Technical Specification Group Services and System Aspects
Meeting #26, Athens, Greece

TSGS#26(04)0858

Source: SA WG3

Title: 22 CRs to 33.234: (Rel-6)

Document for: Approval

Agenda Item: 7.3.3

The following CRs have been agreed by SA WG3 and are presented to TSG SA for approval.

TSG SA Doc number	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	SA WG3 Doc number	Work item
SP-040858	33.234	019	2	Rel-6	Profile for PDG certificates in Scenario 3	F	6.2.1	S3-041100	WLAN
SP-040858	33.234	020	4	Rel-6	Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces)	B	6.2.1	S3-041151	WLAN
SP-040858	33.234	024	1	Rel-6	Sending of W-APN identification	B	6.2.1	S3-040864	WLAN
SP-040858	33.234	025	2	Rel-6	Clean up of not completed chapters	F	6.2.1	S3-040886	WLAN
SP-040858	33.234	027	6	Rel-6	Correction of WLAN UE function split	C	6.2.1	S3-041149	WLAN
SP-040858	33.234	028	-	Rel-6	Passing keying material to the WLAN-AN during the Fast re-authentication procedure	F	6.2.1	S3-040763	WLAN
SP-040858	33.234	029	1	Rel-6	Clarification on Deletion of Temporary IDs	F	6.2.1	S3-040837	WLAN
SP-040858	33.234	030	-	Rel-6	Clarification on Protecting Re-authentication ID in FAST/FULL Re-Authentication procedure	F	6.2.1	S3-040765	WLAN
SP-040858	33.234	031	-	Rel-6	Assigning Remote IP Address to WLAN UE using IKEv2 configuration Payload	B	6.2.1	S3-040766	WLAN
SP-040858	33.234	033	1	Rel-6	Tunnel Establishment Procedure	F	6.2.1	S3-040861	WLAN
SP-040858	33.234	036	-	Rel-6	Deletion of inconclusive text on A5/2 countermeasures	F	6.2.1	S3-040771	WLAN
SP-040858	33.234	037	1	Rel-6	Alignment of IPsec profile with RFC2406	F	6.2.1	S3-040842	WLAN
SP-040858	33.234	040	2	Rel-6	Control of simultaneous sessions in WLAN 3GPP IP access	C	6.2.1	S3-041153	WLAN
SP-040858	33.234	041	1	Rel-6	Completion of definition and abbreviations	D	6.2.1	S3-041109	WLAN
SP-040858	33.234	042	1	Rel-6	Fallback from re-authentication to full authentication	F	6.2.1	S3-041110	WLAN
SP-040858	33.234	043	-	Rel-6	Clarification on the use of IMSI in WLAN 3GPP IP access	F	6.2.1	S3-040947	WLAN
SP-040858	33.234	044	2	Rel-6	Clarification on the use of MAC addresses	F	6.2.1	S3-041138	WLAN
SP-040858	33.234	045	-	Rel-6	Clarifications and corrections on the use of pseudonyms	F	6.2.1	S3-040949	WLAN
SP-040858	33.234	047	-	Rel-6	Wn Reference Point Description	D	6.2.1	S3-040958	WLAN
SP-040858	33.234	048	-	Rel-6	Removal of word ìscenarioî	F	6.2.1	S3-040959	WLAN
SP-040858	33.234	049	1	Rel-6	Correction of WRAP to CCMP	F	6.2.1	S3-041108	WLAN
SP-040858	33.234	050	1	Rel-6	Removal of resolved editors' notes	D	6.2.1	S3-041155	WLAN

3GPP TSG SA WG3 Security ó S3#36
Shenzhen, China, 23ñ26 November 2004

Tdoc ⌘S3-041100

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**019**	⌘**rev**	**2**	⌘	Current version:	**6.2.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Profile for PDG certificates in Scenario 3		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	07/09/2004
Category:	⌘	**F**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	33.234 says PDG is authenticated with certificates, but does not specify how the certificates are handled.
Summary of change:	⌘	Specifies the contents of PDG certificates and requirements for their processing at the WLAN UE.
Consequences if not approved:	⌘	Reduced interoperability.

Clauses affected:	⌘	2, 6.1.5, new clause between 6.6 and 6.7				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

********** FIRST CHANGE **********

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] draft-arkko-pppext-eap-aka-12, April 2004: "Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA)". IETF Work in progress

[5] draft-haverinen-pppext-eap-sim-13, April 2004: "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)". IETF Work in progress

[6] IEEE Std 802.11i/D7.0, October 2003: "Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security".

[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] draft-ietf-ipsec-ikev2-14.txt, May 2004: "Internet Key Exchange (IKEv2) Protocol".

[30] RFC 2406, November 1998: "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-mariblanca-aaa-eap-lla-01.txt, June 2004: "EAP lower layer attributes for AAA protocols".

[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".

********** NEXT CHANGE **********

6.1.5 Mechanisms for the set up of UE-initiated tunnels (Scenario 3)

- 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 with an identity, for example, "pdg.mncNNN.mccMMM.3gppnetwork.org". 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 section 6.x.
- 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.

Editor's note: The discussion on the security mechanisms for the set up of UE-initiated tunnels is still ongoing in SA3. The text in this section reflects the current working assumption of SA3. Alternatives still under discussion in SA3 are contained in Annex E. They may replace the current working assumption in this section if problems with the working assumption arise. Otherwise, Annex E will be removed before the TS is submitted for approval. The above points on the use of IKEv2 are dependent on the analysis of the open issues on legacy VPN clients and key management; in particular, the use of EAP-AKA and EAP-SIM will be studied.

********** FINAL CHANGE **********

Insert new section below after 6.6 (Profile for IPsec ESP) but before 6.7 (WLAN UE split interworking)

6.x 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 RFC3280 [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 RFC3280 [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" (RFC3279 [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 support paths of at least four certificates (self-signed CA certificate, intermediate CA 1, intermediate CA 2, PDG certificate).

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. Support for CRLs is optional. Support for OCSP is mandatory.

********** END OF CHANGE **********

3GPP TSG SA WG3 Security ó SA3#36 **S3-041151**

Shenzhen, 23 ñ 26 November 2004

CR-Form-v7

CHANGE REQUEST

⌘	**TS 33.234**	**CR**	**020**	⌘ **rev**	**4**	⌘	Current version:	**6.2.1** ⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network □

Title:	⌘	Impact of Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces			
Source:	⌘	SA WG3			
Work item code:	⌘	WLAN	***Date:***	⌘	25/11/2004
Category:	⌘	**B**	***Release:***	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	TS 33.234 currently does not consider the Reuse of a Single SIM, USIM, or ISIM by peripheral devices on local interfaces to access multiple networks. This aspect has been studied in the feasibility study report (i.e. TR 33.817).
Summary of change:	⌘	Some minor changes to accommodate the additional feature.
Consequences if not approved:	⌘	New feature could not be supported.

Clauses affected:	⌘	4.1.4, 4.2.4.2, C.3.1

Other specs affected: ⌘ ⌘

Y	N
	N
	N
	N

Other comments:	⌘	The CR is the outcome of TR 33.817 that was supported by the following companies. Toshiba, Intel, T-Mobile, Telcordia, Thomson, Fujitsu, HP, RIM, SmartTrust, BT Group PLC, Alcatel and Gemplus

***** Start of change *****

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;

Editors note: definition of simultaneous access still TBA with SA1- LS in S3 030169] Reply to SA2 in S3-030188 provides some clarification. (Already studied and declared feasible in TR 33.817, however the mechanisms still need to be defined).

  - 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;

Editors note: All these alternatives must be carefully studied from a security perspective.

- 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 (PDGW)** 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.

***** End of change *****

***** Start of change *****

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, e.g. 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 ì Allowî, or ì Disallowî. 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.

Editors note: It was agreed at SA3#31 that for WLAN interworking, modification of EAP parameters on the Bluetooth interface will cause EAP to fail in the network or on the USIM. It was therefore agreed to remove the "undetected modification" requirement from this TS.

***** End of change *****

***** Start of change *****

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.

***** End of change *****

3GPP TSG SA WG3 Security ó S3#35
St. Paulís Bay, Malta 5 - 8 October 2004

Tdoc ⌘S3-040864

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**024**	⌘**rev**	**1**	⌘ Current version:	**6.2.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Sending of W-APN identification		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	07/10/2004
Category:	⌘	**B**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The sending of W-APN identification in Idr payload of IKEv2 has been confirmed as suitable by IETF people. This CR includes this parameter in the authentication description and the associated editorís notes are removed.
Summary of change:	⌘	Addition of Idr payload and removal of editorís notes related to W-APN parameter
Consequences if not approved:	⌘	W-APN not available in the AAA server, and authorization functions cannot be performed in WLAN 3GPP IP access

Clauses affected:	⌘	6.1.5.1, 6.1.5.2				
		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	24.234, 29.234
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

