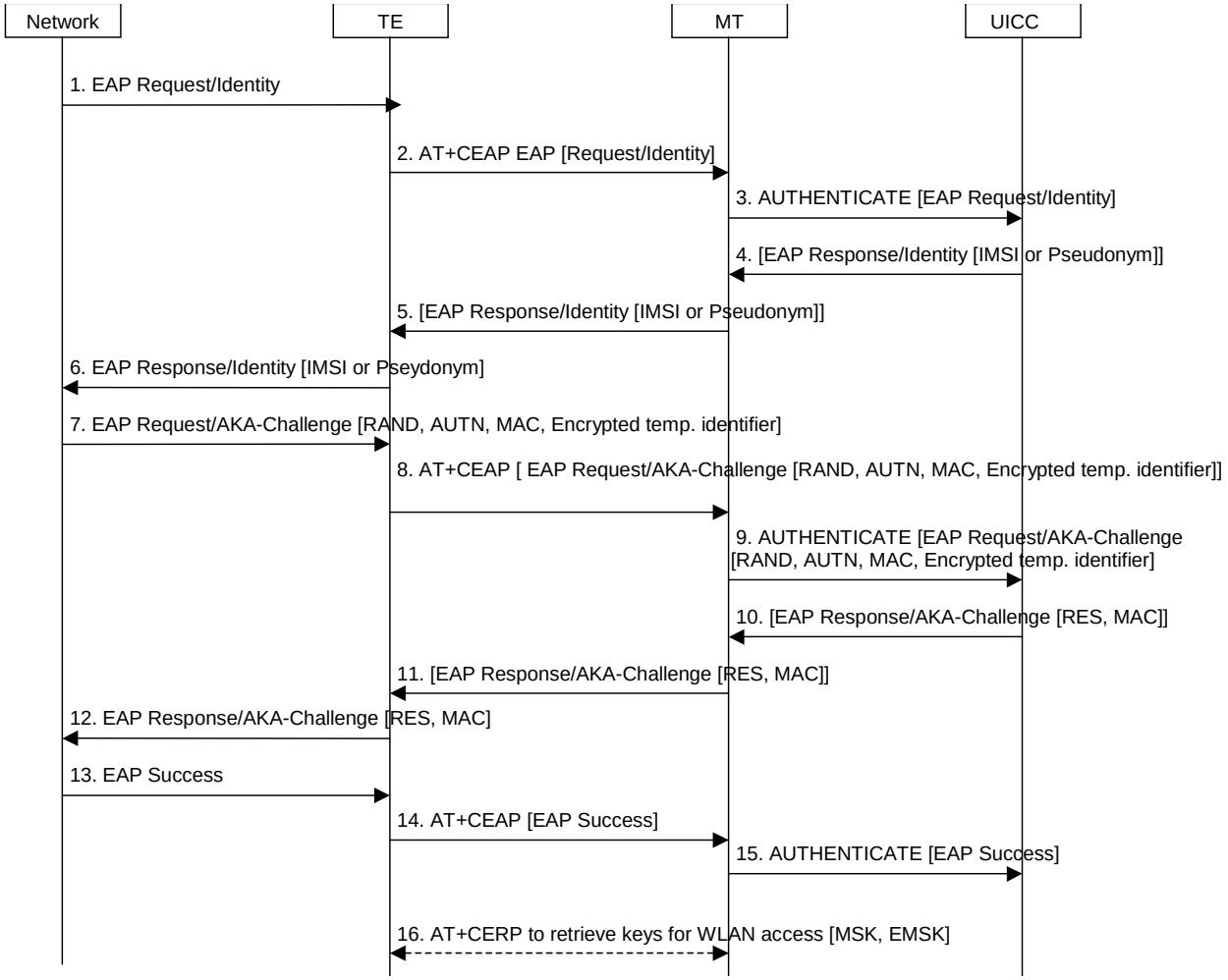


Figure 11: Full authentication with EAP-AKA

1. The network sends an EAP request identity (either a IMSI or a pseudonym) message to the TE (the device providing WLAN access) in order to initiate the procedure.

2. The TE sends the EAP packet received in message 1 to the UICC application using +CEAP AT command. The EAP request identity message is forwarded via the MT to the UICC application. Prior to step 2, the MT shall open a communication session with the UICC application, as indicated in TS 27.007 [40], and then shall select the appropriate DF, as indicated in ETSI TS 102.310 [41].

3. The MT performs the received +CEAP AT command (see TS 27.007 [40]).

4. The UICC application returns the EAP Response/Identity packet to the MT.

5. The MT returns the EAP Response/Identity packet to the TE, in the +CEAP AT command response data.

6. The TE sends the EAP Response/Identity packet to the network.

7. The network initiates the EAP AKA authentication process.
8. The TE sends the EAP packet received in message 7 to the UICC application via the MT using +CEAP AT command.
9. The MT performs the received +CEAP AT command (see TS 27.007 [40]).
10. The UICC application returns the EAP Response/AKA-Challenge packet to the MT.
11. The MT returns the EAP Response/AKA-Challenge packet to the TE, in the +CEAP AT command response data.
12. The TE sends the EAP Response/AKA-Challenge packet to the network, which checks the validity of the RES and compute the MAC of the entire message received, comparing it with the received MAC.
13. If both checks are correct, the network sends an EAP Success packet to the TE.
14. The TE sends the EAP packet received in message 13 to the UICC application using +CEAP AT command.
15. The MT performs the received +CEAP AT command (see TS 27.007 [40]).
16. After a successful EAP authentication, the TE shall retrieve the key material (i.e. MSK and EMSK) from EFEAPKEYS (for this purpose, the TE uses the +CERP AT command). The TE uses MSK and EMSK for security purposes, for example for WLAN link layer security

6.7.1.2 Termination in the MT

The process is shown in figure 12.

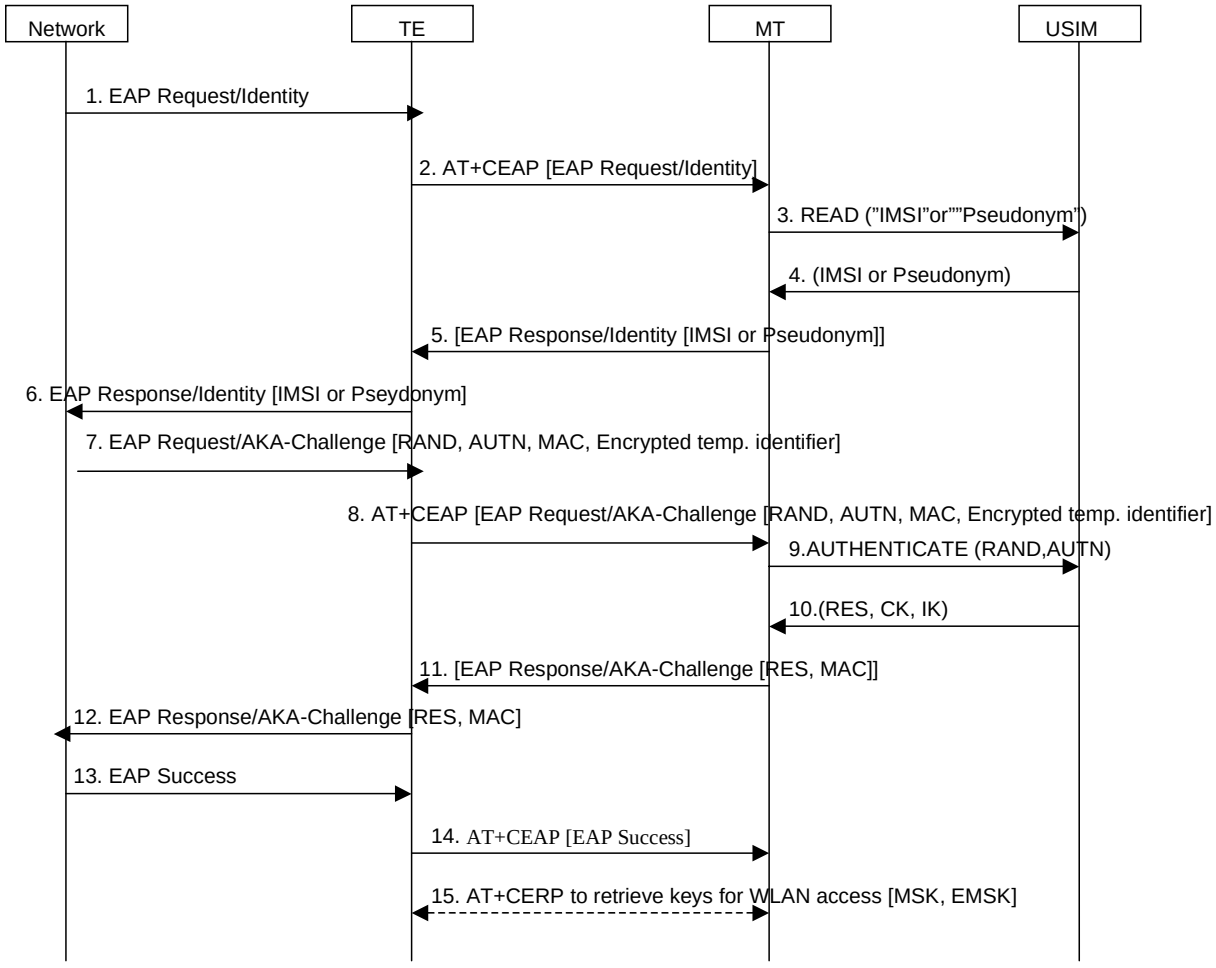


Figure 12: Full authentication with EAP AKA

1. The network sends a EAP request identity (either a IMSI or a pseudonym) message to the TE (the device providing WLAN access) in order to initiate the procedure.
2. The TE sends the EAP packet received in message 1 to the MT using +CEAP AT command.
3. If the MT does not have the identity available, it requests the identity from the USIM.
4. The USIM returns the identity to the MT.
5. The MT inserts the identity in the EAP response identity message and sends it to the network via the TE, using the +CEAP AT command.
6. The TE sends the EAP response identity message to the network.
7. The network initiates the EAP AKA authentication process.
8. The TE forwards the EAP request to the MT with all the parameters, using the +CEAP AT command.
9. The MT sends the authentication challenge to the USIM, using the AUTHENTICATE command.
10. The USIM replies with the calculated keys CK and IK, which will be used by the MT to derive the Master Key (MK) according to ref. [4]. The USIM also returns RES. The MK is then used as input to generate the keys needed to calculate the MAC of message 8 (which will be checked against the received one) and the new MAC for the next message.
11. The EAP response message, sent by the MT to the TE using the +CEAP AT command, includes the RES and the calculated MAC.
12. The TE forwards the response message to the network, which will check the validity of the RES and compute the MAC of the of the entire message received, comparing it with the received MAC.
13. If both checks are correct, the network will send an EAP success message to the TE.
14. The TE forwards the EAP success to the MT as a success indication, using the +CEAP AT command.
15. After receiving the success indication, the MT will derive according to ref. [4] the Master Session Key and Extended Master Session Key (MSK and EMSK). The TE requests these keys, using the +CERP AT command.

6.7.2 Full authentication with EAP SIM

6.7.2.1 Termination in the UICC

The process is shown in figure 13, and it''s very similar to EAP AKA (from MT-TE interface point of view).

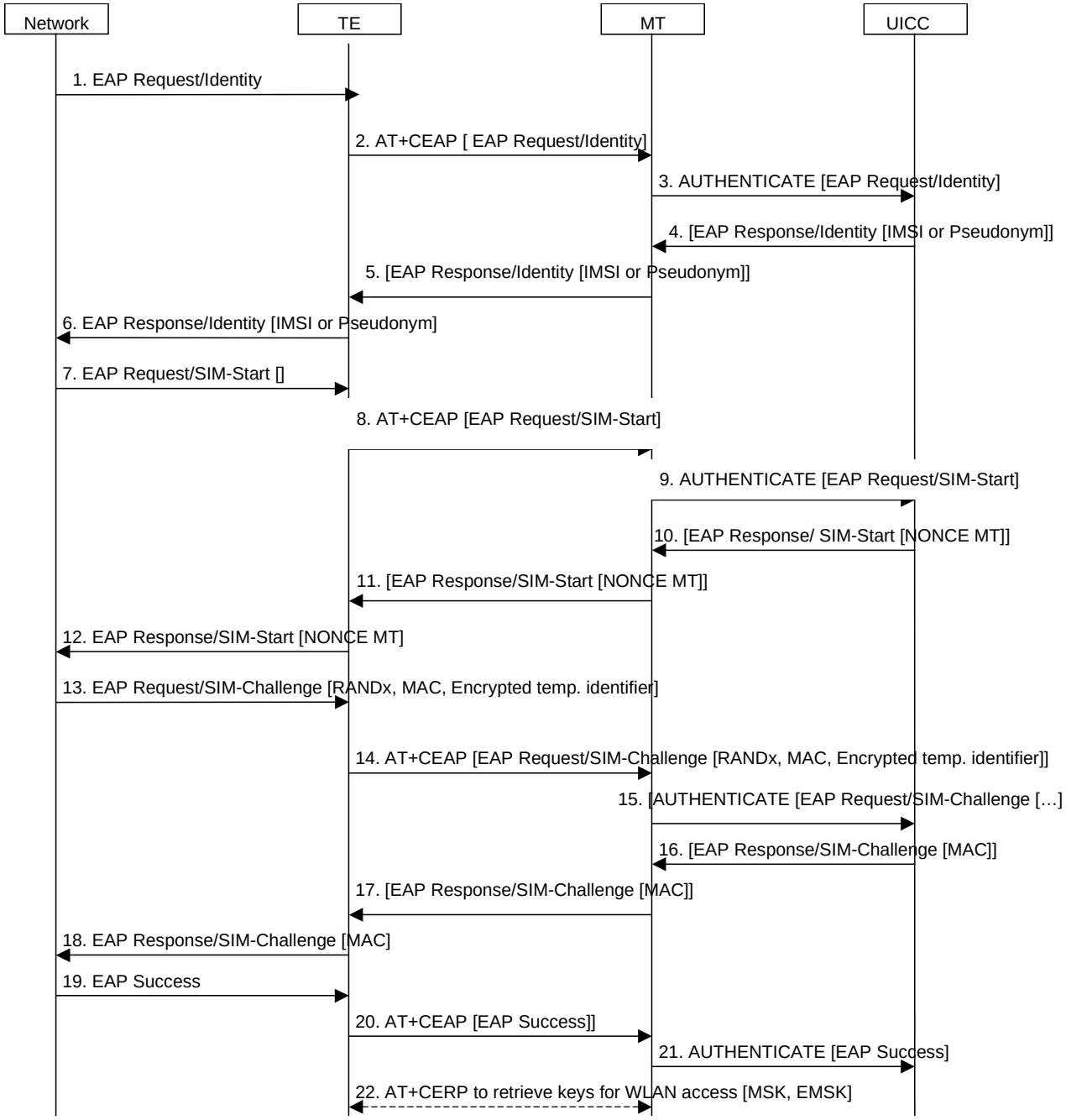


Figure 13: Full authentication with EAP-SIM

1. The network sends an EAP request identity (either a IMSI or a pseudonym) message to the TE (the device providing WLAN access) in order to inititiate the procedure.

2. The TE sends the EAP packet received in message 1 to the UICC application using +CEAP AT command. The EAP request identity message is forwarded via the MT to the UICC application. Prior to step 2, the MT shall open a communication session with the UICC application, as indicated in TS 27.007 [40], and shall select the appropriate DF, as indicated in ETSI TS 102.310 [41].

3. The MT performs the received +CEAP AT command (see TS 27.007 [40]).

4. The UICC application returns the EAP Response/Identity packet to the MT.

5. The MT returns the EAP Response/Identity packet to the TE, in the +CEAP AT command response data.

6. The TE sends the EAP Response/Identity packet to the network.

7. The network initiates the EAP SIM authentication process.

8. The TE sends the EAP packet received in message 7 to the UICC application via the ME using +CEAP AT command.
9. The MT performs the received + CEAP AT command (see TS 27.007 [40]).
10. The UICC application returns the EAP Response/SIM-Start packet to the MT.
11. The MT returns the EAP Response/SIM-Start packet to the TE, in the + CEAP AT command response data.
12. The TE sends the EAP Response/SIM-Start packet to the network, which uses the NONCE to calculate the MAC.
13. The network sends an EAP SIM challenge request with the calculated MAC (over the whole EAP message and the NONCE) and the rest of parameters.
14. The TE sends the EAP packet received in message 13 to the UICC application via the MT using +CEAP AT command.
15. The MT performs the received +CEAP AT command (see TS 27.007 [40]).
16. The UICC application returns the EAP Response/SIM-Challenge packet to the MT.
17. The MT returns the EAP Response/SIM-Challenge packet to the TE, in the + CEAP AT command response data.
18. The TE sends the EAP Response/SIM-Challenge packet to the network, which computes the MAC and compares it with the received MAC.
19. If checks are correct, the network sends an EAP Success packet to the TE.
20. The TE sends the EAP packet received in message 19 to the UICC application using +CEAP AT command.
21. The MT performs the received +CEAP AT command (see TS 27.007 [40]).
22. After a successful EAP authentication, the TE shall retrieve the key material (i.e. MSK and EMSK) from $EF_{EAPKEYS}$ (for this purpose, the TE uses the +CERP AT command). The TE uses MSK and EMSK for security purposes, for example, for WLAN link layer security.

6.7.2.2 Termination in the MT

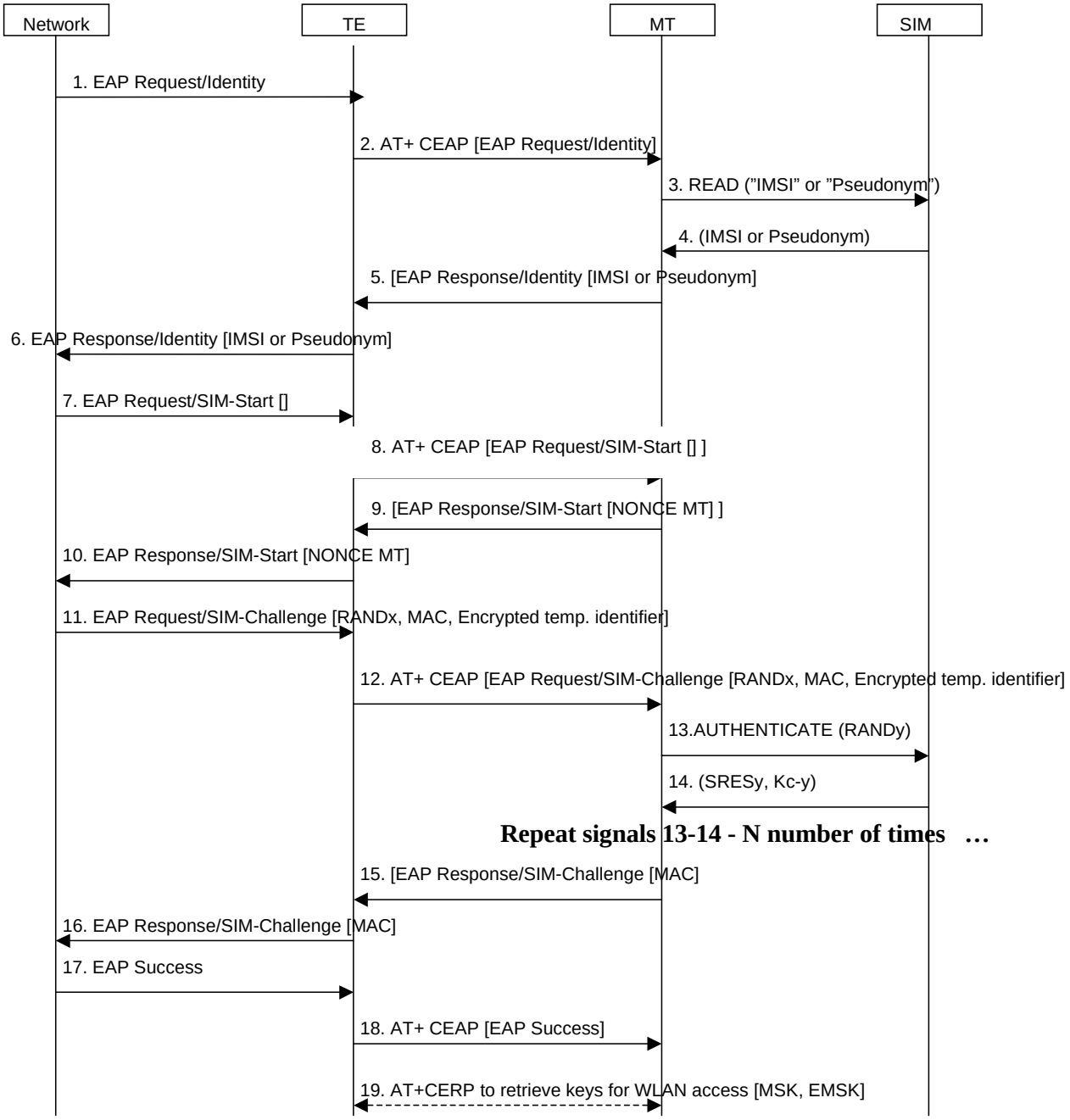


Figure 14: Full authentication with EAP SIM

1. The network sends a EAP request identity (either a IMSI or a pseudonym) message to the TE (the device providing WLAN access) in order to inititiate the procedure.
2. The TE sends the EAP packet received in message 1 to the MT using +CEAP AT command.
3. If the MT does not have the identity available, it requests the identity from the USIM.
4. The USIM returns the identity to the MT.
5. The MT inserts the identity in the EAP response identity message and sends it to the network via the TE, using the +CEAP AT command..
6. The TE sends the EAP response identity message to the network.
7. The network initiates the EAP SIM authentication process.

8. The TE forwards the EAP SIMstart request to the MT, using the +CEAP AT command.
9. The MT generates a NONCE and sends it to the TE, using the +CEAP AT command.
10. The TE forwards the NONCE to the network, which uses the NONCE to calculate the MAC.
11. The network sends an EAP SIM challenge request with the calculated MAC (over the whole EAP message and the NONCE) and the rest of parameters.
12. The TE forwards the message to the MT, using the +CEAP AT command.
13. The MT extracts the RAND and sends it to the SIM for key calculation, using the AUTHENTICATE command.
14. The SIM responds with the calculated SRES and Kc (the two latter messages will be repeated two or three times). The MT will use the received Kcs (among other inputs) to derive the Master Key (MK) according to ref. [5]. The MK is then used as input to generate the keys needed to calculate the MAC of message 11 (which will be checked against the received one) and the new MAC for the next message.
15. The MT sends the EAP SIM challenge response with the MAC, calculated over the whole EAP message and the SRES (the SRES is the concatenated values of the individual SRESy received from the SIM) to the TE, using the +CEAP AT command.
16. The TE forwards the message to the network.
17. The network calculates its own copy of the MAC and if it matches the received one, it sends an EAP success message.
18. The TE forwards the EAP success to the MT as a success indication, using the +CEAP AT command.
19. After receiving the success indication, the MT will derive according to ref. [5] the Master Session Key and Extended Master Session Key (MSK and EMSK) and send them to the TE, using the +CERP AT command, which will use them for other security purposes, for example WLAN link layer security.

6.7.3 Fast re-authentication with EAP AKA

The procedures specified in this clause use the same UICC application as the preceding full authentication. So, there is no need to run the AT command +CUAD prior to the procedures specified in this clause.

6.7.3.1 Termination in the UICC

The keys needed to protect the EAP packets are re-used from the previous full authentication process. The MSK and EMSK are calculated again using the original MK, as specified in reference [4]. For this reason, the new MSK and EMSK are transferred from the UICC application to the TE when the fast re-authentication process is finished. The process is shown in figure 15.

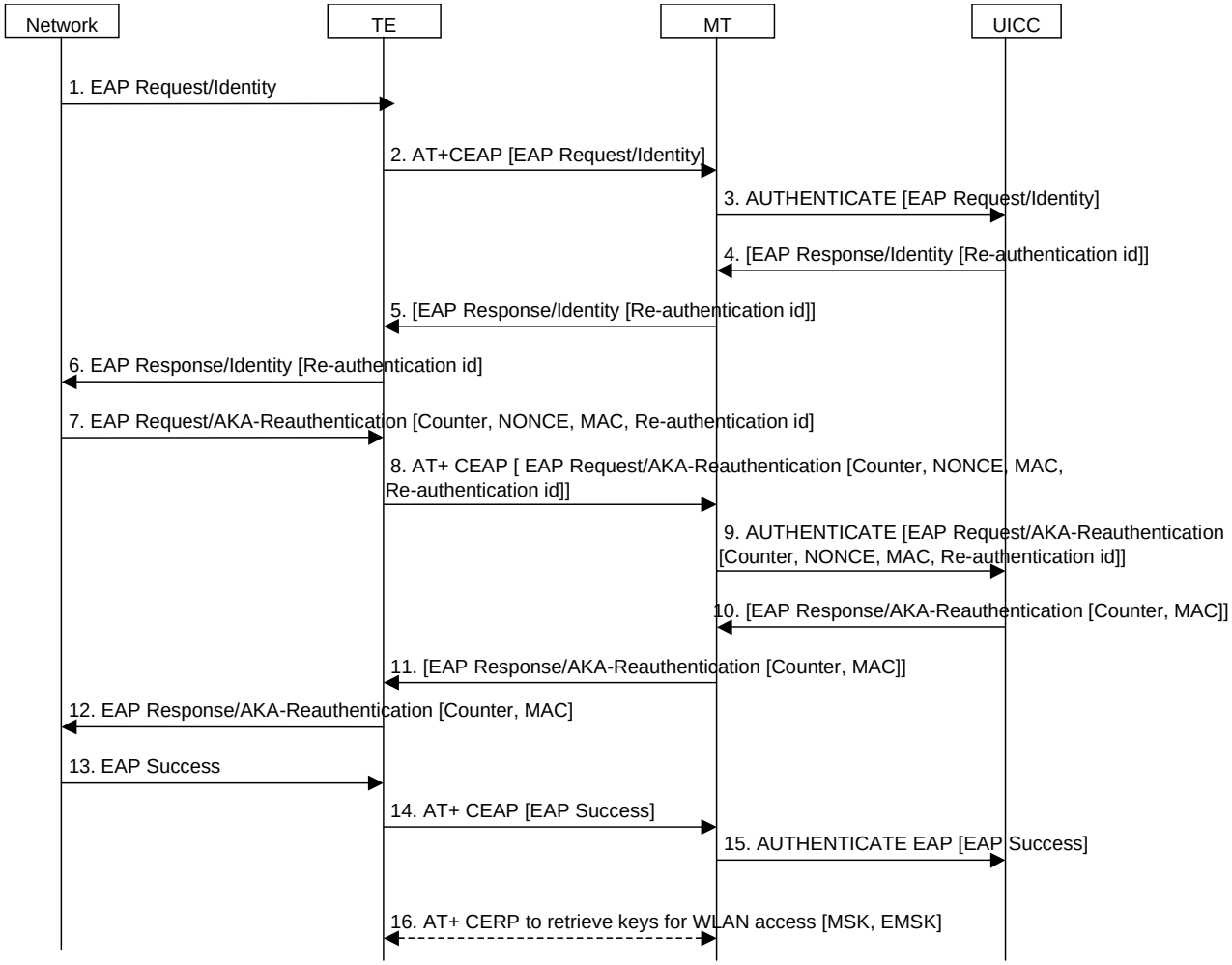


Figure 15: Fast re-authentication with EAP AKA

1. The network sends an EAP request identity message.
2. The TE sends the EAP packet received in message 1 to the UICC application USIM using +CEAP AT command.
3. The MT performs the received +CEAP AT command see TS 27.007 [40]).
4. If the UICC application received a fast re-authentication identity in the last authentication process (either full or fast), it shall reply with this fast re-authentication identity in the EAP response identity message. Consequently, the UICC application returns the EAP Response/Identity packet to the MT.
5. The MT returns the EAP Response/Identity packet to the TE, in the + CEAP AT command response data.
6. The TE sends the EAP Response/Identity packet to the network.
7. The network initiates the EAP AKA reauthentication process.
8. The TE sends the EAP packet received in message 7 to the UICC application via the MT using +CEAP AT command.
9. The MT performs the received +CEAP AT command (see TS 27.007 [40]).
10. The UICC application returns the EAP Response/AKA-Reauthentication packet to the MT.
11. The MT returns the EAP Response/AKA-Reauthentication packet to the TE, in the +CEAP AT command response data.
12. The TE sends the EAP Response/AKA-Reauthentication packet to the network, which computes the MAC of the entire received message, and comapres it with the received MAC.