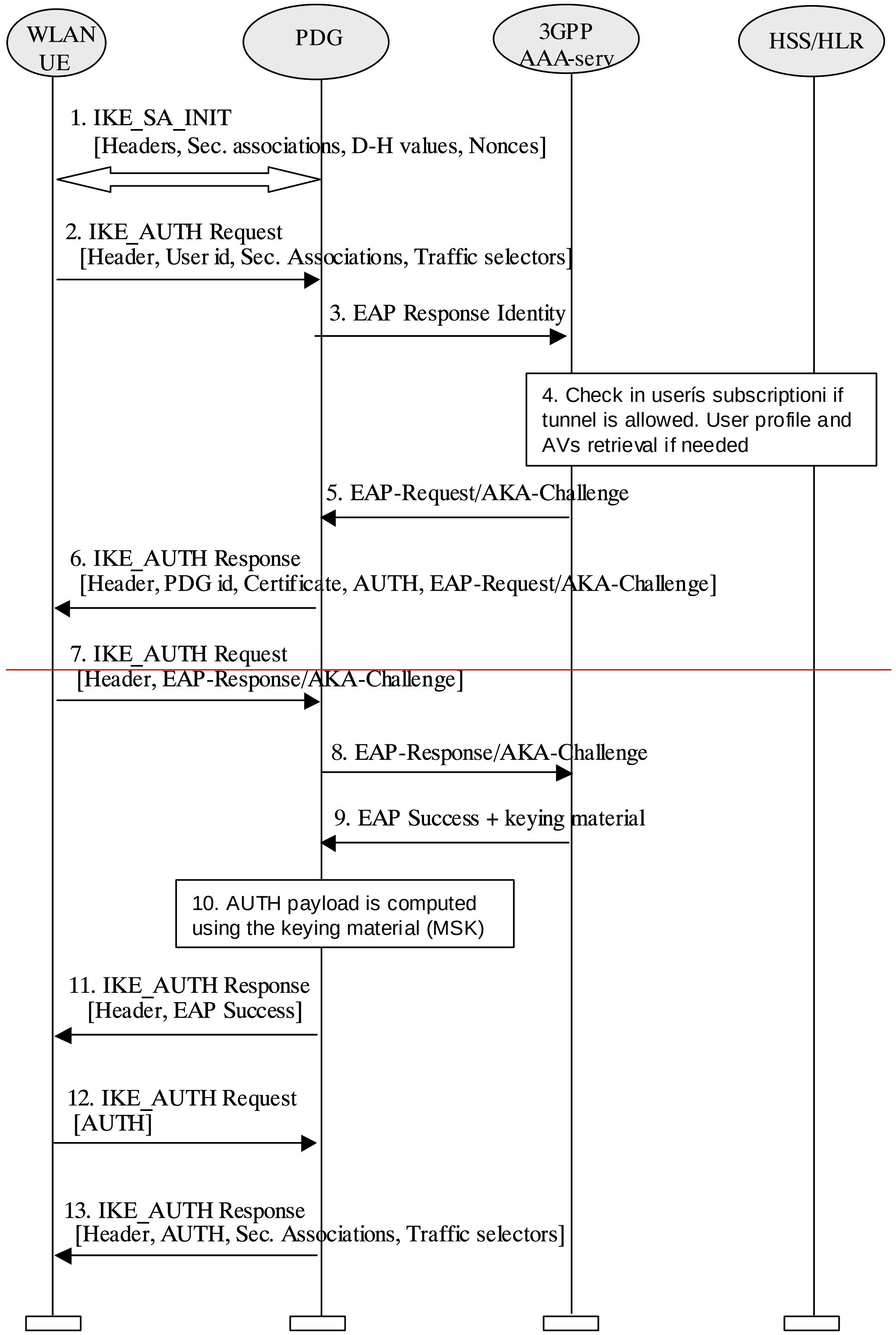
*** BEGIN SET OF CHANGES ***

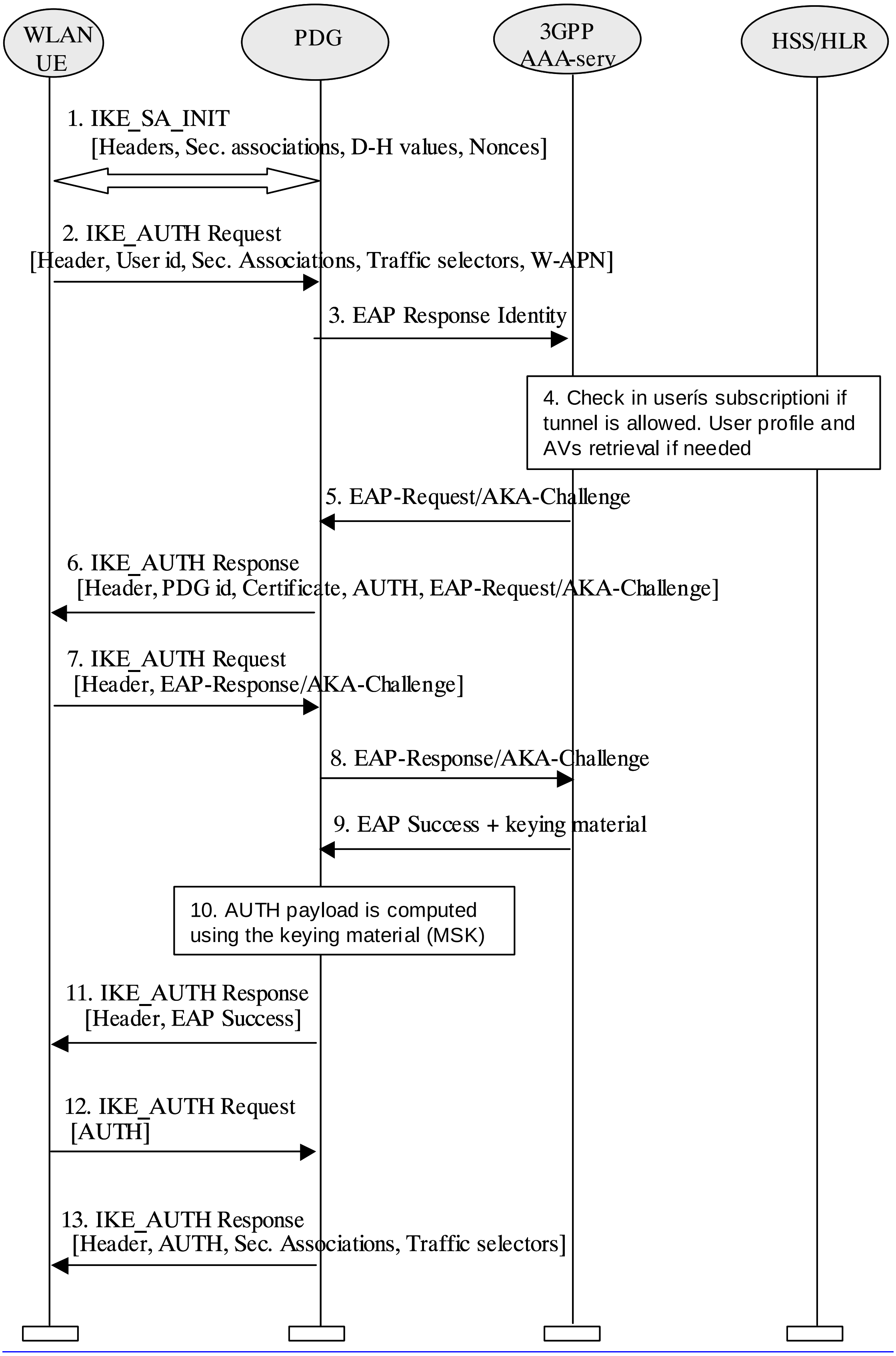
6.1.5.1 Tunnel full authentication and authorization

The tunnel end point in the network is the PDG. 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 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 AAA server over Diameter (the opposite for messages sent from the AAA server).

The sequence diagram is shown in this chapter. 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 AAA server to request the user identity again using the EAP AKA or EAP SIM specific methods (as specified in ref. [4] and [5]), because the AAA server is certain that no intermediate node has modified or changed the user identity.


WLAN UE
PDG
3GPP AAA-serv
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request
[Header, User id, Sec. Associations, Traffic selectors]
3. EAP Response Identity
4. Check in userís subscriptioni if tunnel is allowed. User profile and AVs retrieval if needed
5. EAP-Request/AKA-Challenge
6. IKE_AUTH Response
[Header, PDG id, Certificate, AUTH, EAP-Request/AKA-Challenge]
7. IKE_AUTH Request
[Header, EAP-Response/AKA-Challenge]
8. EAP-Response/AKA-Challenge
9. EAP Success + keying material
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response
[Header, EAP Success]
12. IKE_AUTH Request
[AUTH]
13. IKE_AUTH Response
[Header, AUTH, Sec. Associations, Traffic selectors]


WLAN UE
PDG
3GPP AAA-serv
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request
[Header, User id, Sec. Associations, Traffic selectors, W-APN]
3. EAP Response Identity
4. Check in userís subscriptioni if tunnel is allowed. User profile and AVs retrieval if needed
5. EAP-Request/AKA-Challenge
6. IKE_AUTH Response
[Header, PDG id, Certificate, AUTH, EAP-Request/AKA-Challenge]
7. IKE_AUTH Request
[Header, EAP-Response/AKA-Challenge]
8. EAP-Response/AKA-Challenge
9. EAP Success + keying material
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response
[Header, EAP Success]
12. IKE_AUTH Request
[AUTH]
13. IKE_AUTH Response
[Header, AUTH, Sec. Associations, Traffic selectors]

Sequence of events:

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 ref [14], containing the IMSI or the pseudonym. The identity in NAI format generated from the IMSI is described in ref. [4] and [5], depending on the type of EAP method to be used (EAP SIM or EAP AKA).

Editors note: The control of simultaneous sessions in the EAP authentication has to be possible as in WLAN access authentication. Nevertheless, it is needed to study in detail how the parameters to perform this control have to be transferred in EAP/IKEv2. For example, the VPLMN id could be included in the NAI (see TS 23.234 [13], section 5.3.4)

~~Editors' note: W-APN should be sent in this step, because in TS 23.234 [13], there is following sentence; "The WLAN UE shall include the W-APN and the user identity in the initial tunnel establishment request." One possibility is to include the W-APN in the IDr parameter in the IKE_AUTH phase, but this has to be studied in detail.~~

3. The PDG sends the EAP Response identity message to the 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 ref. [32]. This will help the AAA server to distinguish between authentications for WLAN access and authentications for tunnel setup.

4. The AAA server shall fetch the user profile and authentication vectors from HSS/HLR (if these parameters are not available in the 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. The AAA server checks in userís subscription if he/she is authorized to establish the tunnel.

   In this sequence diagram, it is assumed that the user has a USIM and EAP AKA will be used. For EAP SIM there is no difference from the IKEv2-EAP relationship point of view, but only for the EAP SIM mechanism itself, which is explained in this technical specification

5. The 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 AAA server (EAP-Request/AKA-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 to the AAA server

9. When all checks are successful, the AAA server sends 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-AAA server) is implemented using Diameter, the MSK shall be encapsulated in the EAP-Master-Session-Key parameter, as defined in [23]

Editors note: Registration procedure, including transport of parameters needed to perform simultaneous access control, should be performed in order to update registration status in HSS and fetch the necessary data to the AAA server, but this still needs to be studied in detail.