13. If checks are correct, the network sends an EAP Success packet to the TE.

14. The TE sends the EAP packet received in message 13 to the UICC application using +CEAP AT command.

15. The MT performs the received +CEAP AT command (see TS 27.007 [40]).

16. After a successful EAP reauthentication, the TE shall retrieve the key material (i.e. MSK and EMSK) from EFEAPKEYS (for this purpose, the TE uses the +CERP AT command). The TE uses MSK and EMSK for security purposes, for example for WLAN link layer security.

6.7.3.2 Termination in the MT

The keys needed to protect the EAP packets are re-used from the previous full authentication process. The MSK and EMSK are calculated again using the original MK, as specified in reference [4]. For this reason, the new MSK and EMSK are transferred from the MT to the TE when the fast re-authentication process is finished. The process is shown in figure 16.

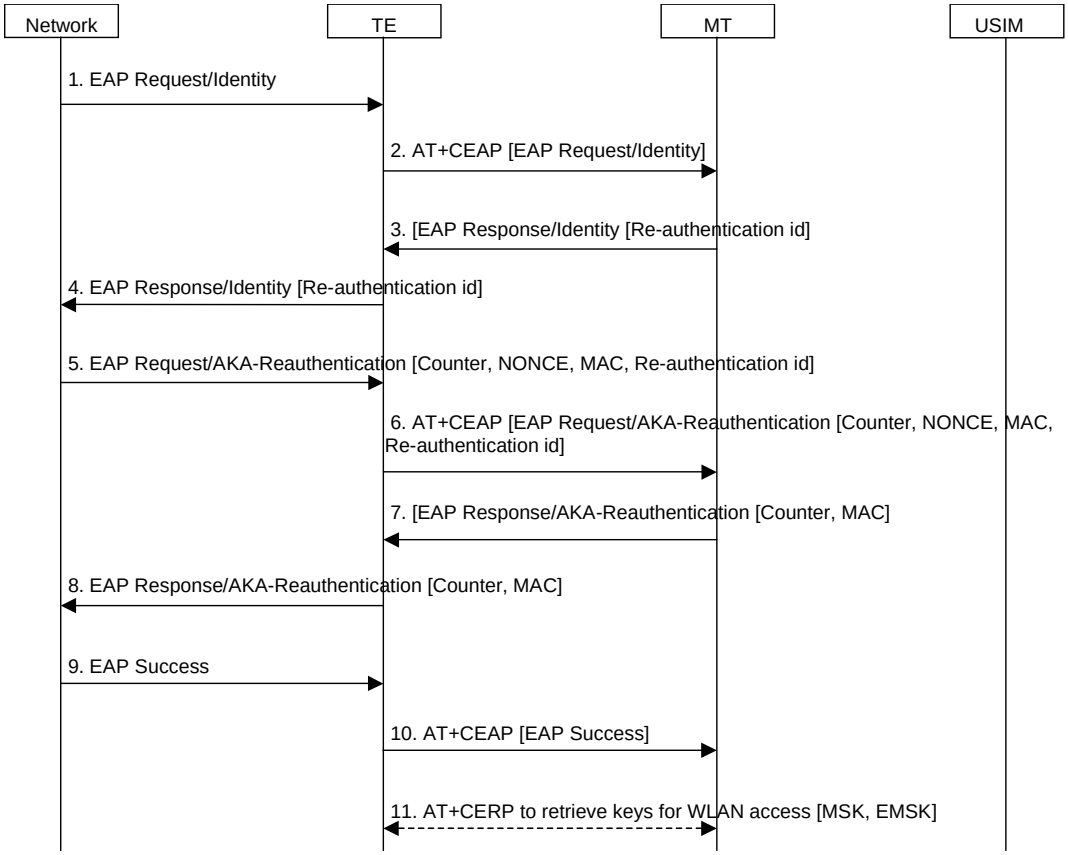


Figure 16: Fast re-authentication with EAP AKA

1. The network sends a EAP request identity message.

2. The TE sends the EAP packet received in message 1 to the MT using +CEAP AT command.

3. If the MT received a fast re-authentication identity in the last authentication process (either full or fast), it replies with this fast re-authentication identity in the EAP response identity message.

NOTE: The MT may need to access the USIM to check if there is a re-authentication id available. However, it is still to be decided whether the USIM will store the re-authentication identities.

4. The MT forwards the message to the network via the TE, using the +CEAP AT command.

5. The network sends the EAP AKA challenge with the needed parameters.

6. The TE transfers the message to the MT with the parameters, using the +CEAP AT command.

7. The MT uses the same keys as in the previous authentication process to calculate the MAC, and checks if it matches the received one. If it is correct, it calculates a new MAC and sends it in the response message to the TE with the Counter received from the network, using the +CEAP AT command.

8. The TE forwards the response message to the network.

9. The network calculates its own copy of the MAC over the received message and checks it with the received one. If it is correct, it sends a EAP success message.

10. The TE forwards the EAP success to the MT as a success indication, using the +CEAP AT command.

11. After receiving the success indication, the MT sends the new calculated MSK and EMSK and sends them to the TE, using the +CERP AT command.

6.7.4 Fast re-authentication with EAP SIM

6.7.4.1 Termination in the UICC

The keys needed to protect the EAP packets are re-used from the previous full authentication process, as in EAP AKA fast re-authentication. The MSK and EMSK are calculated again using the original MK, as specified in reference [5]. The new MSK and EMSK are transferred from the UICC application to the TE when the fast re-authentication process is finished. The process is shown in figure 17.

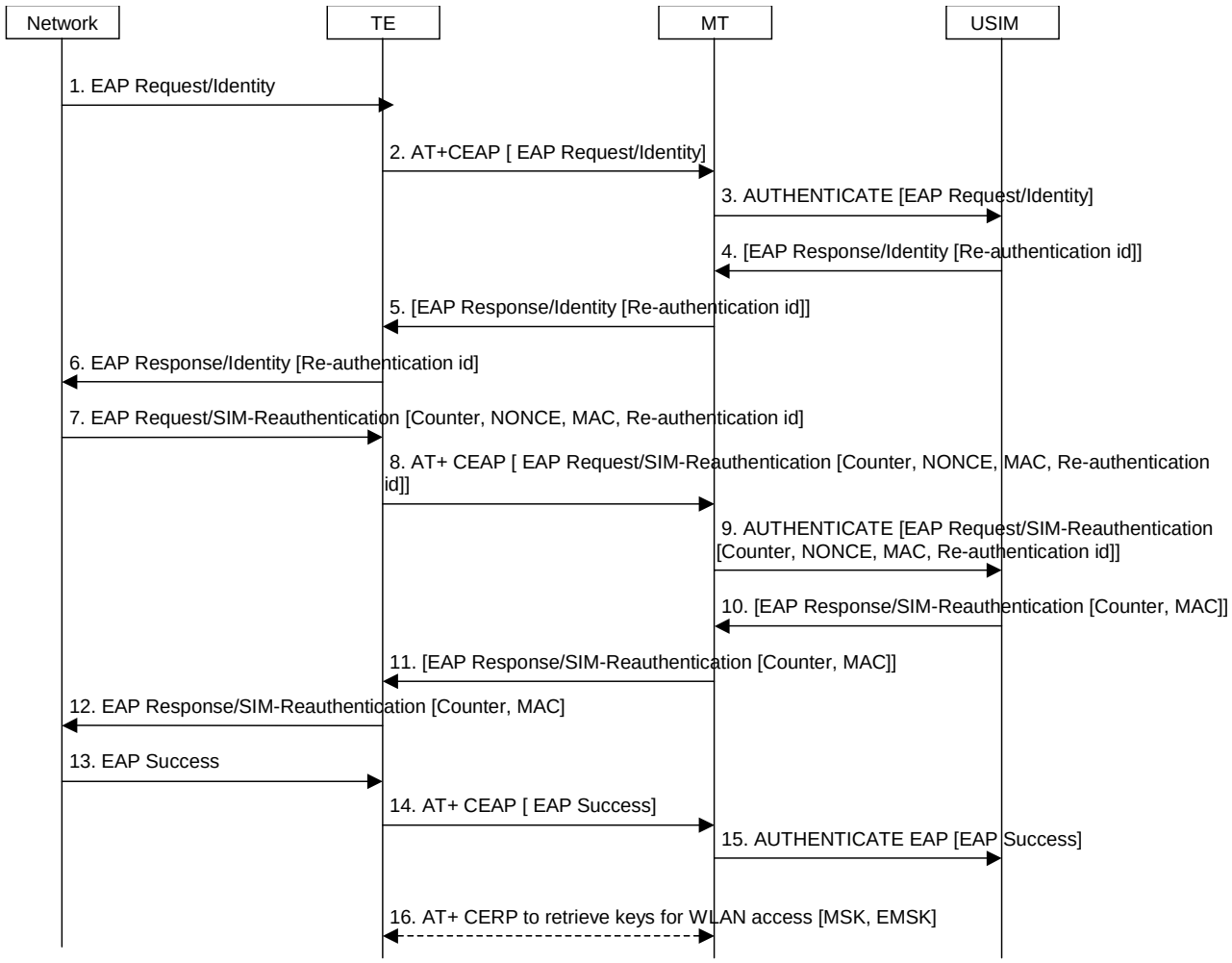


Figure 17: Fast re-authentication with EAP SIM

1. The network sends an EAP request identity message.

2. The TE sends the EAP packet received in message 1 to the UICC application using +CEAP AT command.

3. The MT performs the received +CEAP AT command (see TS 27.007 [40]).
4. If the UICC application received a fast re-authentication identity in the last authentication process (either full or fast), it shall reply with this fast re-authentication identity in the EAP response identity message. Consequently, the UICC application returns the EAP Response/Identity packet to the MT.
5. The MT returns the EAP Response/Identity packet to the TE, in the +CEAP AT command response data.
6. The TE sends the EAP Response/Identity packet to the network.
7. The network initiates the EAP SIM reauthentication process.
8. The TE sends the EAP packet received in message 7 to the UICC application via the ME using +CEAP AT command.
9. The MT performs the received +CEAP AT command (see TS 27.007 [40]).
10. The UICC application returns the EAP Response/SIM-Reauthentication packet to the MT.
11. The MT returns the EAP Response/SIM-Reauthentication packet to the TE, in the +CEAP AT command response data.
12. The TE sends the EAP Response/SIM-Reauthentication packet to the network, which computes the MAC of the entire received message, and compares it with the received MAC.
13. If checks are correct, the network sends an EAP Success packet to the TE.
14. The TE sends the EAP packet received in message 13 to the UICC application using +CEAP AT command.
15. The MT performs the received +CEAP AT command (see TS 27.007 [40]).
16. After a successful EAP reauthentication, the TE shall retrieve the key material (i.e. MSK and EMSK) from EFEAPKEYS (for this purpose, the TE uses the +CERP AT command). The TE uses MSK and EMSK for security purposes, for example for WLAN link layer security.

6.7.4.2 Termination in the MT

The keys needed to protect the EAP packets are re-used from the previous full authentication process, as in EAP AKA fast re-authentication. The MSK and EMSK are calculated again using the original MK, as specified in ref. [5]. The new MSK and EMSK are transferred from the MT to the TE when the fast re-authentication process is finished. The process is shown in figure 18.

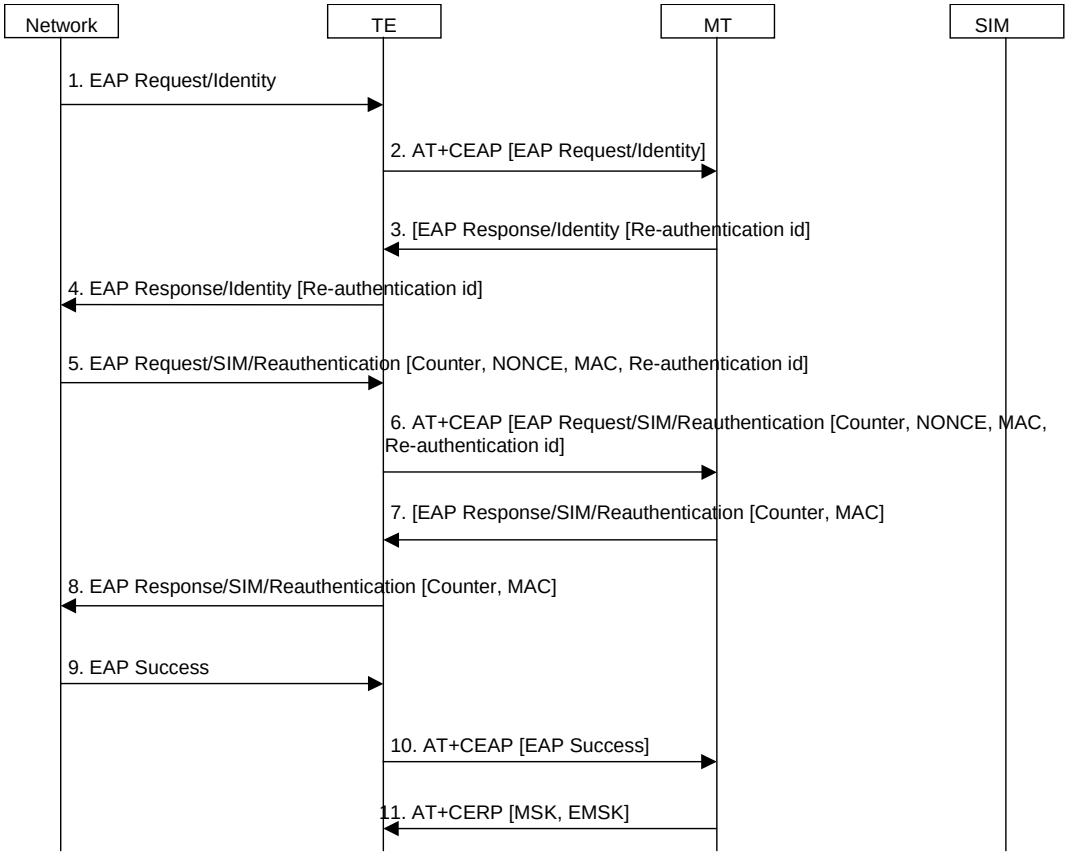


Figure 18: Fast re-authentication with EAP SIM

1. The network sends a EAP request identity message.
2. The TE sends the EAP packet received in message 1 to the MT using the +CEAP AT command.
3. If the MT received a fast re-authentication identity in the last authentication process (either full or fast), it replies to the TE with this fast re-authentication identity in the EAP response identity message, using the +CEAP AT command.