10. 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

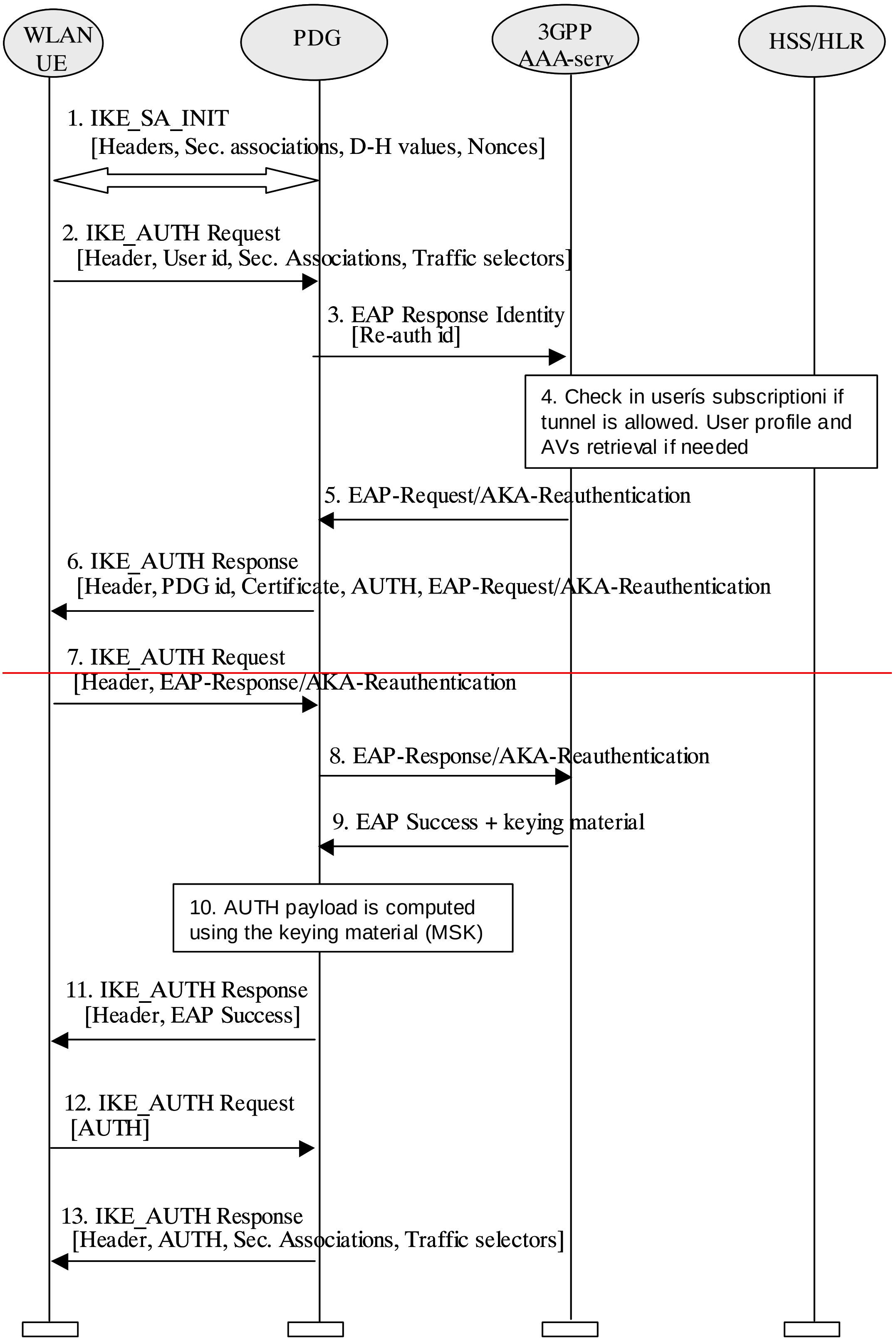
12. The WLAN UE shall take its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the PDG

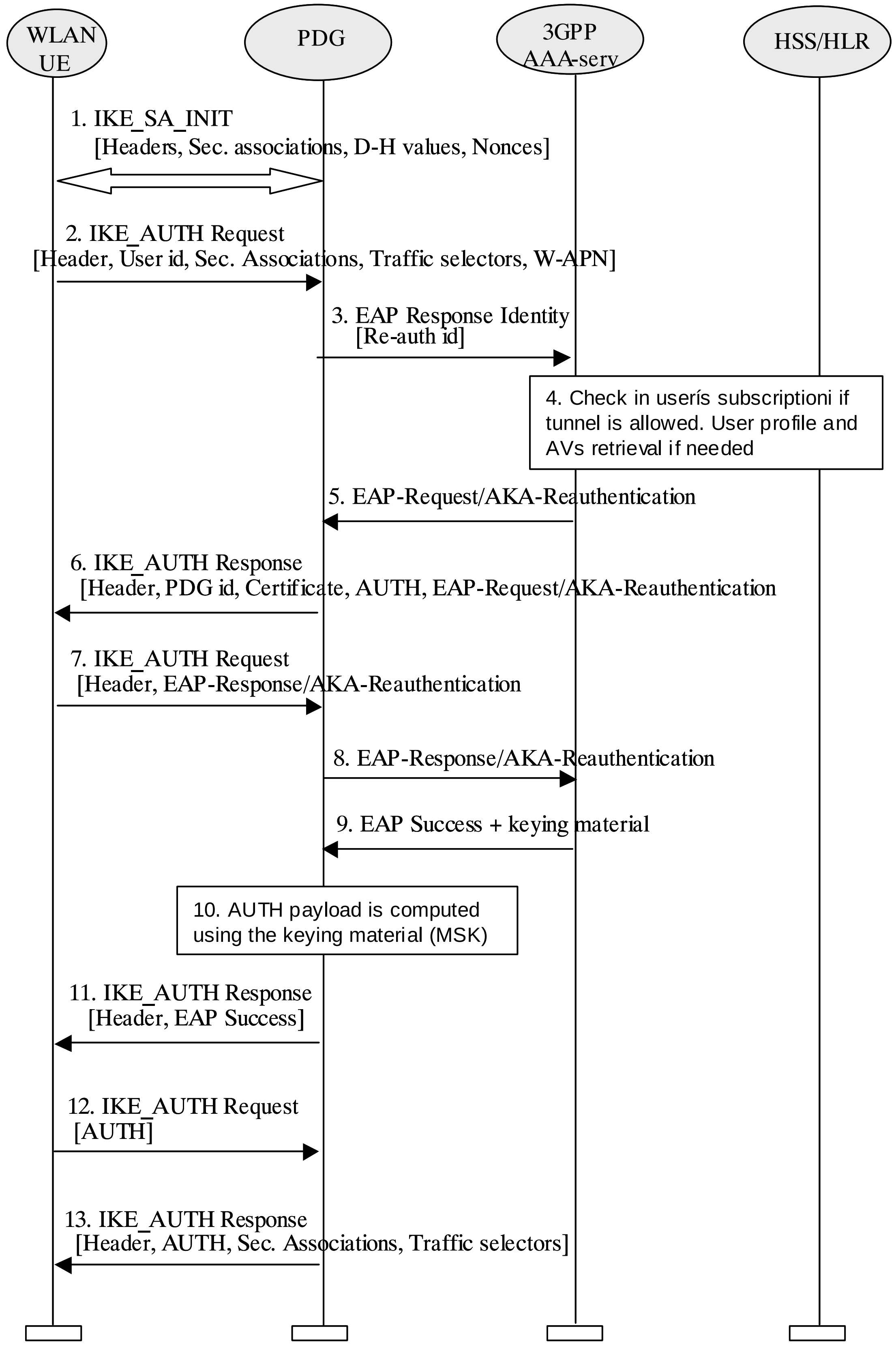
13. The PDG checks the correctness of the AUTH received from the WLAN UE and calculates the AUTH parameter which authenticates the second IKE_SA_INIT message. This AUTH parameter is sent to the WLAN UE together with the security associations and rest of IKEv2 parameters and the IKEv2 negotiation terminates

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 this chapter. 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


WLAN UE
PDG
3GPP AAA-serv
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request
[Header, User id, Sec. Associations, Traffic selectors]
3. EAP Response Identity
[Re-auth id]
4. Check in userís subscriptioni if tunnel is allowed. User profile and AVs retrieval if needed
5. EAP-Request/AKA-Reauthentication
6. IKE_AUTH Response
[Header, PDG id, Certificate, AUTH, EAP-Request/AKA-Reauthentication
7. IKE_AUTH Request
[Header, EAP-Response/AKA-Reauthentication
8. EAP-Response/AKA-Reauthentication
9. EAP Success + keying material
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response
[Header, EAP Success]
12. IKE_AUTH Request
[AUTH]
13. IKE_AUTH Response
[Header, AUTH, Sec. Associations, Traffic selectors]


WLAN UE
PDG
3GPP AAA-serv
HSS/HLR
1. IKE_SA_INIT [Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request [Header, User id, Sec. Associations, Traffic selectors, W-APN]
3. EAP Response Identity [Re-auth id]
4. Check in userís subscriptioni if tunnel is allowed. User profile and AVs retrieval if needed
5. EAP-Request/AKA-Reauthentication
6. IKE_AUTH Response [Header, PDG id, Certificate, AUTH, EAP-Request/AKA-Reauthentication
7. IKE_AUTH Request [Header, EAP-Response/AKA-Reauthentication
8. EAP-Response/AKA-Reauthentication
9. EAP Success + keying material
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response [Header, EAP Success]
12. IKE_AUTH Request [AUTH]
13. IKE_AUTH Response [Header, AUTH, Sec. Associations, Traffic selectors]

Sequence of events:

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.

3. The PDG sends the EAP Response identity message 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. [32]. This will help the AAA server to distinguish between authentications for WLAN access and authentications for tunnel setup.

4. The AAA server shall fetch the user profile and authentication vectors from HSS/HLR (if these parameters are not available in the AAA server) and determines the EAP method (SIM or AKA) to be used, according to the user subscription. The AAA server checks in userís subscription if he/she is authorized to establish the tunnel.

   In this sequence diagram, it is assumed that the user has a USIM and EAP AKA will be used. For EAP SIM there is no difference from the IKEv2-EAP relationship point of view, but only for the EAP SIM mechanism itself, which is explained in this technical specification

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

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 AAA server (EAP-Request/AKA-Reauthentication is included in order to start the EAP procedure over IKEv2.

7. 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

8. The PDG forwards the EAP-Response/AKA-Reauthentication message to the AAA server

9. When all checks are successful, the AAA server sends 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 [23]

10. 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. This AUTH parameter is sent to the WLAN UE together with the security associations and rest of IKEv2 parameters and the IKEv2 negotiation terminates

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Security ó S3#35
St. Paulís Bay, Malta 5 - 8 October 2004

Tdoc* ⌘*S3-040886

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**025**	⌘**rev**	**2**	⌘	Current version:	**6.2.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects:	UICC apps⌘ □	ME □	Radio Access Network □	Core Network ☒

Title:	⌘	Clean up of not completed chapters		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	07/10/2004
Category:	⌘	**F**	***Release:*** ⌘	Rel-6
		Use <u>one</u> of the following categories: ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.	*Use <u>one</u> of the following releases:* *Ph2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)* *Rel-7 (Release 7)*	

Reason for change:	⌘	TS 33.234 still contains some chapters which at the beginning were created in order to insert some text later on, but that have not been filled. This lack of specifications for these chapters has happened because of two reasons: the issue is not under SA3 responsibility, or lack of SA3 interest for the issue. This CR proposes some text to close the chapters
Summary of change:	⌘	The main change is in the ìLink layer requirementsî chapter. The proposal is to remove the questions and write some summary of the state of the art. The requirements are removed as SA3 is not in charge of this issue, but it corresponds to IEEE instead
Consequences if not approved:	⌘	TS 33.234 will contain some chapters not completed

Clauses affected:	⌘	2, 4.2.5				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

*** BEGIN SET OF CHANGES ***

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] draft-arkko-pppext-eap-aka-12, April 2004: "Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA)". IETF Work in progress

[5] draft-haverinen-pppext-eap-sim-13, April 2004: "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)". IETF Work in progress

[6] ~~IEEE Std 802.11i/D7.0, October 2003: "Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security".~~ 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] draft-ietf-ipsec-ikev2-14.txt, May 2004: "Internet Key Exchange (IKEv2) Protocol".

[30] RFC 2406, November 1998: "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-mariblanca-aaa-eap-lla-01.txt, June 2004: "EAP lower layer attributes for AAA protocols".

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

4.2.5 Link layer security requirements

Editors note: This section is FFS, LS (S3-030167) sent to SA2 group on 1) the need for requiring 802.11i in TS 23.234. SA2 to explain the impact (if any) a change of technology from 802.11i to WPA would have on the standardisation work. 2) SA2 to study the architectural impacts of implementing protection on Wa interface 3) SA2 to Investigate the importance of specifying specific WLAN technologies to be used for the WLAN access network.

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.

~~In order to set the bar for allowed WLAN protocols, 3GPP should define requirements on link layer security. The existing and work-in-progress WLAN standards can then be evaluated based on these requirements.~~

Areas in which relevant requirements are~~should be~~ 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 ref. [6]. Other WLAN access technologies are not excluded to be used although not described here.

~~4.2.5.1 Confidentiality and integrity protection of user data~~

- ~~Can user data be sent in the clear or is some kind of protection required?~~
- ~~Is it enough to integrity protect user data or should it be encrypted as well?~~
- ~~How strong must the WLAN security protocols be? Compare e.g. WEP, TKIP and CCMP in the case of 802.11 WLAN.~~

~~4.2.5.2 Protection of signalling~~

- ~~What implications on 3GPP-WLAN security does it have if the WLAN control signalling is unprotected? (Currently 802.11 management frames are not protected by 802.11i).~~

~~4.2.5.3 Key distribution, key freshness validation and key ageing~~

- ~~Can encryption keys generated during EAP authentication be used directly as encryption keys for the link layer or must there be a handshake between UE and AP to e.g. ensure freshness? (Like the 4-way handshake of 802.11i).~~

- ~~What are the security implications of not having a UE-AP key handshake?~~

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Meeting SA3#36
Shenzhen, China, 23 ñ 26 November, 2004

Tdoc ⌘ S3-041149

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**027**	⌘ **rev**	**6**	⌘ Current version:	**6.2.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☒ ME ☒ Radio Access Network □ Core Network □

Title:	⌘ Correction of WLAN UE function split		
Source:	⌘ SA WG3		
Work item code:	⌘ WLAN	***Date:***	⌘ 25/11/2004
Category:	⌘ **C**	***Release:***	⌘ Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change: ⌘ At SA3#32 alternative 2 was chosen as the working assumption for WLAN UE functional split (see S3-040197). However, the required standardized API for local interface between the TE and the ME did not exist yet. But at T2#27, the CRs T2-040439 and T2-040468 to TS 27.007 were agreed, which introduced the new AT commands +CUAD, +CEAP and +CERP. The present CR implements solutions for WLAN UE functional split, using these commands.

Summary of change: ⌘ Modify the WLAN UE functional split to include the termination of EAP in the UICC or in the MT by the new AT commands +CUAD, +CEAP and +CERP.

Consequences if not approved: ⌘ Functional split cannot be implemented in release 6 in a standardized manner.

Clauses affected: ⌘ 2, 5.6, 6.1.3, (new) 6.1.3.1, (new) 6.1.3.2, 6.7, 6.7.1, 6.7.2, 6.7.3, 6.7.4

Other specs affected: ⌘

Y	N		
	X	Other core specifications	⌘
	X	Test specifications	
	X	O&M Specifications	

Other comments: ⌘ The final approval of this CR is conditional on the approval of T2-040439 and T2-040468 by the T-plenary (8 - 10 Dec 2004).

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] draft-arkko-pppext-eap-aka-12, April 2004: "Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA)". IETF Work in progress

[5] draft-haverinen-pppext-eap-sim-13, April 2004: "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)". IETF Work in progress

[6] IEEE Std 802.11i/D7.0, October 2003: "Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security".

[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] draft-ietf-ipsec-ikev2-14.txt, May 2004: "Internet Key Exchange (IKEv2) Protocol".

[30] RFC 2406, November 1998: "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-mariblanca-aaa-eap-lla-01.txt, June 2004: "EAP lower layer attributes for AAA protocols".

[38] 3GPP TS 27.007: "Technical Specification Group Terminals; AT command set for User Equipment (UE)".

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

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

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 ~~will~~ provides WLAN access, while the MT or UICC ~~or SIM card will~~ 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 ~~will~~ can be retrieved by ~~be sent to~~ the WLAN TE in order to be used for link layer security in the WLAN access.

~~NOTE: It shall be possible to have the termination of EAP in the UICC (or SIM card). Details are FFS.~~

6.1.3 EAP support in UICC~~Smart Cards~~

~~Editors note: LS (S3-030187/ S1-030546) from SA1 has stated, "There are requests from operators for a secure SIM based WLAN authentication solution". SA3 has SA1 in an LS (S3-030306) if this request is confirmed. The input paper to SA3 on this can be found at: http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_28_Berlin/Docs/ZIP/S3-030198.zip~~

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 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 TS 102.310 [39]) 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, c.f. [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 33.102 [21]). For this purpose, all steps of the EAP-SIM authentication mechanism described in 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 TS 102.310 [39]) 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.

6.7 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, Ö) at any authentication or re-authentication process, using the AT commands +CUAD, +CEAP and +CERP, as defined in TS 27.007 [38]. The ~~Bluetooth~~ local interface ~~(e.g. Bluetooth, IrDa, RS232, USB, Ö)~~ 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.

~~NOTE: It shall be possible to have the termination of EAP in the UICC (or SIM card). Details are FFS.~~

6.7.1 Full authentication with EAP AKA

The procedures specified in subsections 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 [40].

6.7.1.1 Termination in the UICC

The process is shown in figure 11.

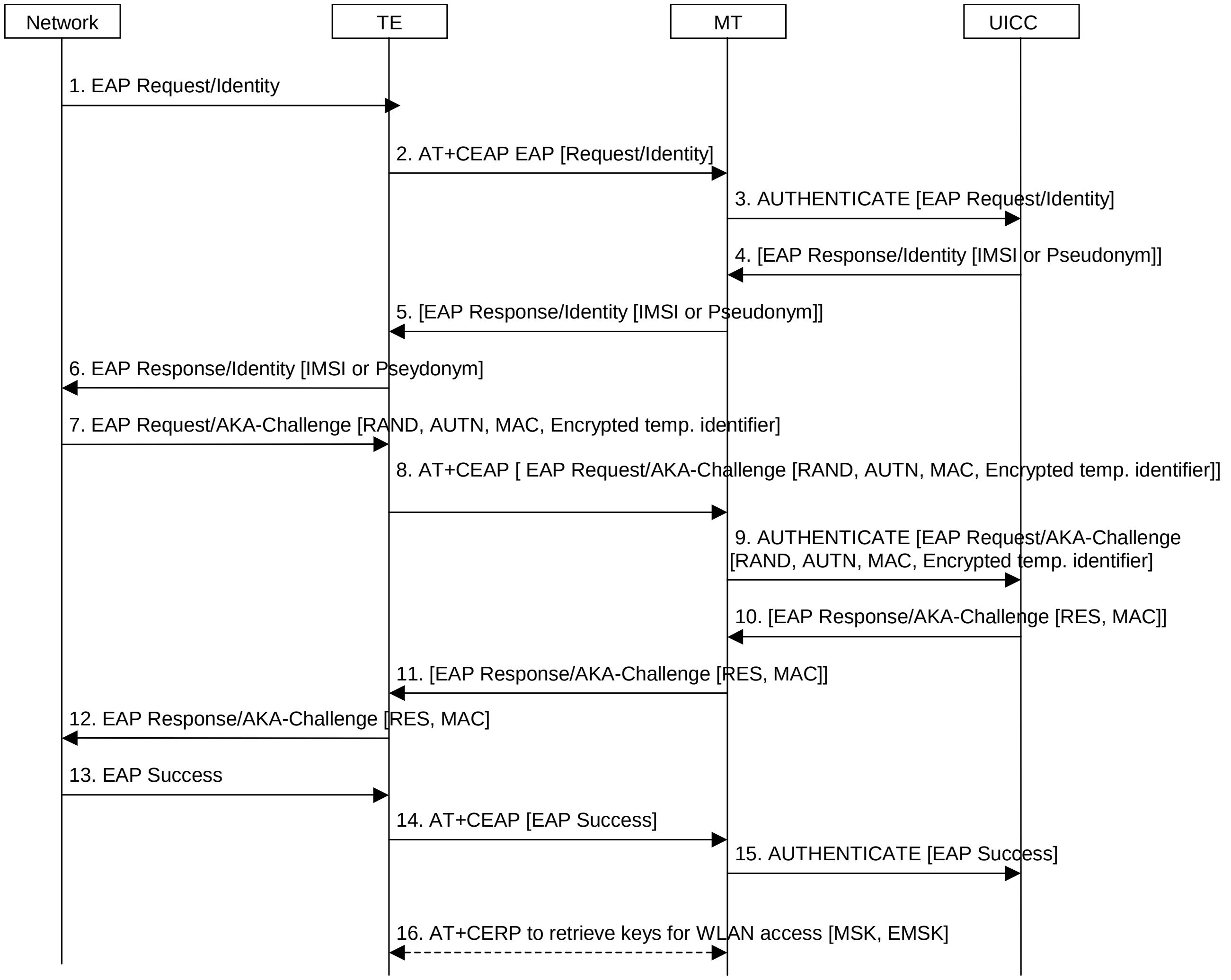

Network
TE
MT
UICC
1. EAP Request/Identity
2. AT+CEAP EAP [Request/Identity]
3. AUTHENTICATE [EAP Request/Identity]
4. [EAP Response/Identity [IMSI or Pseudonym]]
5. [EAP Response/Identity [IMSI or Pseudonym]]
6. EAP Response/Identity [IMSI or Pseydonym]
7. EAP Request/AKA-Challenge [RAND, AUTN, MAC, Encrypted temp. identifier]
8. AT+CEAP [EAP Request/AKA-Challenge [RAND, AUTN, MAC, Encrypted temp. identifier]]
9. AUTHENTICATE [EAP Request/AKA-Challenge [RAND, AUTN, MAC, Encrypted temp. identifier]
10. [EAP Response/AKA-Challenge [RES, MAC]]
11. [EAP Response/AKA-Challenge [RES, MAC]]
12. EAP Response/AKA-Challenge [RES, MAC]
13. EAP Success
14. AT+CEAP [EAP Success]
15. AUTHENTICATE [EAP Success]
16. AT+CERP to retrieve keys for WLAN access [MSK, EMSK]

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 [38], and then shall select the appropriate DF, as indicated in TS 102.310 [39].
3. The MT performs the received +CEAP AT command (see TS 27.007 [38]).
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 [38]).
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.