NOTE: the MT may need to access the USIM to check if there is a re-authentication id available. However, it is still to be decided whether the USIM will store the re-authentication identities.

4. The TE forwards the message to the network.
5. The network sends the EAP AKA challenge with the needed parameters.
6. The TE transfers the message to the MT with the parameters, using the +CEAP AT command.
7. The MT uses the same keys as in the previous authentication process to calculate the MAC, and checks if it matches the received one. If it is correct, it calculates a new MAC and sends it in the response message to the TE with the Counter received from the network, using the +CEAP AT command.
8. The TE forwards the response message to the network.
9. The network calculates its own copy of the MAC over the received message and checks it with the received one. If it is correct, it sends a EAP success message.
10. The TE forwards the EAP success to the MT as a success indication, using the +CEAP AT command.
11. After receiving the success indication, the MT sends the new calculated MSK and EMSK and sends them to the TE, using the +CERP AT command.

Annex A (informative): Review of the security of existing WLAN-related technologies

A.1 IEEE

A.1.1 IEEE 802 Project

IEEE Project 802 develops LAN and MAN standards, mainly for the lowest 2 layers of the OSI Reference Model. IEEE 802.11 is the Wireless LAN Working Group (WG) within Project 802. The existing 802.11 standard with amendments are:

- 802.11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.
- 802.11a High-speed Physical Layer in the 5 GHz Band.
- 802.11b Higher-Speed Physical Layer Extension in the 2.4 GHz Band.
- 802.11d Specification for operation in additional regulatory domains.

Currently there are a number of Task Groups (TG) in the 802.11 WG that each work on new amendments to the standard:

- 802.11e Medium Access Control (MAC) Enhancements for Quality of Service (QoS).
- 802.11f Inter Access Point Protocol (IAPP). (A recommended practice, not a standard).
- 802.11g Higher-Speed Physical Layer Extension in the 2.4 GHz Band.
- 802.11h Spectrum and Power Management extensions in the 5 GHz band in Europe.
- 802.11i Specification for Enhanced Security.

Membership in IEEE 802.11 is individual (i.e. not based on company) and anyone that has been present at a certain number of meetings becomes member in the WG. Membership is required in order to get voting rights and all members have one vote (again, votes are not company based).

A.1.2 Authentication

Legacy 802.11 authentication

The 802.11-1999 authentication mechanism works at the data link layer (MAC layer). Two authentication methods exist, open system authentication and shared key authentication. Open system authentication is in principle a null authentication scheme and accepts anyone that requests authentication.

Shared key authentication is a challenge-response authentication based on a shared secret. The mobile station sends an Authentication request to the Access Point (AP). The Access Point sends a chosen plaintext string to the station and the station responds with the WEP-encrypted string. (See below for more details on WEP). If the string is correctly encrypted the AP sends an Authentication message to the station to indicate that the authentication was successful. The standard allows for up to four keys in a cell but in practice all communication parties in the cell share the same secret. Note that the authentication is not mutual, only the mobile terminals are authenticated. Shared key authentication is very weak. An attacker that listens to a successful authentication exchange will have all elements that are needed to successfully perform an authentication of his/her own, even if the shared key is unknown. Today shared key authentication is not considered useful.

IEEE 802.1X and EAP

The 802.11i Task Group (TGi) within IEEE is working on enhancements to the 802.11 security IEEE Std 802.11i [6]. It has been decided to use IEEE 802.1X as the authentication framework IEEE P802.1X [19]. IEEE 802.1X in turn uses the Extensible Authentication Protocol (EAP) that allows for end-to-end mutual authentication between a Mobile Station and an Authentication Server (see ref. [3]). Thus, even though 802.11i still performs access control on layer 2, the authentication message exchange is not restricted to the MAC layer but uses other IEEE standard as well as IETF standards.

IEEE 802.1X is a standard for port-based access control. IEEE 802.1X can be described to lie between the MAC layer and higher layers and takes care of filtering of frames to/from non-authenticated stations. Before authentication is completed only EAP-traffic is allowed to pass. This allows an authentication exchange to cross the Access Point before general data is allowed to pass. When the 802.1X entity in the Access Point (AP) is informed that a mobile station has successfully authenticated, the AP starts to forward data packets to/from that station.

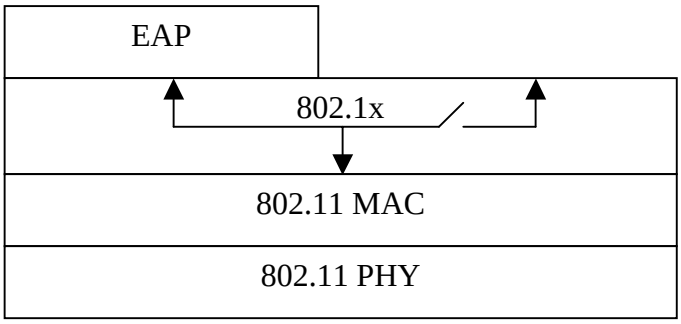


Figure A.1: IEEE 802.1X in part of protocol stack in Access Point or mobile station. EAP messages are always accepted while other packets are filtered based on authentication status

EAP allows for end-to-end authentication between a Mobile Station and an Authentication Server (AS). EAP is a generic protocol that allows different authentication mechanisms (called EAP methods) to be transported. EAP has a general part that describes the general packet format and header content. Each EAP method then has a more specific description for how the actual authentication mechanism is carried by the EAP packets. The EAP packets can then be transported over different protocols. In 802.1X a special frame format called EAP over LAN (EAPOL) is defined for sending EAP messages over 802 links. This allows EAP messages to be sent over the LAN before higher layer protocols, e.g. IP, have been initiated. Between the Access Point (AP) and the AS, EAP messages are typically encapsulated in an AAA protocol, e.g. in RADIUS or DIAMETER (see figure A.2). It is out of the scope of 802.11i to specify a certain AAA protocol. IEEE 802.11i can in principle also be used without AAA protocol if the EAP method is implemented in the AP.

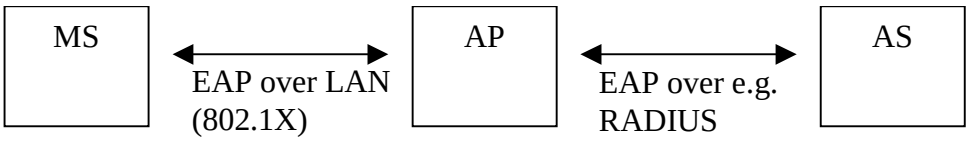


Figure A.2: Example of end-to-end authentication using EAP

Examples of EAP methods (RFCs or Internet Drafts) are:

- EAP-SIM for SIM-based authentication. (Internet Draft) (ref. [5]);
- EAP-AKA for SIM and USIM-based authentication (Internet Draft) (ref. [4]);
- EAP-TLS for certificate-based authentication (RFC) [EAP-TLS] (RFC 2716 [7]).

The actual EAP authentication takes place between the MS and the AS and is in principle transparent to the AP. The AP only has to forward EAP messages: EAPOL-encapsulated on the wireless side and e.g. RADIUS-encapsulated on the wired side. If authentication is successful, the AS sends a RADIUS-Access Accept message to the AP (in the case RADIUS is used as AAA protocol). The AP then knows that the MS has been authenticated and can start forwarding traffic to/from the MS. After reception of the Access-Accept message from the AS, the AP sends an EAP-Success message to the MS (see figure A.3).

Key management

To use an EAP method with 802.11i it is required that a 256-bit master key is established as part of the authentication process. Many EAP methods generate key material as part of the authentication (e.g. EAP-SIM, EAP-AKA, EAP-TLS) but the exact way in which the master key is generated depends on the EAP method and is outside the scope of 802.11i. After the EAP authentication is finished, both the MS and the AS will know the master key. If RADIUS is used, the AS then sends the master key to the AP as an attribute in the RADIUS-Access Accept message. The MS and AP use the master key to derive session keys for encryption and integrity protection, as specified in 802.11i. This provides unique unicast keys for each MS-AP association.

The broadcast/multicast key in a cell is generated by the AP and sent in an EAPOL-Key message (defined in 802.1X) to each station. To protect the broadcast/multicast key the EAPOL packet is encrypted with TKIP or AES (see below) using the unicast key. The AP can in principle update the broadcast/multicast key any time, e.g. when a MS leaves the cell.

It shall also be possible to use a pre-shared key instead of the EAP master key material.

Message exchange (example with RADIUS)

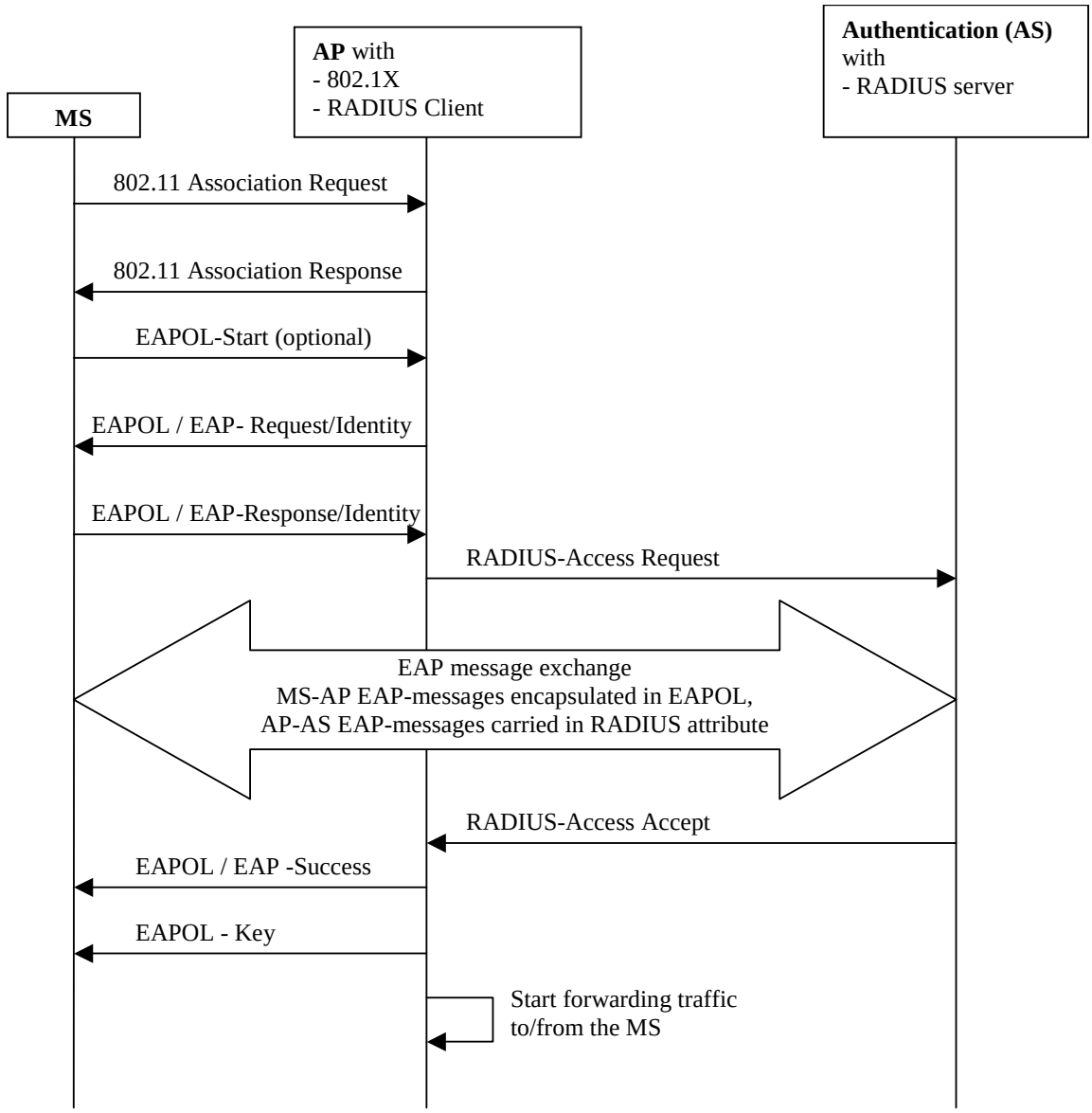


Figure A.3: General EAP authentication with 802.11i and RADIUS as AAA protocol

A.1.3 Encryption and integrity protection

The air-link protection in IEEE 802.11 occurs in the MAC layer. This means that all layer-2 data frames, including LAN broadcasts, are protected. The 802.11-1999 standard specifies the Wired Equivalent Privacy (WEP) for encryption and integrity protection. The 802.11i task group is specifying two new encryption/integrity-protection protocols, the Temporal Key Integrity Protocol (TKIP) and the CTR with CBC-MAC Protocol (CCMP). The 802.1X/EAP authentication mechanism can in principle be used with any of the three encryption protocols but configuration can restrict the number of allowed encryption protocols in a cell.

In order to be backwards compatible, an 802.11i-capable cell could support several encryption protocols simultaneously. For example, to support legacy stations a manually configured shared WEP key may need to be used for those stations. This key will then also be used as broadcast/multicast key for 802.11i-capable stations that instead use unique pair-wise keys for unicast traffic.

WEP

The IEEE 802.11-1999 Standard specified the Wireless Equivalent Privacy (WEP). WEP uses RC4 with a 40-bit key and 24-bit initialisation vector (IV) for encryption. RC4 is a stream cipher where a seed is used as input to the RC4 PRNG, which produces an output bit string, that is XOR'ed with the plaintext to produce the ciphertext. For WEP the seed to the RC4 PRNG is the key concatenated with the IV. The key is shared between the communicating parties and the IV is transmitted in clear text in each packet. Message integrity is provided using a CRC checksum that is added to the payload and then encrypted together with the rest of the payload. WEP does not protect against replay.

Since the publication of the standard, several shortcomings of WEP have been discovered. Attacks to retrieve the WEP key and to modify the payload have been described. One weakness is the seed derivation. With RC4 it is important that each packet has a different RC4 seed. The RC4 seed in 802.11-1999 is constructed by concatenating the IV and the 40-bit key but the standard did not contain specifications to ensure uniqueness of <key,IV> pairs.