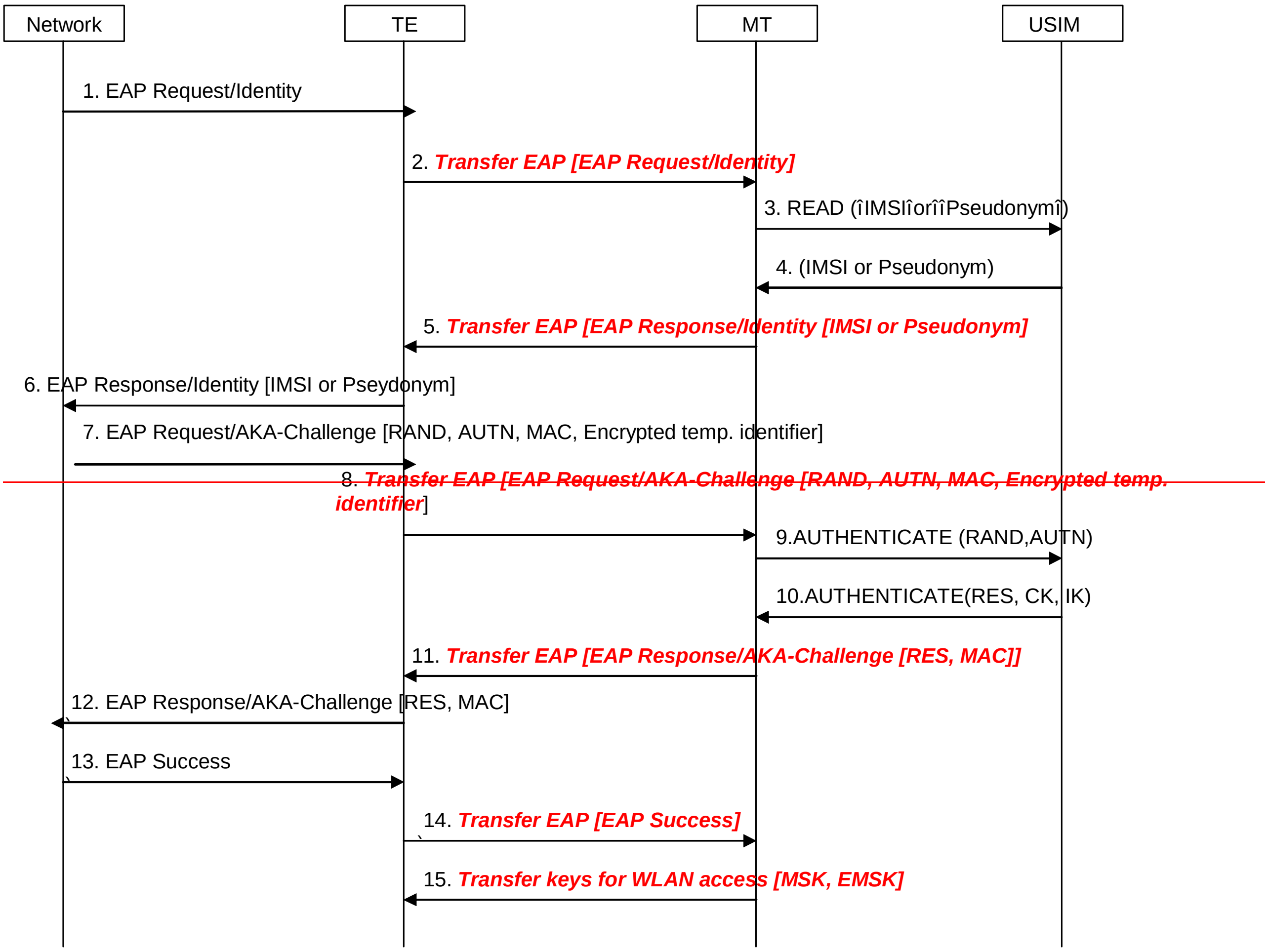
14. The TE sends the EAP packet received in message 13 to the UICC application using +CEAP AT command.

15. The MT performs the received +CEAP AT command (see TS 27.007 [38]).

16. 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

6.7.1.2 Termination in the MT

The process is shown in figure 12~~1~~.


Network
TE
MT
USIM
1. EAP Request/Identity
2. Transfer EAP [EAP Request/Identity]
3. READ (îIMSIîorîîPseudonymî)
4. (IMSI or Pseudonym)
5. Transfer EAP [EAP Response/Identity [IMSI or Pseudonym]
6. EAP Response/Identity [IMSI or Pseydonym]
7. EAP Request/AKA-Challenge [RAND, AUTN, MAC, Encrypted temp. identifier]
~~8. Transfer EAP [EAP Request/AKA-Challenge [RAND, AUTN, MAC, Encrypted temp.~~
identifier]
9.AUTHENTICATE (RAND,AUTN)
10.AUTHENTICATE(RES, CK, IK)
11. Transfer EAP [EAP Response/AKA-Challenge [RES, MAC]]
12. EAP Response/AKA-Challenge [RES, MAC]
13. EAP Success
14. Transfer EAP [EAP Success]
15. Transfer keys for WLAN access [MSK, EMSK]

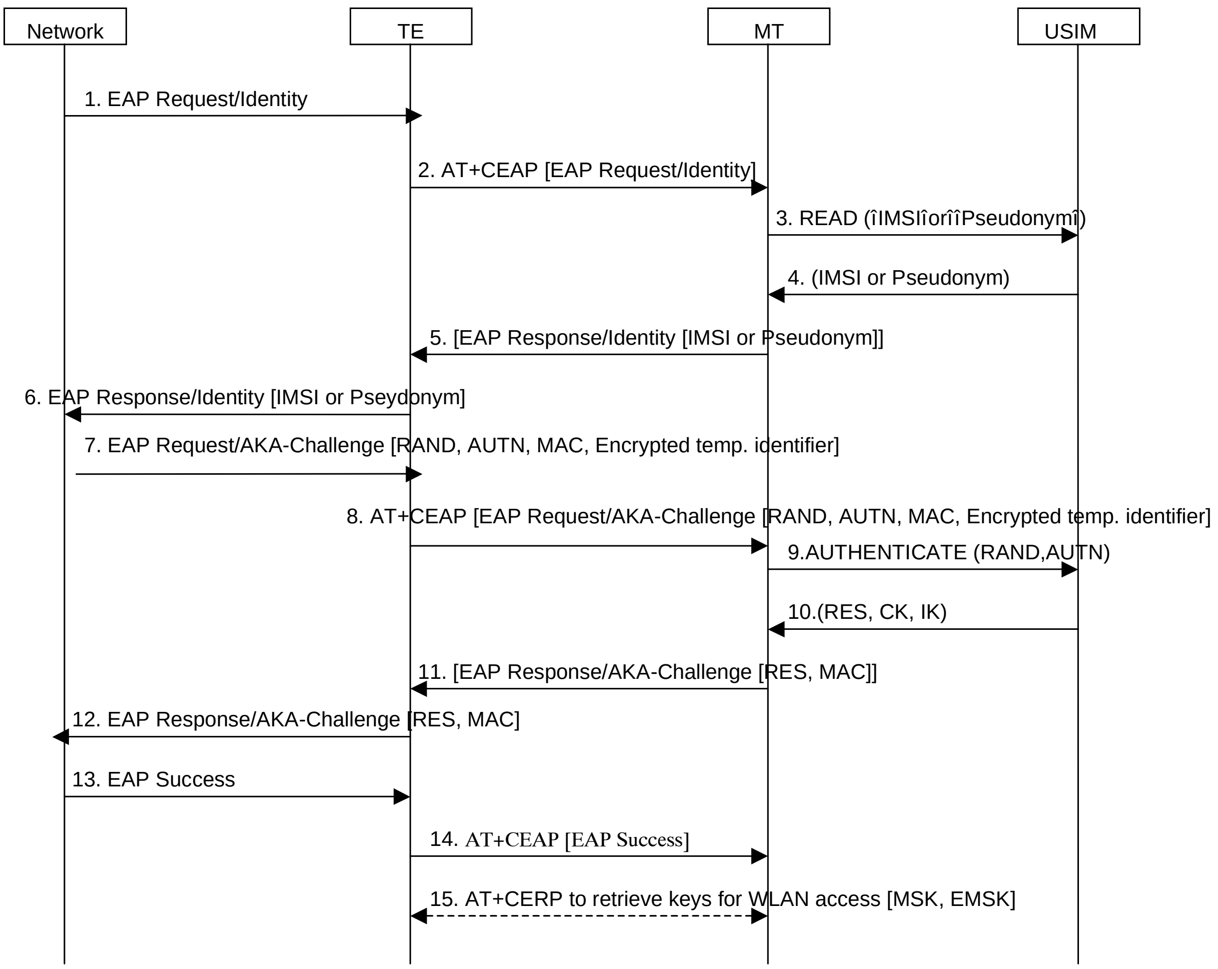

Network
TE
MT
USIM
1. EAP Request/Identity
2. AT+CEAP [EAP Request/Identity]
3. READ (îIMSIîorîîPseudonymî)
4. (IMSI or Pseudonym)
5. [EAP Response/Identity [IMSI or Pseudonym]]
6. EAP Response/Identity [IMSI or Pseydonym]
7. EAP Request/AKA-Challenge [RAND, AUTN, MAC, Encrypted temp. identifier]
8. AT+CEAP [EAP Request/AKA-Challenge [RAND, AUTN, MAC, Encrypted temp. identifier]
9.AUTHENTICATE (RAND,AUTN)
10.(RES, CK, IK)
11. [EAP Response/AKA-Challenge [RES, MAC]]
12. EAP Response/AKA-Challenge [RES, MAC]
13. EAP Success
14. AT+CEAP [EAP Success]
15. AT+CERP to retrieve keys for WLAN access [MSK, EMSK]

Figure 12~~1~~: 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 EAP request identity message is forwarded via the Bluetooth interface to the MT.~~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 ~~requests~~ sends the authentication ~~vectors from~~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 ~~and send them to the TE~~, using the +CERP AT command. ~~The TE uses them for security purposes, for example for WLAN link layer security~~

6.7.2 Full authentication with EAP SIM

6.7.2.1 Termination in the UICC

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

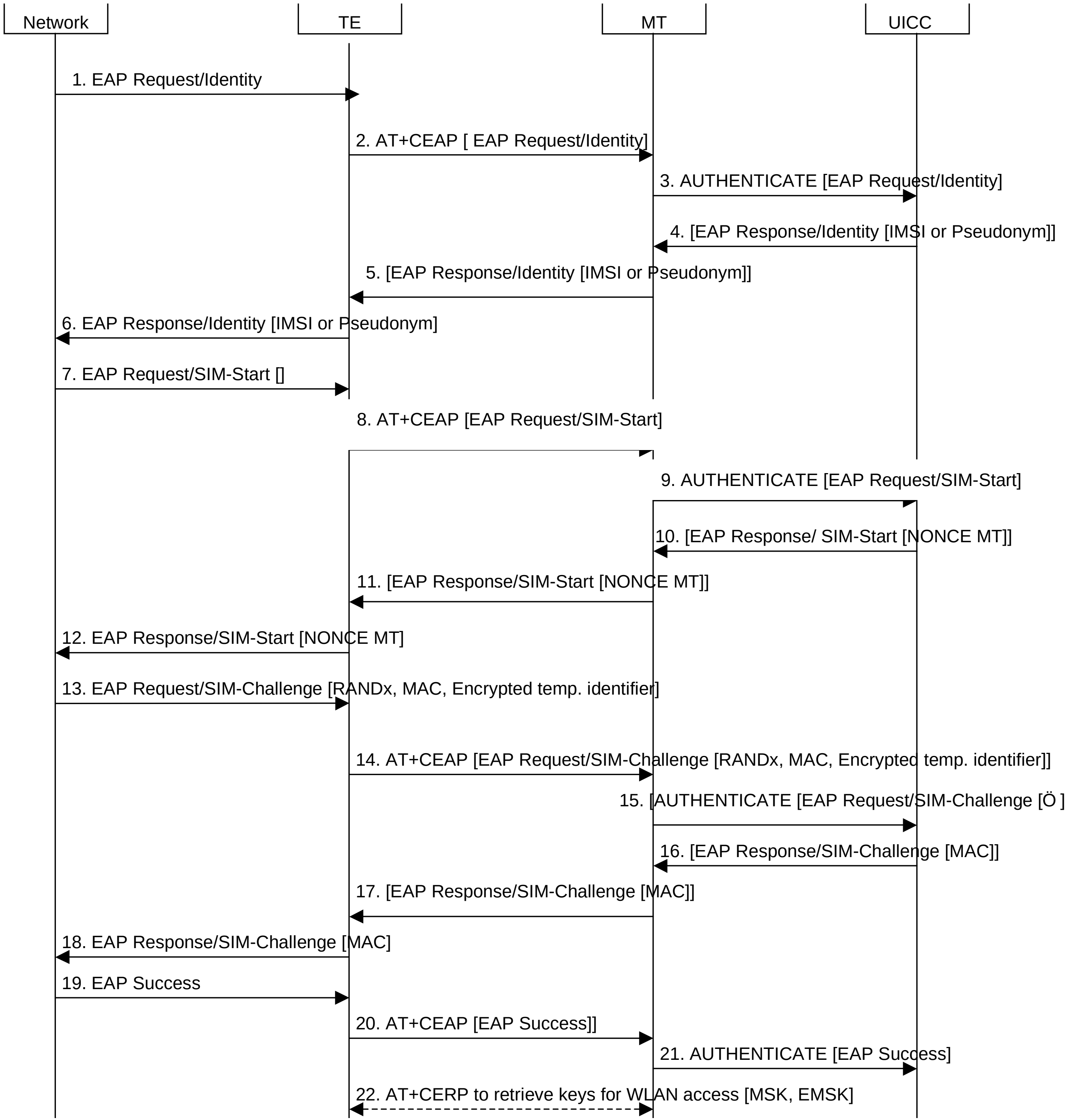

Network
TE
MT
UICC
1. EAP Request/Identity
2. AT+CEAP [EAP Request/Identity]
3. AUTHENTICATE [EAP Request/Identity]
4. [EAP Response/Identity [IMSI or Pseudonym]]
5. [EAP Response/Identity [IMSI or Pseudonym]]
6. EAP Response/Identity [IMSI or Pseudonym]
7. EAP Request/SIM-Start []
8. AT+CEAP [EAP Request/SIM-Start]
9. AUTHENTICATE [EAP Request/SIM-Start]
10. [EAP Response/ SIM-Start [NONCE MT]]
11. [EAP Response/SIM-Start [NONCE MT]]
12. EAP Response/SIM-Start [NONCE MT]
13. EAP Request/SIM-Challenge [RANDx, MAC, Encrypted temp. identifier]
14. AT+CEAP [EAP Request/SIM-Challenge [RANDx, MAC, Encrypted temp. identifier]]
15. [AUTHENTICATE [EAP Request/SIM-Challenge [Ö]
16. [EAP Response/SIM-Challenge [MAC]]
17. [EAP Response/SIM-Challenge [MAC]]
18. EAP Response/SIM-Challenge [MAC]
19. EAP Success
20. AT+CEAP [EAP Success]]
21. AUTHENTICATE [EAP Success]
22. AT+CERP to retrieve keys for WLAN access [MSK, EMSK]

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 [38], and shall select the appropriate DF, as indicated in TS 102.310 [39].

3. The MT performs the received +CEAP AT command (see TS 27.007 [38])

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 [38]).

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 [38]).

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.

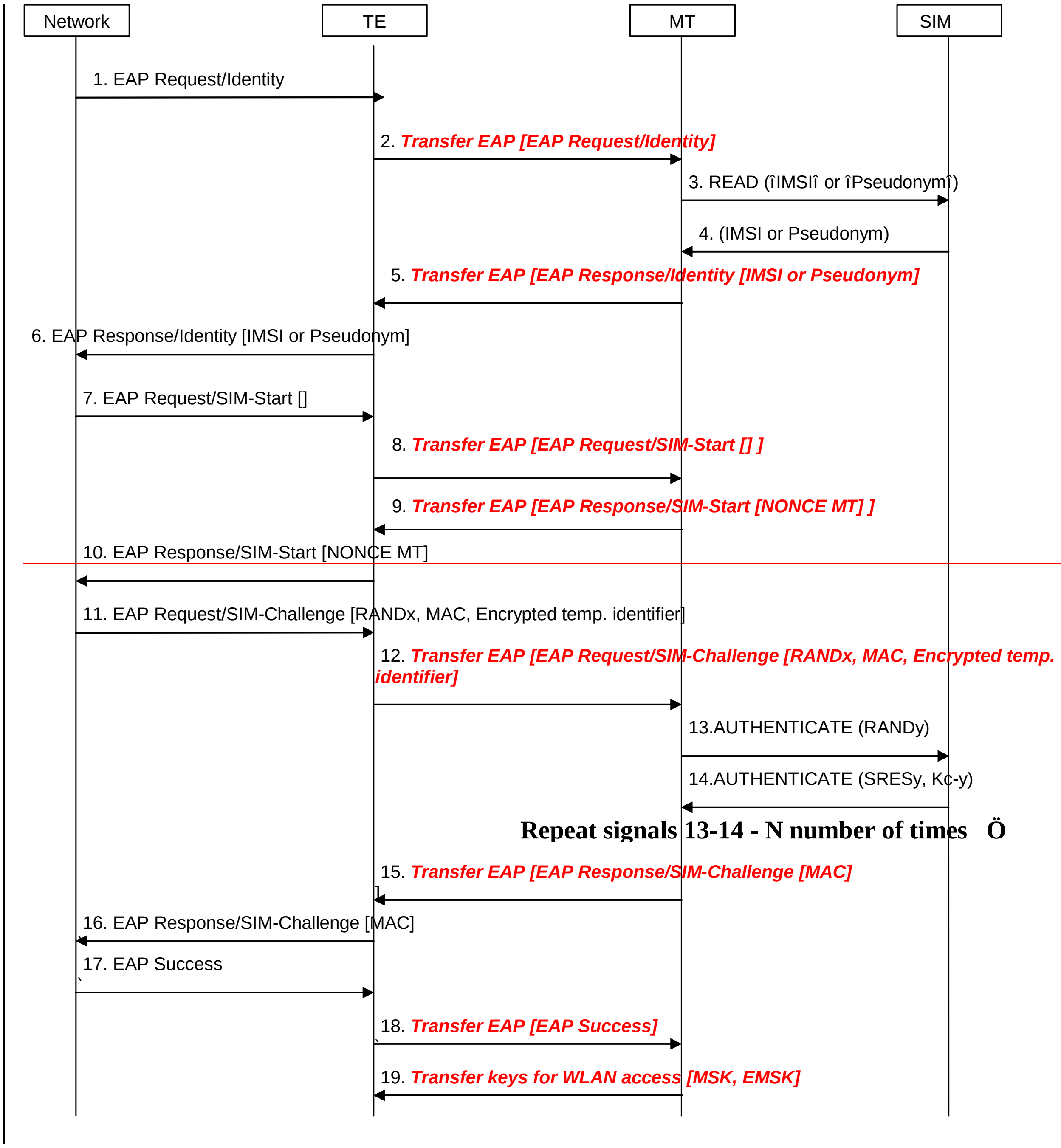
20. The TE sends the EAP packet received in message 19 to the UICC application using +CEAP AT command.

21. The MT performs the received +CEAP AT command (see TS 27.007 [38]).

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

~~The process is shown in figure 12, and itís very similar to EAP AKA (from MT-TE interface point of view).~~


Network
TE
MT
SIM
1. EAP Request/Identity
2. Transfer EAP [EAP Request/Identity]
3. READ (îIMSIî or îPseudonymî)
4. (IMSI or Pseudonym)
5. Transfer EAP [EAP Response/Identity [IMSI or Pseudonym]
6. EAP Response/Identity [IMSI or Pseudonym]
7. EAP Request/SIM-Start []
8. Transfer EAP [EAP Request/SIM-Start []]
9. Transfer EAP [EAP Response/SIM-Start [NONCE MT]]
10. EAP Response/SIM-Start [NONCE MT]
11. EAP Request/SIM-Challenge [RANDx, MAC, Encrypted temp. identifier]
12. Transfer EAP [EAP Request/SIM-Challenge [RANDx, MAC, Encrypted temp. identifier]
13.AUTHENTICATE (RANDy)
14.AUTHENTICATE (SRESy, Kc-y)
Repeat signals 13-14 - N number of times Ö
15. Transfer EAP [EAP Response/SIM-Challenge [MAC]
]
16. EAP Response/SIM-Challenge [MAC]
17. EAP Success
18. Transfer EAP [EAP Success]
19. Transfer keys for WLAN access [MSK, EMSK]