Today, WEP is not considered useful.

TKIP

The Temporal Key Integrity Protocol (TKIP) is a new protocol that will fix the known problems with WEP. TKIP uses the same ciphering kernel as WEP (RC4) but adds a number of functions:

- 128-bit encryption key;
- 48-bit Initialisation Vector;
- New Message Integrity Code (MIC);
- Initialisation Vector (IV) sequencing rules;
- Per-packet key mixing algorithm that provides a RC4 seed for each packet;
- Active countermeasures.

The purpose of TKIP is to provide a fix for WEP for existing 802.11b products. It is believed that essentially all existing 802.11b products can be software-upgraded with TKIP (all major 802.11 vendors participate in the 802.11i standardisation).

The TKIP MIC was designed with the constraint that it must run on existing 802.11 hardware. It does not offer very strong protection but was considered the best that could be achieved with the majority of legacy hardware. It is based on an algorithm called Michael that is a 64-bit MIC with 20-bit design strength. Details can be found in IEEE Std 802.11i [6].

The IV sequence is implemented as a monotonically incrementing counter that is unique for each key. This makes sure that each packet is encrypted with a unique <key, IV> pair, i.e. that an IV is not reused for the same key. The receiver shall also use the sequence counter to detect replay attacks. Since frames may arrive out of order due to traffic-class priority values, a replay window (16 packets) has to be used.

A number of "weak" RC4 keys have been identified for which knowledge of a few number of RC4 seed bits makes it possible to determine the initial RC4 output bits to a non-negligible probability. This makes it easier to crypto analyse data encrypted under these keys. The per-packet mixing function is designed to defeat weak-key attacks. In WEP, the IV and the key are concatenated and then used as seed to RC4. In TKIP, the cryptographic per-packet mixing function

combines the key and the IV into a seed for RC4.
Because the TKIP MIC is relatively weak, TKIP uses countermeasures to compensate for this. If the receiver detects a MIC failure, the current encryption and integrity protection keys shall not be used again. To allow a follow-up by a system administrator the event shall be logged. The rate of MIC failure must also be kept below one per minute, which means that new keys shall not be generated if the last key update due to a MIC failure occurred less than a minute ago. In order to minimize the risk of false alarms, the MIC shall be verified after the CRC, IV and other checks have been performed.

TKIP is an interim solution to support 802.11i on legacy hardware. It is not considered as secure as the AES solution (CCMP) but very much better than WEP.

CCMP(AES)

Advanced Encryption Standard (AES) is a block cipher that can be used in different modes of operation. CCM is a mode of operation of AES that consists of Conter mode (CTR) for confidentiality and CBC-MAC mode for authentication and integrity. In 802.11i, CCMP is adopted as the long term solution. CCM based on AES can provide robust encryption and message integrity.

The AES implementation requires hardware support and the majority of legacy 802.11b products will thus not be able to run CCMP.

A.2 ETSI/BRAN

A.2.1 HIPERLAN/2 Security architecture

The BRAN Hiperlan/2 (references [9], [10], [11] and [12]) protocol stack consists of a physical layer at the bottom, a DLC layer in the middle, which includes the RLC sub-layer and the convergence layer(s) at the top. The RLC sub-layer is responsible for Radio Resource Control, Association Control and Data Link Control Connection Control. The DLC take cares of error control. Between the RLC and the DLC is the Medium Access Control located per instance of AP, cf. the two figures below.

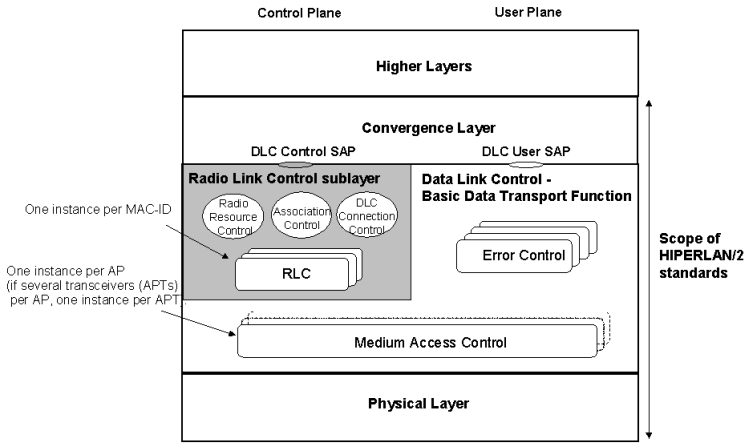


Figure A.4: Protocol stack in the AP/CC

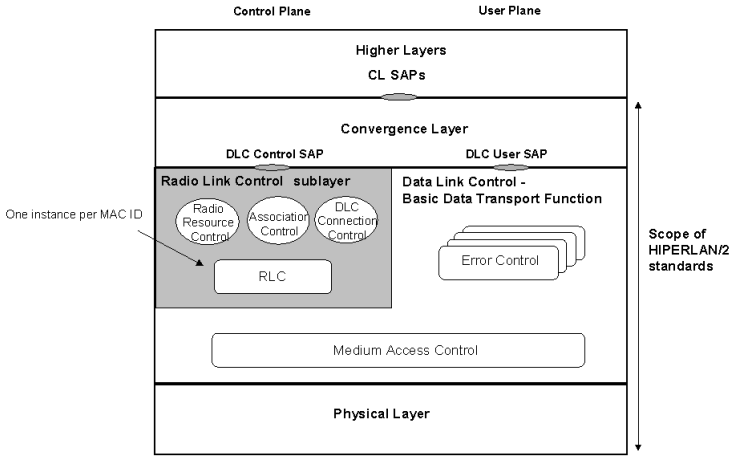


Figure A.5: Protocol stack in the MT

An AP is a device responsible for the centralized control of the resources in a radio cell and is in the most cases connected to a fixed network. A CC is a device that that provides with the same functionality as an AP but is not necessarily connected to a fixed network. The term CC is normally used when the central controller and the MT functionality is located in single device.

The Association Control Function performs 1) encryption startup, 2) authentication and 3) DM Common Key Distribution (OMT/OAP) in that order, see figure below.

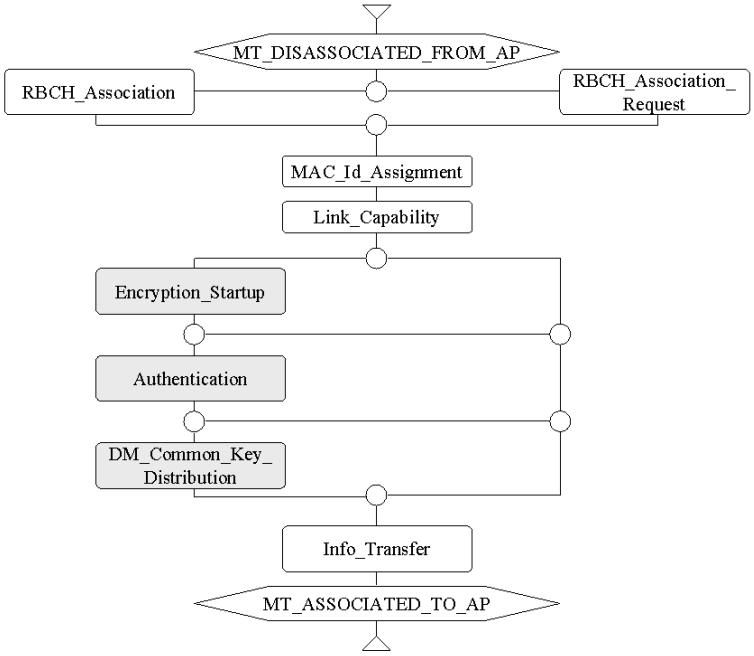


Figure A.6: The Association Control Function

A.2.1.1 Confidentiality protection

Confidentiality protection is provided for user data and part of RLC signalling. The protection can be provided between:

1 MT and AP/CC;

2 MT and MT (note that the AP has to be trusted).

The following algorithms are defined for confidentiality protection:

1 No-encryption;

2 DES, Data Encryption Standard;

3 Triple-DES (Optional).

A.2.1.2 Authentication

The authentication mechanism provides mutual authentication between the MT and the AP. If the authentication of the MT is successful then access to the connected fixed network is granted. It is the policy of the operator that decides whether authentication of the MT is necessary or not for access.

The authentication of the AP allows the MT to cancel an access attempt if the AP cannot be proven to be authentic. The mechanism allows the MT to detect false AP. The authentication protocol is a challenge-response protocol.

Three protocols are defined, based on:

1. Pre-shared keys:
   - A pre-shared key shall be at least 128 bits.
2. RSA signatures:
   - Three lengths are supported: 512, 768 and 1024 bits (OAP/OMT).
3. No Authentication.

How the keys for the authentication is generated, configured, stored and fetched is out of the scope of the Hiperlan/2 standard.

Each MT will be assigned an authentication key identifier (AKI). The AKI will be sent to the AP with which the MT has a Security Association. There are six different types that can be used:

1. 48-bit IEEE address;
2. 64-bit extended IEEE address.
3. A NAI, Network Access Identifier;
4. Distinguished name;
5. Compressed type, which is used when an available AKI is too long to be carried in the RLC messages;
6. Generic type, which is a non-structured octet string.

A.2.1.3 Integrity protection

No integrity mechanism is defined for HIPERLAN/2.

A.2.2 Security mechanisms

A.2.2.1 Confidentiality

Confidentiality protection can be used for Unicast, Multicast and Broadcast scenarios. In order to have Multicast and/or Broadcast confidentiality protection a Unicast encryption has to be established first. The Unicast encryption is optional to use.

The algorithms defined for confidentiality protection are:

- DES which is mandatory to implement for AP/CC and MT;
- Triple-DES (EDE mode), which is optional to implement for AP/CC and MT.

It is possible to provide confidentiality protection for the User Data Channel, User Multicast Channel, User Broadcast Channel, the Dedicated Control Channel and all LCH PDUs except the downlink RLC Broadcast Channel since it has to reach all MT's. The encryption/decryption mechanism is visualized in the figure below.

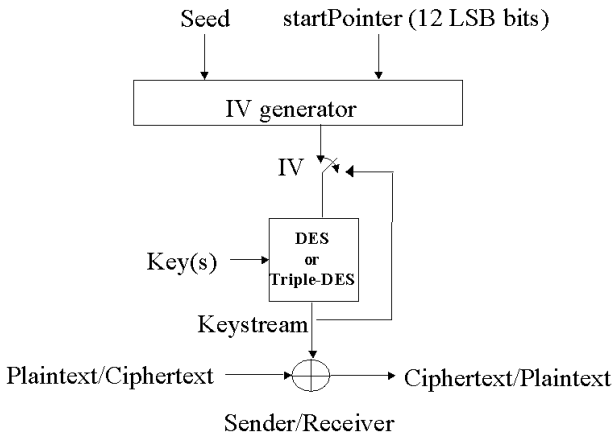


Figure A.7: The encryption/decryption function

Unicast

A Unicast security association is defined between a MT and an AP.

Calculate a Session Secret Key (SSK).

During an Encryption Startup both the MT and the AP calculate a public Diffie-Hellman value and send it to the other party.

This material is used at both sides to calculate an SSK.

Assume that the MT sends gx mod n and the AP sends gy mod n where:

g=2 the generator of the group;

n=2768-2704-1+264 *{ [2638pi] + 149686 }, First Oakley Group 1 (768 bit prime).

The AP and the MT now have a shared secret: gxy mod n, which is the basis for calculating the Session Secret Key.

DES

DES is mandatory to implement.

SSK is defined as the most significant 8 octets defined from KeyMat where:

1. KeyMat=HMAC-MD5(gxy mod n, 0x00)
2. KeyMat=HMAC-MD5(gxy mod n, 0x01)
3. KeyMat=HMAC-MD5(gxy mod n, 0x02)
4. etc.

This process ends when the SSK is found to be a non-weak and a non-semi-weak DES key.

Triple-DES

Triple-DES is optional to implement.

SSK is for this case defined as three keys k1, k2 and k3 where k1 is taken from KeyMat=K1|K2 as the most significant 8 octets, k2 as the next 8 octets and k3 as the following 8 octets where:

1. K1= HMAC-MD5(gxy mod n, 0x00) & K2= HMAC-MD5(gxy mod n, K1|0x00);
2. K1= HMAC-MD5(gxy mod n, 0x01) & K2= HMAC-MD5(gxy mod n, K1|0x01);
3. K1= HMAC-MD5(gxy mod n, 0x02) & K2= HMAC-MD5(gxy mod n, K1|0x02);
4. etc.

Until all three keys k1, k2 and k3 are unequal and that all of them are non-weak and non-semi-weak DES keys.

Multicast and Broadcast

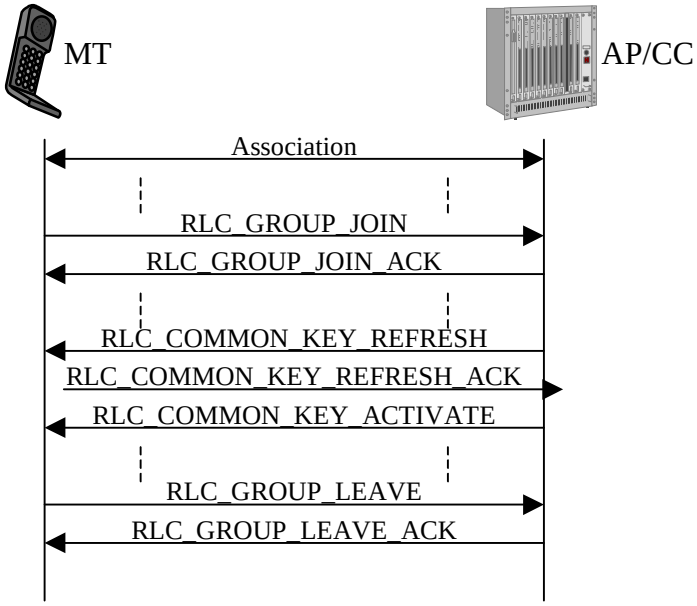


Figure A.8: A Multicast example

To join a broadcast or multicast group, the MT must first be associated with an AP/CC. There are two ways of implementing multicast:

- Using multicast MAC ID and transmitting the information once to the multicast group over the air;
- Using n times unicast, i.e. transmitting the information individually to each member of the group.