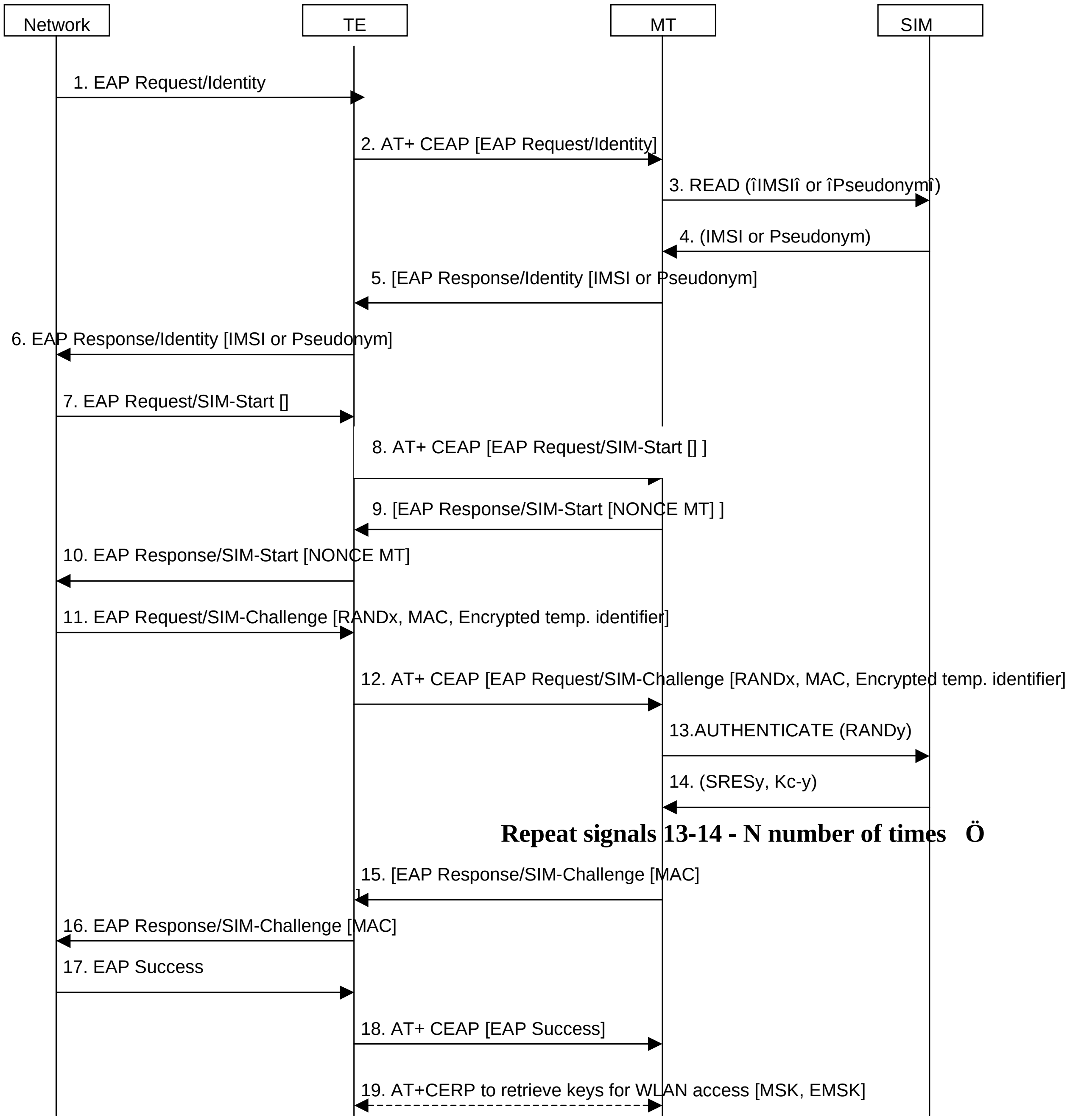

Network
TE
MT
SIM
1. EAP Request/Identity
2. AT+ CEAP [EAP Request/Identity]
3. READ (îIMSIî or îPseudonymî)
4. (IMSI or Pseudonym)
5. [EAP Response/Identity [IMSI or Pseudonym]
6. EAP Response/Identity [IMSI or Pseudonym]
7. EAP Request/SIM-Start []
8. AT+ CEAP [EAP Request/SIM-Start []]
9. [EAP Response/SIM-Start [NONCE MT]]
10. EAP Response/SIM-Start [NONCE MT]
11. EAP Request/SIM-Challenge [RANDx, MAC, Encrypted temp. identifier]
12. AT+ CEAP [EAP Request/SIM-Challenge [RANDx, MAC, Encrypted temp. identifier]
13.AUTHENTICATE (RANDy)
14. (SRESy, Kc-y)
Repeat signals 13-14 - N number of times Ö
15. [EAP Response/SIM-Challenge [MAC]
]
16. EAP Response/SIM-Challenge [MAC]
17. EAP Success
18. AT+ CEAP [EAP Success]
19. AT+CERP to retrieve keys for WLAN access [MSK, EMSK]

Figure 14~~2~~: 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. ~~The EAP request identity message is forwarded via the Bluetooth interface to the MT.~~
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 section 6.7.3 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 section 6.7.3.

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 ref. [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.

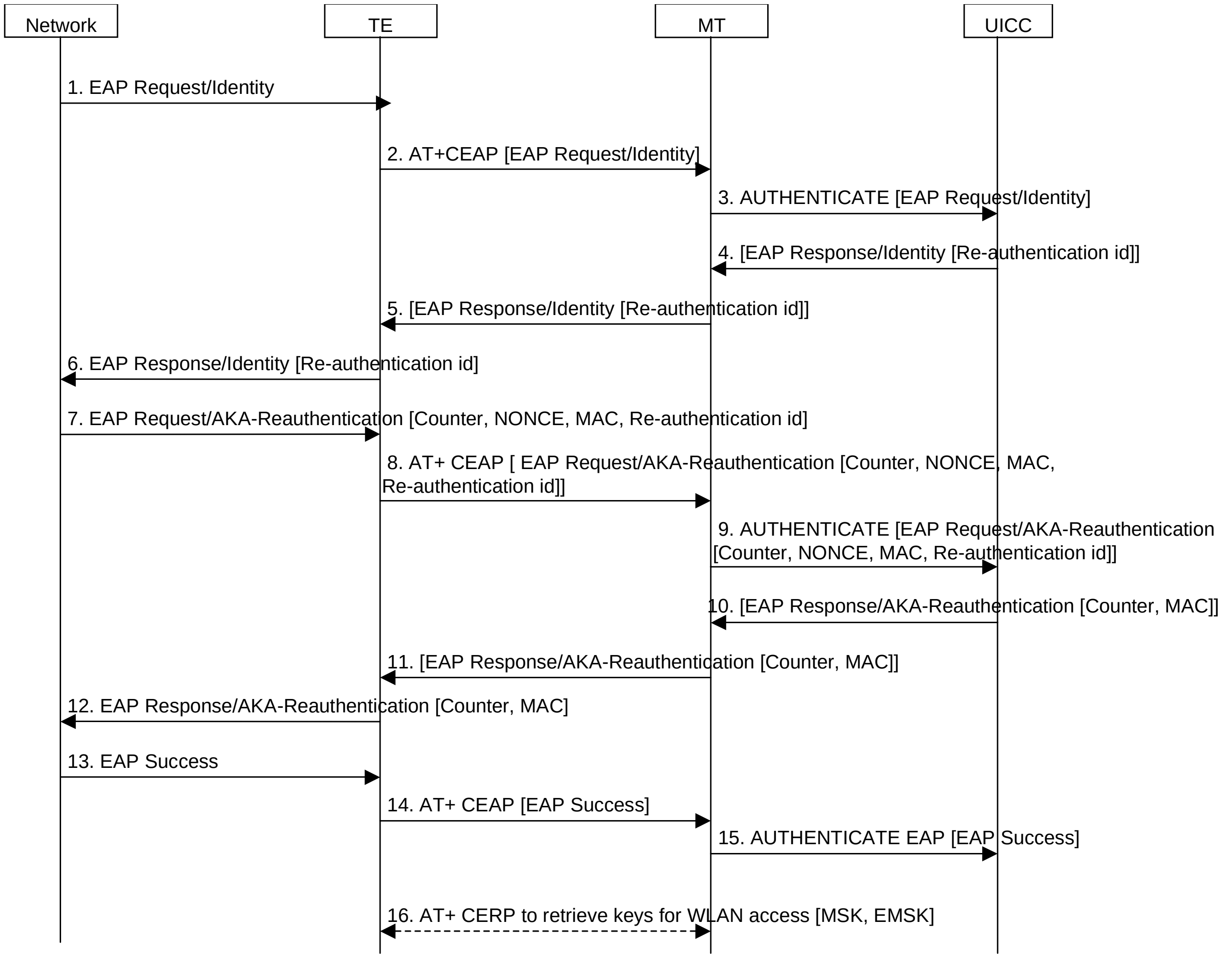

Network
TE
MT
UICC
1. EAP Request/Identity
2. AT+CEAP [EAP Request/Identity]
3. AUTHENTICATE [EAP Request/Identity]
4. [EAP Response/Identity [Re-authentication id]]
5. [EAP Response/Identity [Re-authentication id]]
6. EAP Response/Identity [Re-authentication id]
7. EAP Request/AKA-Reauthentication [Counter, NONCE, MAC, Re-authentication id]
8. AT+ CEAP [EAP Request/AKA-Reauthentication [Counter, NONCE, MAC, Re-authentication id]]
9. AUTHENTICATE [EAP Request/AKA-Reauthentication [Counter, NONCE, MAC, Re-authentication id]]
10. [EAP Response/AKA-Reauthentication [Counter, MAC]]
11. [EAP Response/AKA-Reauthentication [Counter, MAC]]
12. EAP Response/AKA-Reauthentication [Counter, MAC]
13. EAP Success
14. AT+ CEAP [EAP Success]
15. AUTHENTICATE EAP [EAP Success]
16. AT+ CERP to retrieve keys for WLAN access [MSK, EMSK]

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 [38]).

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 [38]).

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.

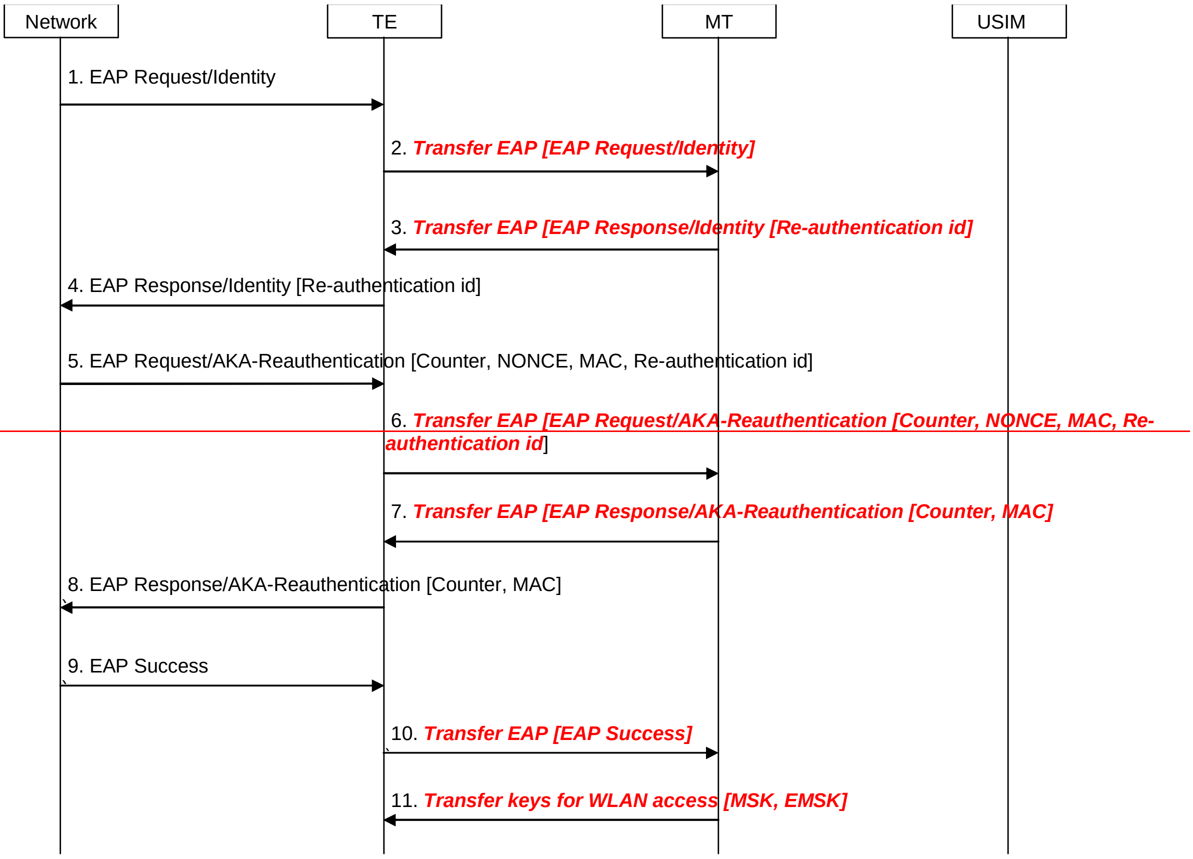
14. The TE sends the EAP packet received in message 13 to the UICC application using +CEAP AT command.