The figure above describes a scenario where the MT joins a multicast group. The MT begins with sending a join-message, to indicate what group(s) it would like to join. In this message it also specifies what encryption algorithms it supports or would like to use. The AP/CC response consists of an acknowledgment, which includes the encryption algorithm and encryption key to be used for the group(s). The AP/CC is responsible for handling the key refresh. When a MT wishes to leave a group it sends a group-leave request to the AP/CC, which the AP/CC must acknowledge.

For the broadcast scenario, similar join and leave procedures apply for the MT, as in the multicast case. Instead of sending an RLC_GROUP_JOIN request the MT sends an RLC_CL_BROADCAST_JOIN request.

Direct Link Scenario

In a direct link connection, two mobile terminals set up a direct communication channel between themselves. The data will be sent directly between the terminal, while the AP/CC still handles the control functions (see figure below). Note that when direct link is not used between two parties, all traffic must go via the AP/CC. Therefore, the direct link is a feature that helps to off-load the AP/CC, so not all traffic have to be routed through it.

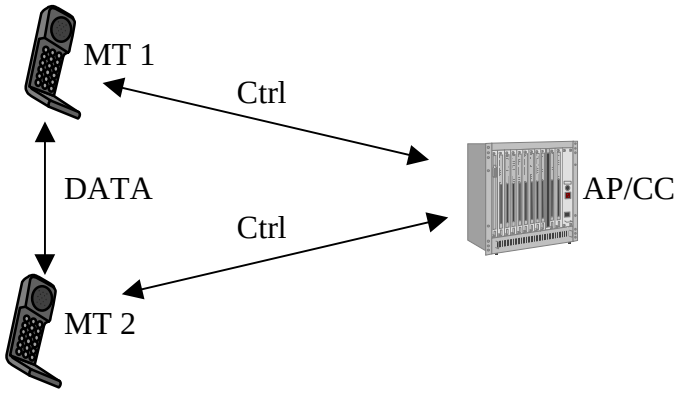


Figure A.9: The data and control flow in a direct link scenario

The figure above describes a small scenario where the AP/CC initiates a Direct Link Setup. Both terminals must be associated with the AP/CC before this can be done. The AP/CC initiates by sending the RLC_DM_SETUP message, which include information about the peer's MAC id, common attributes etc. The AP/CC is responsible for distributing a common encryption key to the terminals and also for handling (when needed) the key refresh. To synchronize the two terminals, the AP/CC sends the RLC_DM_CONNECT_COMPLETE message.

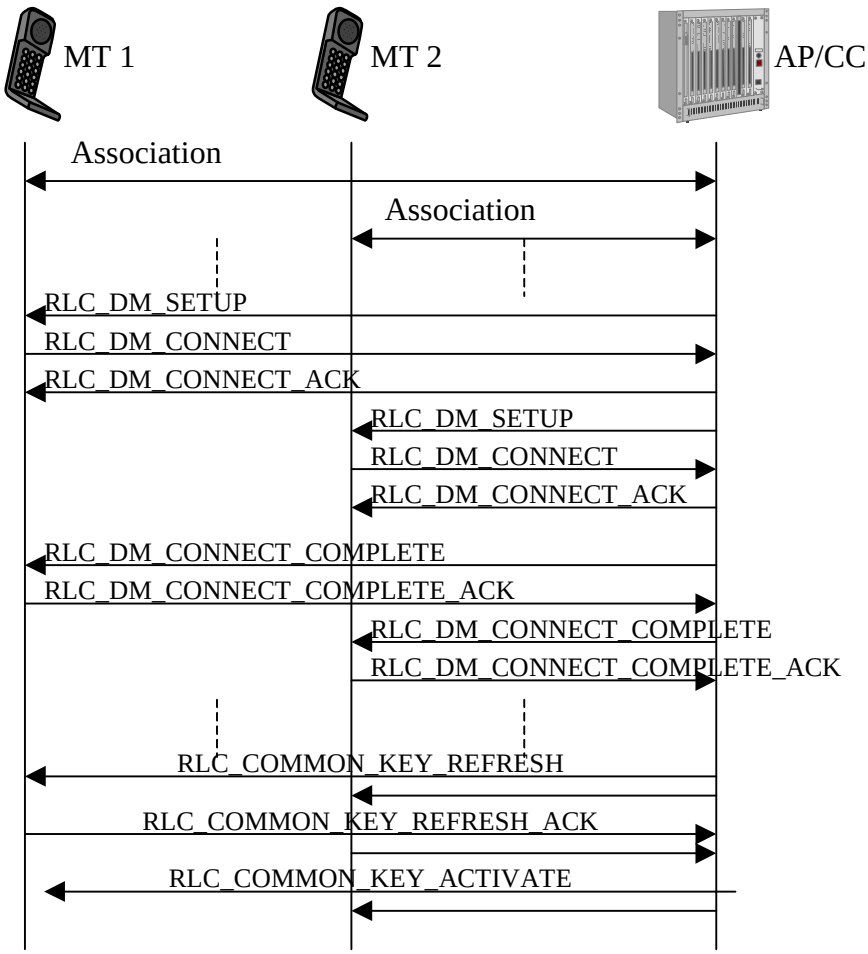


Figure A.10: AP/CC Initiated DiL setup with key refresh

A.2.2.2 Authentication

When encryption has been activated the mechanism for mutual authentication can start. Authentication with a pre-shared key is mandatory to implement and RSA based signatures are optional to implement. There are six different key identifiers and one of them is mandatory to be implement but since all of them are optional it is a choice to choose one of them. The MT fetches the authentication key of the AP based on identities that are sent over the broadcast channels.

The MT sends a RLC_AUTHENTICATION including the type of the AKI. Upon receiving this message the AP sends a challenge to the MT. The MT calculates the response and creates a challenge to the AP. The MT sends a RLC_AUTHENTICATION_AP to the AP including the response and the challenge. The AP checks the response and it is equals the expected response the AP sends a RLC_AUTHENTICATION_ACK including the response based on the challenge sent by the MT. The MT checks the response if it is a valid one i.e. if the AP is authentic.

Since the Diffie-Hellman exchange is vulnerable to a man-in-the-middle attack this mutual authentication mechanism prevents this attack. Furthermore the proposed and selected encryption and authentication alternative is checked to prevent an attack aiming for a lower security level than requested.

The challenge response protocol is based on a good random number generator but there is no random generator specified in the standards so it is implementation specific.

Pre-shared key

The keys have to be distributed to the MTs and the APs in a secure manner. It is suggested in the standard to use this key management to business and residential environment for scalability reasons.

The responses are calculated as:

Response=HMAC-MD5(Preshared Key, AuthenticationString)

AuthenticationString = challenge [| mt_dh | ap_dh |] auth_encryption_list | auth_encr_selected

The AuthenticationString shall include the received challenge, the proposed encryption and authentication algorithms proposed by the MT and the selected encryption and authentication algorithms selected by the AP. If encryption is chosen, i.e. Encryption Startup preceded the Authentication, then the received Diffie-Hellman public value and the sent Diffie-Hellman public value shall also be included in the AuthenticationString. The challenge is 128 bit long and the Diffie-Hellman public value is 768 bit long. The length of the pre-shared keys shall be at least 128 bit long.

RSA-based

It is suggested in the standard that a public-key certificate signed by a trusted party is an efficient way to implement this system. A PKI, Public Key Infrastructure, is needed to issue, verify and revoke public-key certificates. The signature and the verification shall be calculated by using PKCS#1 and the MD5 hash algorithm. The response is calculated as:

Response=RSASSA_PKCS_V1_5_SIGN(Private Key, AuthenticationString)

The AuthenticationString is specified in the same way as for the pre-shared key case. There are three public key lengths specified: 512, 768 and 1024 bits.

A.3 IETF

A.3.1 Key Generation and EAP Methods

Reference [27] discusses the security aspects of EAP methods generating keys, distributing them to access points via AAA protocols such as Diameter EAP [23], and using them in establishing link-layer security

A.3.2 Co-Existence of RADIUS and Diameter

While Diameter does not share a common protocol data unit (PDU) with RADIUS [15], considerable effort has been expended in enabling backward compatibility with RADIUS, so that the two protocols may be deployed in the same network. Initially, it is expected that Diameter will be deployed within new network devices, as well as within gateways enabling communication between legacy RADIUS devices and servers. This capability, described in [23], enables Diameter support to be added to legacy networks, by addition of a gateway or proxy speaking both RADIUS EAP [15], [26] and Diameter EAP [23], [24].

RADIUS is currently widely used protocol in WLAN environments. At the same time RADIUS is missing several features, such as server initiated messages and may not operate with the highest possible security turned on. Diameter is a better protocol, but it is not very widely deployed yet. Therefore, gradual migration from RADIUS to Diameter seems to be one potential way to go further.

It seems reasonable to start from an initial model of the AAA network where most or all of the access points implement only RADIUS, and a core which uses Diameter but is capable of talking to the RADIUS-only capable access points. This would mean that leaf AAA proxies should support both RADIUS and Diameter. As Diameter-capable access points are inserted to the network, they can be taken into use immediately. An advantage of placing the RADIUS/Diameter-capable nodes on the leafs of the network is that it becomes easier to take advantage of the features found in Diameter. For instance, even accounting may be more reliable if only the first hop is run in RADIUS but the traversal of the access provider, roaming consortium, and home operator proxies is done via DIAMETER.

The actual translation gateway must be able to run both RADIUS and Diameter protocols. The [24] extension defines a framework for the protocol conversion, where the RADIUS attribute space is included into Diameter, which eliminates the need to perform many attribute translations. However, some explicit translations between RADIUS and Diameter attributes must be made, like translating vendor specific and accounting information.

Some Diameter related messages cannot be translated during the communication with RADIUS client, such as messages initiated by Diameter server. Interoperability between RADIUS and DIAMETER in the presence of some of the non-standard RADIUS extensions has not been specified.

The gateway needs to add RADIUS application layer security mechanisms towards RADIUS, and IPSec or TLS towards Diameter. Given the use of the hop-by-hop security mechanisms, this translation can be performed without the knowledge of the original sender of the message. RADIUS requires pre-shared keys, while Diameter can take advantage of either IKE or TLS.

In addition, the translation gateway must secure attribute data towards the home server using Diameter CMS techniques (when the RFC is published). That is, end-to-end security mechanisms can be employed between the translation proxy and the home server, but not between the RADIUS-only access point and the translation proxy.

Diameter – RADIUS compatibility mode should support both protocols along with the necessary translation mechanisms in order to enable the use of RADIUS-only access points. Such translation should occur as near the leaves of the network as possible. As not all functions can be translated in full, some loss of functionality occurs for those devices, which use RADIUS.

It is possible to use IPSec in those cases where RADIUS is used, as currently required in RFC 2869bis. This may help to eliminate some of the vulnerabilities of RADIUS. In addition, 3GPP may adopt the use of RFC 2869bis and corresponding Diameter counterpart as the standard for running EAP over AAA protocols.

A.4 Bluetooth

Text to be added.

Annex B (informative): Trust Model

B.1 Trust model entities

Although any real implementation of a trusted access solution will depend on the exact system architecture, for the high-level concepts presented in this contribution we restrict attention to the three key players: the user/customer, the cellular operator, and the WLAN access provider.

Figure B.1 shows a simplified system model showing only the three roles and their trust relationships.

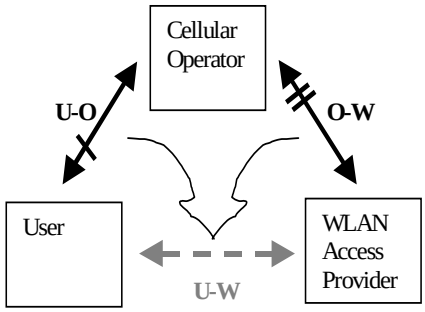


Figure B.1: Trust model

The cellular operator offers GSM/GPRS/UMTS services. Architecture-wise, the "cellular operator" box represents the complete cellular network (including radio access network, core network, service network), and also extends to partners in a roaming consortium.

The WLAN access provider offers public Wireless LAN access as a service. The "WLAN Access Provider" box in the figure groups the WLAN access network and its possible supporting nodes. The WLAN access provider may be "part of" (owned by) the cellular operator or a cellular roaming partner, or it could be a WLAN-only access provider or Wireless ISP.

The user in this model is assumed to be a subscriber/customer of the cellular operator who wishes to use both the traditional cellular services and the complementary (but not complimentary) WLAN access, when available. As such, the user is assumed to operate equipment capable of both GPRS/UMTS and WLAN access. This could be some combination of a phone (handset or PC-card) and a laptop / PDA, or possibly a combined WLAN/GPRS terminal. The collection of a user's devices acting on behalf of the user will often be called a client.

Legally, the user-operator trust relation, labelled "U-O" in figure B.1, is based on the service agreement between these two parties. From a technological perspective, this trust is embodied in a shared secret stored securely both on the user's (U)SIM and at the operator's Authentication Centre, and allows for an authenticated secure connection between the user's terminal and the cellular network.

If the cellular operator and the WLAN access provider are part of the same legal entity their trust relation is self-evident, and results in an intra-domain security solution. In the more general case, the operator-WLAN trust, labelled O-W in figure B.1, is based on roaming agreements or other partnerships (such as a Single Sign-On federation). Physically, this trust can translate to a security solution for roaming, AAA, trusted or semi-trusted servers in the context of WAP, or SMS-gateway access.

B.2 Trust relations

To design or evaluate a security solution, the trust relations between the participants must be identified. In a public WLAN access scenario, we have one or more operators and (possibly independent) access providers, and several subscribers.

The subscribers cannot trust each other. Someone else accessing the network from the same WLAN access network as the user, may be trying to perform DoS attacks targeted at the user, or eavesdrop on his traffic, steal his credentials to gain access at a later time, etc.

An operator cannot trust any mobile terminal that tries to connect to the network. Before authentication, the mobile station could belong to anyone, with or without a subscription. Even after a mobile station has been authenticated, the device may act maliciously. The user himself may be performing fiendish activities, or someone else may have hijacked his session.

The operators and/or access providers may choose to trust each other. Such trust relations normally rely on (legally binding) roaming agreements. If such an agreement is in place, a user may use another operator's access network, and will be authenticated by the "home operator". Depending on which solution is chosen, the user may have to put trust in other, visited operators, as well as in his home operator.

The cellular operators may provide the WLAN access in the future In addition, there also will be important WLAN-only operators on the market. The level of trust of communication between the WLAN and the 3GPP system may be considered to have three levels:

1) The WLAN may be completely untrusted by the UE and the 3GPP system.

2) The WLAN contains elements that may be trusted by the UE and the 3GPP system. For example, the WLAN may include trusted servers that look after aspects of security and authentication interworking with the 3GPP systems (e.g. 802.1x, 802.11i). However, other elements of the network may be untrusted.

3) All of the elements of the WLAN may be fully trusted by the UE and the 3GPP system.

Table B.1

	LOW TRUST	HIGH TRUST
Access to services provided by the WLAN Access Provider	- Charging based on usage or authorisation level. Maybe risky for the Cellular Operator, the accounting information may be not reliable. - Cellular Operator cannot grant user data protection.	- Cellular Operator controls sessions, charging, authorisation, etc., based on information received from the WLAN Access Provider Network, and actions performed at said network. - The WLAN Access Provider is trusted to grant adequate protection of user data.
Access to services provided by the Cellular Operator	- Charging, authorisation enforcement, control of sessions, etc. must be performed at the Cellular Operator Network, counting on user data received via tunnels. - The tunnelling mechanism must be able to provide data origin authentication and integrity protection at least. - The tunnelling mechanism may have as end point either the HPLMN or the VPLMN, depending on some aspects e.g. the need to access services in the VPLMN	- Charging, authorisation enforcement, control of sessions, etc. can be performed with participation of both networks. - It may be unnecessary that the tunnelling mechanism implements any protection mechanism, if there is protection of user data in the WLAN AP and there is some security mechanism between the WLAN AP and the Cellular Operator.

Annex C (informative): Analysis of Threats

C.1 Security for Public WLAN Access

These questions related to security in the 3GPP-WLAN architecture, must be addressed:

- What needs to be protected? i.e. what are the assets, and to whom are they valuable?
- What trust relations can be assumed? i.e. who can trust whom, and to what degree? The Trust Model is described in Annex B.
- What are possible attacks against the assets, how can they be performed, and what is done to detect/prevent them?

In section C.2 the relevant assets and threats to those assets are identified. Section C.3 contains examples of possible attacks. Countermeasures are not discussed in this section but the threats and specific attacks should be taken into consideration when defining security mechanisms for 3GPP-WLAN interworking.

C.2 Assets and Threats

This section describes different types of assets that are valuable to the parties involved. Threats to these assets are also identified.

C.2.1 3GPP Operator's Assets

C.2.1.1 Access to WLAN Services

The WLAN Services is what the 3GPP Network Operator is offering to its WLAN customers. The 3GPP Network Operator expects some benefit in return for providing this asset.

The following threats are relevant for this asset:

- An attacker bypasses the access control and authorisation mechanisms in order to get the WLAN services for free.
- An attacker impersonates a legitimate WLAN user. This way the attacker has free access to WLAN services and the victim gets charged for the attacker's usage of the services.
- The attacker is a legitimate WLAN user in the sense that he has a customer relationship with the operator (i.e. a WLAN user account), but he bypasses the authorisation mechanism to get services he has not paid for.
- The attacker interferes with the charging mechanism for the WLAN services, rending a legitimate user's bills incorrect.
- The attacker is a legitimate WLAN user and he gets to interfere with the charging mechanism, e.g. to reduce the own bill.
- The attacker is a legitimate prepaid user that avoids disconnection when the prepaid account expires.
- The attacker prevents WLAN users from accessing to WLAN services (DoS).
- The attacker prevents WLAN users from accessing to the operator's WLAN services, and sets up rogue "services" (e.g. propaganda) instead.

C.2.1.2 Non-WLAN Assets

Other 3GPP operator assets may not be offered over WLAN access networks. Such assets are e.g. access to GSM/UMTS CS services, access to GPRS services, etc. There is a threat that an attacker takes advantage of the WLAN access to perform attacks (e.g. impersonation, DoS, MitM, etc.) against these assets whenever the WLAN access is not properly secured and isolated.

C.2.2 WLAN User's Assets

Since the user's subscription can be considered as an asset for the 3GPP Network Operator, the assets of the user can be considered, to some extent, as 3GPP Operator's assets too. That is, if the user perceives that the utilisation of WLAN services poses a threat to his/her assets, it is likely that the user will avoid using those services, or that the price the user is willing to pay for the services will diminish. Moreover, users might claim liability of the 3GPP Network Operator for the damage caused to their assets.

C.2.2.1 Access to WLAN Services

From the WLAN user's standpoint, this is the asset the user expects to obtain. The user is willing to pay a price to get this asset.

The following threats should be considered:

- The WLAN user gets impersonated by an attacker, which obtains access to WLAN services at the user's expense. Moreover, the attacker can utilise the WLAN services of the victim to perform deceitful activities.
- An attacker gets to make the user charged for services that the victim has not requested.
- The WLAN user cannot get WLAN services due to a DoS attack against the network, or to a targeted DoS attack against that specific user.
- The WLAN user cannot access to the operator's WLAN services, and gets rogue "services" (e.g. propaganda) set up by an attacker instead.

NOTE: There is some overlapping between these threats and those relevant for this asset from the 3GPP Network Operator's standpoint. For instance, a DoS attack is a problem for the user in the sense that he/she cannot get the WLAN services. It is also a problem for the Operator because it cannot charge the users for the services while they are unavailable (unless they are charged as a flat rate) and the Operator's image gets damaged. Similar arguments can be used for the rest of the overlaps.

C.2.2.2 User Data and Privacy

The user expects that the data he sends/receives while accessing to WLAN services, personal information (such as identity, which services he/she uses or where he/she is located at a given time) is kept away from unauthorised parties and data stored in his/her WLAN UE is not accessed by unauthorized users.

The following threats are relevant:

- An attacker obtains the information that the user sends/receives while accessing to WLAN services. This includes user credentials transferred during the authentication phase, as well as any other data (e.g. documents) exchanged once the user has gained access to the WLAN services. The attacker might know or not who the user is;
- An attacker manipulates or substitutes the information that the user sends/receives while accessing to WLAN services. The attacker might know or not who the user is;
- An attacker analyses the information sent/received by users (even if it is mostly concealed) in order to derive some personal information about the users (such as which services they are using or where they are located at a given time).
- An attacker obtains information about the user (permanent identity etc.) and traces where and when the user has been accessing WLAN services.

- An attacker (also a legal user) accesses the user's WLAN UE in link layer without the user's permission.

In some situations, such as public hotspots, it is considered a real threat that users can access each other in link layer directly. It is recommended to segregate user traffic at AP and access controller in WLAN AN to protect assets of users and operator.

C.2.3 WLAN Access Network Provider's Assets

In principle, the WLAN Access Network is outside the scope of 3GPP-WLAN interworking standardisation. Nevertheless, it is important to consider the "Access to WLAN Services" asset of the WLAN Access Network provider, since it can be regarded as a part of the "Access to WLAN Services" asset of the 3GPP Operator. In fact, many threats against the 3GPP Operator's assets can be realised by attacking the WLAN AN. Therefore, it is important that 3GPP-WLAN interworking sets security requirements on the WLAN AN and/or chooses a security solution that is robust to different levels of WLAN AN security.

The same threats as for the "Access to WLAN Services" asset of the 3GPP Operator are valid here.

C.3 Attacks

This section is an attempt to give a concrete form to the threats of the previous section, and to identify several attacks that are applicable in a typical WLAN-3GPP interworking scenario. A single attack can be used to realise one or possibly several of the threats described in the Sec. 3, depending on the intent of the attacker. An attacker setting up a rouge AP may e.g. attempt to get free access, modify a legitimate user's traffic or do a Denial of Service attack. Most of the attacks are performed by an attacker in the WLAN AN but may have implications on the 3GPP operator's assets. Attacks can also be performed remotely over the Internet. For certain types of attacks, the perpetrator does not need to "be a part" of the network. Examples are some types of layer 2 attacks and certain DoS attacks, e.g. setting up a radio jammer in a hotspot. Other attacks require that the attacker has access to the WLAN AN or the Internet. It should be noted that an easy way of getting access to the WLAN AN is to simply become a legitimate subscriber.

The attacks are classified according to where the attack is performed/launched:

- Victim's WLAN UE;
- Attacker's WLAN UE and/or AP;
- WLAN Access Network infrastructure;
- Other device on the Internet.

The attacks mentioned are by no means the only ones possible. Moreover, the actual possibility to carry out an attack may depend on the WLAN technology and the level of WLAN specific protection used.

Even though some attacks can be easily prevented no effort is made in this section to describe countermeasures.

C.3.1 Attacks at the Victim's WLAN UE

Open platform terminals may be infected by viruses, Trojan horses or other malicious software. The software operates without the knowledge of the user on his terminal, and can be used for different types of attacks:

- If the user has credentials stored on a smart card connected to his terminal, a Trojan residing in the terminal can make fake requests to the smart card and send challenge-response results to another MS. For example, the owner of the latter MS could then get access with the stolen credentials.

NOTE: This attack is performed inside the terminal, and it is independent of the external link between the terminal and the smart card reader, which can be secured or assumed to be physically secure.

- Trojans may perform all the usual activities: monitor the user's keyboard or sensitive data, and forward the information to another machine.
- Malicious software can be used to perform Distributed DoS (DDoS) attacks. That is, several instantiations of the software (residing on different hosts) synchronise and start a DoS attack simultaneously against a target.

- Malicious software could be trying to connect to different WLANs, just to annoy the user.

Alternatively, the (U)SIM in the cellular phone can be used remotely from the WLAN client through a serial, infrared, or Bluetooth connection, in order to use the phone as a smart card reader. As the terminal must access the (U)SIM in the phone, the link in between must be secure. Both cable and Infrared can be assumed physically secure, and Bluetooth will depend highly on the current Bluetooth security mechanism.

C.3.2 Attacks from an Attacker's WLAN UE and/or AP

Several types of attacks are possible if the attacker has access to a laptop with WLAN interfaces and/or an Access Point. Denial of Service (DoS) attacks are easy to launch, e.g. by setting up a radio jammer at the hot spot. For some WLAN technologies, the layer 2 control signalling is not integrity protected opening up for DoS attacks by e.g. disassociating legitimate users.

Unless protected, an attacker can easily eavesdrop on the traffic between a user and an AP. The only equipment needed to do this is a laptop with a WLAN interface.

In a rogue AP / rogue network attack, the attacker e.g. employs an AP (masqueraded as a legitimate AP in a given hotspot) connected to a WLAN UE. Based on signal strength, an unsuspecting WLAN UE may connect to the rogue AP. This type of attack can be used to realise several different threats. The attacker could possibly modify the user's traffic or divert the traffic to a network other than the WLAN AN the user intended to use. The attacker could e.g. also fake a network or a commercial site to get access to e.g. credit card information. The attacker can also act as a Min in the Middle during the authentication procedure and cause the MAC/IP address-pair of the attacking WLAN UE to be bound to the credentials of the legitimate user. As a consequence, the attacker gains access to anything the legitimate user would, while the legitimate user is denied access.

An important class of IP-network attacks relevant in connection with rogue AP / networks are "service spoofing" attacks, where the attacker impersonates one or several services/servers in the network, e.g., a DNS server or a DHCP server. These attacks could be performed e.g. by setting up a rouge AP. Another set of attacks uses fake configuration/control messages (such as ARP or ICMP messages) to redirect a user's traffic. ARP spoofing could also be used to redirect the AP's traffic, e.g. AAA messages generated by the AP. Note that the above include only the best-known and most serious attacks. Given the rich (and always expanding) set of protocols run over IP, all possible attacks could not be accounted for.

Another way to interfere or possibly gain access for an attacker is to simply eavesdrop on the traffic around an AP. Depending on WLAN technology and the level of protection, the MAC and IP addresses may be sent in the clear (they are not encrypted) and the attacker can record these. When the attacker knows the MAC/IP address-pair of a user currently connected, he can set his own addresses to the same values.

C.3.3 Attacks at the WLAN AN Infrastructure

Attacks can be performed at the WLAN AN infrastructure, e.g. Access Points (AP), the LAN connecting the APs, Ethernet switches etc. To perform any type of attacks "inside" the WLAN AN, the attacker needs access to the network in some way. For ordinary wired networks, an attacker needs to somehow hook up to the wires to get access. The WLAN AN is partially a wired network, and an attacker may hook up to that part of the network. In public spaces the APs and corresponding wired connections may be physically accessible by attackers. Simply connecting a laptop to the wired LAN "behind" the APs may give the attacker free access to WLAN services as well as access to other user's data and signalling traffic.

Depending on where charging data is collected, an attacker with access to the wired LAN of the WLAN AN can also interfere with the charging functions. If the volume based charging model is applied, an attacker could e.g. inject packets with any chosen source or destination MAC and IP addresses, just to increase a user's bill.

For WLAN Direct IP Access if the charging is based on IP address, there exists a threat of IP address spoofing attack against the WLAN AN, which may generate incorrect accounting message for users.

NOTE: 3GPP suggest WLAN operators not to use IP address based accounting; unless there are sufficient countermeasures implemented against IP address spoofing attack in the WLAN AN.

C.3.4 Attacks Performed by Other Devices on the Internet

Several attacks can be performed from devices connected to the Internet.

If the volume based charging model is applied, an attacker could flood a user with garbage packets, just to increase the user's bill. This is e.g. effective if the attacker resides somewhere on the Internet with a flat rate charging model, or if the attacker has infected other users' machines with "bot"-software ("bot" is short for robot, and refers to software that "lives on its own"). The bot could for instance listen for connections on a certain port, and when receiving a command from the attacker on that port, it starts flooding a given IP address with packets. Various Distributed Denial of Service (DDoS) tools using such bots are known and available in the hacker world.

C.3.5 Implications of the A5/2 Attack for 3GPP WLAN Access

This annex provides an analysis of the implications of the A5/2 attack on 3GPP WLAN access, and provides recommendations on how to mitigate the impacts of the attack to 3GPP WLAN access

Barkan et.al. [28] presented a real-time attack on A5/2 algorithm in [Bar03]. The attack breaks the A5/2 algorithm. In the man-in-the-middle version of the attack, the terminal is forced to use A5/2, while the attacker can use A5/1 against the network. The keys that are used for A5/2 algorithm can be used also with A5/1 cipher. Unfortunately, the vulnerability spreads also to A5/3 and GEA algorithms. The main reasons to the A5/2 flaws are: weak cipher, no bidding down protection and usage of same keys for different algorithms. The attack affects SIM usage. This analysis reflects the impacts from WLAN access point of view. The implications can be analyzed as follows:

Table C.1

Scenario:	Implication:
1. SIM shared between WLAN device and GSM device	1 A5/2 should not be allowed in the terminal, OR 2 Some key separation countermeasures should be used in the terminal, OR 3 A5/2 vulnerability may reveal Kc and this may allow WLAN terminal impersonation towards 3G network

Based on the analysis, it may make sense to avoid the use of the A5/2 algorithm in the terminal and/or provide some countermeasures against the attack. If A5/2 is used and there is an attack against it, Kc may be revealed. This implies that the A5/2 vulnerability can spread from the GSM network to the WLAN network. This, in turn, implies that the revealed Kc may be used to impersonate a terminal in the WLAN-3G network towards the network. Similarly an attack using A5/2 can destroy the confidentiality of the WLAN radio access, as the Kc:s used can be retrieved via A5/2 attacks.

It should be noted that the threats applies to EAP-SIM, as specified in 33.234. EAP-SIM can be attacked whenever a few valid GSM triplets have been retrieved.

Annex D (informative): Management of sequence numbers

The example sequence number management schemes in [21] Informative Annex C can be used to ensure that the authentication failure rate due to synchronization failures to kept sufficiently low when the same sequence number mechanism and data is used for authentication in the PS/CS domains, in IMS and WLAN. This can be done by enhancing the method for the allocation of index values in the AuC so that authentication vectors distributed to different service domains shall always have different index values (i.e. separate ranges of index values are reserved for PS, CS, IMS operation and WLAN access). The AuC is required to obtain information about which type of service node has requested the authentication vectors. Reallocation of array elements to the IMS domain can be done in the AuC with no changes required to already deployed USIMs.

As the possibility for out of order use of authentication vectors within the WLAN service domain may be quite low, the number of existing array elements that need to be reallocated to the WLAN domain could be quite small. This means that the ability to support out of order authentication vectors within the PS, CS and IMS domains would not be significantly affected.

Sequence number management is operator specific and for some proprietary schemes over the air updating of the UICC may be needed.

Annex E: (informative): Alternative Mechanisms for the set up of UE-initiated tunnels (WLAN 3GPP IP Access)

E.1 IKE with subscriber certificates

- The UE and the PDG use IKE, as specified in [rfc2409], in order to establish IPsec security associations.
- Public key signature based authentication with certificates, as specified in [rfc2409], is used in order to authenticate the PDG and the UE.
- A profile for IKE is defined in section 6.5.

E.2 IKEv2 with subscriber certificates

- The UE and the PDG use IKEv2, as specified in [ikev2], in order to establish IPSec security associations.
- Public key signature based authentication with certificates, as specified in [ikev2], is used in order to authenticate the PDG and the UE.
- A profile for IKEv2 is defined in section 6.5.

Annex F (informative): Handling of the incompatibilities between the WLAN UE and the UICC or SIM card inserted

If a WLAN UE does not conform to Release 6 specifications, it may not support both authentication methods. In this case, the home network operator needs to decide either to reject the authentication, or to proceed to authenticate the UE using a suitable EAP method. For instance, when a USIM is inserted in a Release 6 non-compliant WLAN UE which support a compatible method with the USIM (e.g. WLAN UE supporting EAP SIM). An operator may decide to convert the authentication vectors in order to adapt them to the EAP SIM authentication. This authentication vector conversion is defined in TS 33.102 [21].

As specified in TS 33.102 [21], it is not possible to have UMTS authentication using a SIM, as some parameters cannot be created from triplets (e.g. sequence number). Similarly, if the WLAN UE only supports EAP AKA and the smart card is a SIM, it is not possible to perform an EAP AKA authentication.

If a AAA server does not conform to Release 6 specifications, it may not be able to support EAP-AKA for USIM subscribers. It is recommended that operators avoid this by upgrading AAA servers when UICCs are issued. In this case, the default policy of the ME should be to not accept EAP-SIM, but the ME can support an alternative policy that accepts EAP-SIM, if enabled.

Annex G (informative): Change history

Change history									
Date	TSG #	TSG Doc.	CR	Rev	Cat	Subject/Comment	Old	New	WI
2004-03	SP-23	SP-040167	-	-		Presented for approval at TSG SA #23	1.0.1	2.0.0	
2004-03	SP-23	-	-	-		Approved and placed under Change Control (Rel-6)	2.0.0	6.0.0	
2004-06	SP-24	SP-040384	001	-		Profiling of IKEv2 and ESP for NAT traversal	6.0.0	6.1.0	WLAN
2004-06	SP-24	SP-040385	002	-		Sending of temporary identities from WLAN UE	6.0.0	6.1.0	WLAN
2004-06	SP-24	SP-040386	003	-		Extension of IKEv2 and IPsec profiles	6.0.0	6.1.0	WLAN
2004-06	SP-24	SP-040462	004	1		Support of EAP SIM and AKA in AAA server and WLAN UE	6.0.0	6.1.0	WLAN
2004-06	SP-24	SP-040388	005	-		Introduction of UE split alternative 2 in TS 33.234	6.0.0	6.1.0	WLAN
2004-06	SP-24	SP-040389	006	-		Re-authentication failure notification to HSS	6.0.0	6.1.0	WLAN
2004-06	SP-24	SP-040390	007	-		Identity request procedure clarification	6.0.0	6.1.0	WLAN
2004-06	SP-24	SP-040391	008	-		WLAN mechanism to allow restrictions on simultaneous sessions	6.0.0	6.1.0	WLAN
2004-06	SP-24	SP-040392	009	-		Requirement on keeping WLAN access keys independent from 2G/3G access keys stored in USIM	6.0.0	6.1.0	WLAN
2004-09	SP-25	SP-040622	010	-		Update reference to RFC3748 "Extensible Authentication Protocol (EAP)"	6.1.0	6.2.0	WLAN
2004-09	SP-25	SP-040622	011	-		References update	6.1.0	6.2.0	WLAN
2004-09	SP-25	SP-040622	012	-		Sending of temporary identities from WLAN UE	6.1.0	6.2.0	WLAN
2004-09	SP-25	SP-040622	013	-		Clarification on fast re-authentication procedure	6.1.0	6.2.0	WLAN
2004-09	SP-25	SP-040622	014	-		Correction of authentication procedure for WLAN UE split	6.1.0	6.2.0	WLAN
2004-09	SP-25	SP-040622	016	-		Wa interface security	6.1.0	6.2.0	WLAN
2004-09	SP-25	SP-040622	017	-		Introduction of protected result indications	6.1.0	6.2.0	WLAN
2004-09	SP-25	SP-040622	018	-		Tunnel authentication procedure in Wm interface	6.1.0	6.2.0	WLAN
2004-09	-	-	-	-		Resolution of CR 015 (see below) which modified the same parts as CR 017 (MCC)	6.2.0	6.2.1	
2004-09	SP-25	SP-040622	015	-		Modification of mechanism to restrict simultaneous WLAN sessions	6.2.0	6.2.1	WLAN
2004-12	SP-26	SP-040858	019	2		Profile for PDG certificates in Scenario 3	6.2.1	6.3.0	WLAN
2004-12	SP-26	SP-040868	020	5		Impact of Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces	6.2.1	6.3.0	WLAN
2004-12	SP-26	SP-040858	024	1		Sending of W-APN identification	6.2.1	6.3.0	WLAN
2004-12	SP-26	SP-040858	025	2		Clean up of not completed chapters	6.2.1	6.3.0	WLAN
2004-12	SP-26	SP-040858	027	6		Correction of WLAN UE function split	6.2.1	6.3.0	WLAN
2004-12	SP-26	SP-040858	028	-		Passing keying material to the WLAN-AN during the Fast re-authentication procedure	6.2.1	6.3.0	WLAN
2004-12	SP-26	SP-040858	029	1		Clarification on Deletion of Temporary IDs	6.2.1	6.3.0	WLAN
2004-12	SP-26	SP-040858	030	-		Clarification on Protecting Re-authentication ID in FAST/FULL Re-Authentication procedure	6.2.1	6.3.0	WLAN
2004-12	SP-26	SP-040858	031	-		Assigning Remote IP Address to WLAN UE using IKEv2 configuration Payload	6.2.1	6.3.0	WLAN
2004-12	SP-26	SP-040858	033	1		Tunnel Establishment Procedure	6.2.1	6.3.0	WLAN
2004-12	SP-26	SP-040858	036	-		Deletion of inconclusive text on A5/2 countermeasures	6.2.1	6.3.0	WLAN
2004-12	SP-26	SP-040858	037	1		Alignment of IPsec profile with RFC2406	6.2.1	6.3.0	
2004-12	SP-26	SP-040858	040	2		Control of simultaneous sessions in WLAN 3GPP IP access	6.2.1	6.3.0	WLAN
2004-12	SP-26	SP-040858	041	1		Completion of definition and abbreviations	6.2.1	6.3.0	WLAN
2004-12	SP-26	SP-040858	042	1		Fallback from re-authentication to full authentication	6.2.1	6.3.0	WLAN
2004-12	SP-26	SP-040858	043	-		Clarification on the use of IMSI in WLAN 3GPP IP access	6.2.1	6.3.0	WLAN
2004-12	SP-26	SP-040858	044	2		Clarification on the use of MAC addresses	6.2.1	6.3.0	WLAN

2004-12	SP-26	SP-040858	045	-		Clarifications and corrections on the use of pseudonyms	6.2.1	6.3.0	WLAN
2004-12	SP-26	SP-040858	047	-		Wn Reference Point Description	6.2.1	6.3.0	WLAN
2004-12	SP-26	SP-040858	048	-		Removal of word 'scenario'	6.2.1	6.3.0	WLAN
2004-12	SP-26	SP-040858	049	1		Correction of WRAP to CCMP	6.2.1	6.3.0	WLAN
2004-12	SP-26	SP-040858	050	1		Removal of resolved editors' notes	6.2.1	6.3.0	WLAN
2005-03	SP-27	SP-050142	051	-		Wu Reference Point Description	6.3.0	6.4.0	WLAN
2005-03	SP-27	SP-050142	052	1		Replacing PDGW with PDG	6.3.0	6.4.0	WLAN
2005-03	SP-27	SP-050142	055	1		Clarification on EAP-AKA(SIM) description in 3GPP IP access authentication and authorization	6.3.0	6.4.0	WLAN
2005-03	SP-27	SP-050142	056	2		Threat of users accessing each other in link layer and corresponding security requirements of user traffic segregation	6.3.0	6.4.0	WLAN
2005-03	SP-27	SP-050142	057	1		Clarifying the status that can"t be changed in the security requirement of WLAN-UE split	6.3.0	6.4.0	WLAN
2005-03	SP-27	SP-050142	058	2		WLAN AN providing protection against IP address spoofing	6.3.0	6.4.0	WLAN
2005-03	SP-27	SP-050142	059	1		Clarification on the handling of simultaneous sessions	6.3.0	6.4.0	WLAN
2005-03	SP-27	SP-050142	060	2		Removal of editors' notes	6.3.0	6.4.0	WLAN
2005-03	SP-27	SP-050142	061	1		Detecting the start of a WLAN Direct IP Access session based on Wa/Wd Accounting Messages	6.3.0	6.4.0	WLAN
2005-03	SP-27	SP-050142	063	1		Adding verification method of PDG certification by OSCP protocol	6.3.0	6.4.0	WLAN
2005-06	SP-28	SP-050265	064	2	F	Specify the number of the IPsec SAs under the same IKE SA in WLAN 3GPP IP access	6.4.0	6.5.0	WLAN
2005-06	SP-28	SP-050265	065	1	F	Terminate WLAN session by AAA server	6.4.0	6.5.0	WLAN
2005-06	SP-28	SP-050265	066	-	F	Correction to the definition of the Wn Reference Point	6.4.0	6.5.0	WLAN
2005-06						Corrects version number on cover page	6.5.0	6.5.1	
2005-09	SP-29	SP-050547	0067	-	F	Correction of reference	6.5.1	6.6.0	WLAN
2005-09	SP-29	SP-050547	0068	-	F	Clarification on obtaining Remote IP address during Tunnel Establishment Procedure	6.5.1	6.6.0	WLAN
2005-09	SP-29	SP-050547	0069	-	F	Profiling of IKEv2 to support Re-keying of IPsec SAs and IKE SAs	6.5.1	6.6.0	WLAN
2005-09	SP-29	SP-050547	0070	-	F	Separation of authentication and authorization in WLAN 3GPP IP access	6.5.1	6.6.0	WLAN
2005-09	SP-29	SP-050547	0071	-	F	Support for simultaneous WLAN direct IP access sessions	6.5.1	6.6.0	WLAN
2005-12	SP-30	SP-050765	0072	-	F	IMSI availability at PDG	6.6.0	6.7.0	WLAN
2006-03	SP-31	SP-060047	0073	-	F	Correction of the incorrect statement in Tunnel fast re-authentication and authorization	6.7.0	6.8.0	WLAN
2006-03	SP-31	SP-060047	0074	-	F	updating the reference	6.7.0	6.8.0	WLAN
2006-03	SP-31	SP-060047	0076	-	F	Correction to authentication information retrieval between 3GPP AAA Server and HSS	6.7.0	6.8.0	WLAN
2007-03	SP-35	SP-070218	0090	2	F	Mandate the format of PDG ID	6.8.0	6.9.0	WLAN
2007-03	SP-35	SP-070144	0092	1	F	Correction and clarification of 3GPP AAA Server behavior	6.8.0	6.9.0	TEI6
2007-03	SP-35	SP-070141	0094	1	F	Extension of scope of TS 33.234	6.8.0	6.9.0	WLAN
2007-03	SP-35	SP-070145	0097	-	F	Clarification on certificate chain handling	6.8.0	6.9.0	TEI6

History

Document history		
V6.3.0	December 2004	Publication
V6.4.0	March 2005	Publication
V6.5.1	June 2005	Publication
V6.6.0	September 2005	Publication
V6.7.0	December 2005	Publication
V6.8.0	March 2006	Publication
V6.9.0	March 2007	Publication