15. The MT performs the received +CEAP AT command (see TS 27.007 [38]).

16. After a successful EAP reauthentication, the TE shall retrieve the key material (i.e. MSK and EMSK) from EF$_{\text{EAPKEYS}}$ (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.

6.7.3.2 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 ref. [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~~3~~.


Network
TE
MT
USIM
1. EAP Request/Identity
2. Transfer EAP [EAP Request/Identity]
3. Transfer EAP [EAP Response/Identity [Re-authentication id]
4. EAP Response/Identity [Re-authentication id]
5. EAP Request/AKA-Reauthentication [Counter, NONCE, MAC, Re-authentication id]
6. Transfer EAP [EAP Request/AKA-Reauthentication [Counter, NONCE, MAC, Re-authentication id]
7. Transfer EAP [EAP Response/AKA-Reauthentication [Counter, MAC]
8. EAP Response/AKA-Reauthentication [Counter, MAC]
9. EAP Success
10. Transfer EAP [EAP Success]
11. Transfer keys for WLAN access [MSK, EMSK]

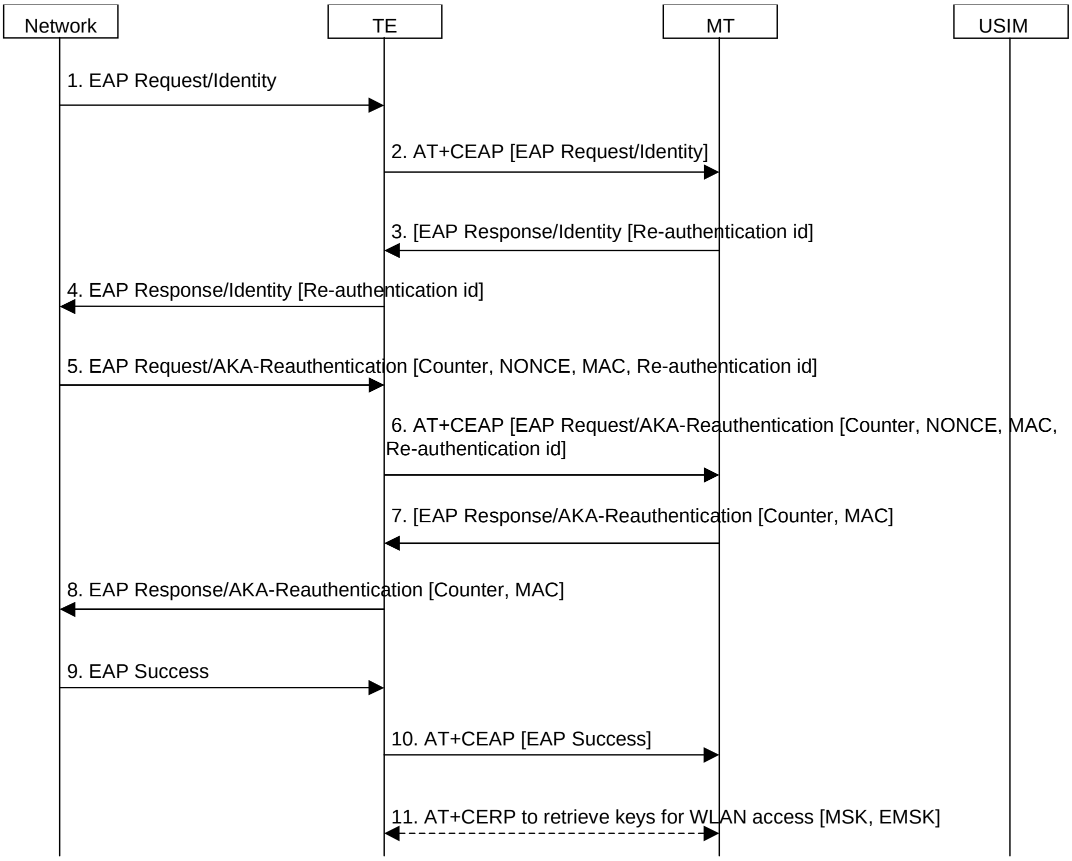

Network
TE
MT
USIM
1. EAP Request/Identity
2. AT+CEAP [EAP Request/Identity]
3. [EAP Response/Identity [Re-authentication id]
4. EAP Response/Identity [Re-authentication id]
5. EAP Request/AKA-Reauthentication [Counter, NONCE, MAC, Re-authentication id]
6. AT+CEAP [EAP Request/AKA-Reauthentication [Counter, NONCE, MAC, Re-authentication id]
7. [EAP Response/AKA-Reauthentication [Counter, MAC]
8. EAP Response/AKA-Reauthentication [Counter, MAC]
9. EAP Success
10. AT+CEAP [EAP Success]
11. AT+CERP to retrieve keys for WLAN access [MSK, EMSK]

Figure 16~~3~~: 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. ~~The TE forwards the message to the MT via the Bluetooth interface.~~
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 ref. [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.

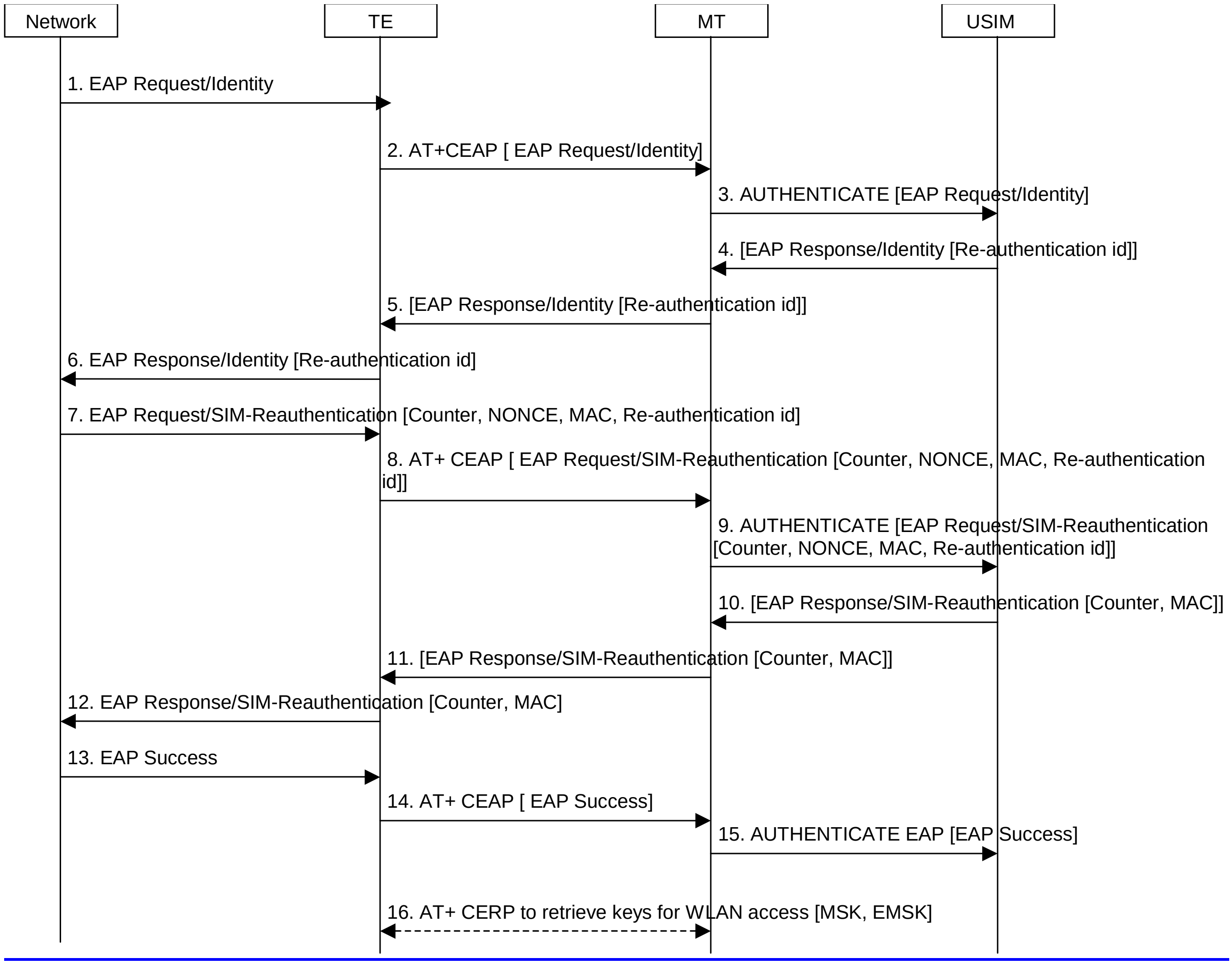

Network
TE
MT
USIM
1. EAP Request/Identity
2. AT+CEAP [EAP Request/Identity]
3. AUTHENTICATE [EAP Request/Identity]
4. [EAP Response/Identity [Re-authentication id]]
5. [EAP Response/Identity [Re-authentication id]]
6. EAP Response/Identity [Re-authentication id]
7. EAP Request/SIM-Reauthentication [Counter, NONCE, MAC, Re-authentication id]
8. AT+ CEAP [EAP Request/SIM-Reauthentication [Counter, NONCE, MAC, Re-authentication id]]
9. AUTHENTICATE [EAP Request/SIM-Reauthentication [Counter, NONCE, MAC, Re-authentication id]]
10. [EAP Response/SIM-Reauthentication [Counter, MAC]]
11. [EAP Response/SIM-Reauthentication [Counter, MAC]]
12. EAP Response/SIM-Reauthentication [Counter, MAC]
13. EAP Success
14. AT+ CEAP [EAP Success]
15. AUTHENTICATE EAP [EAP Success]
16. AT+ CERP to retrieve keys for WLAN access [MSK, EMSK]

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 [38]).
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 [38]).

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.

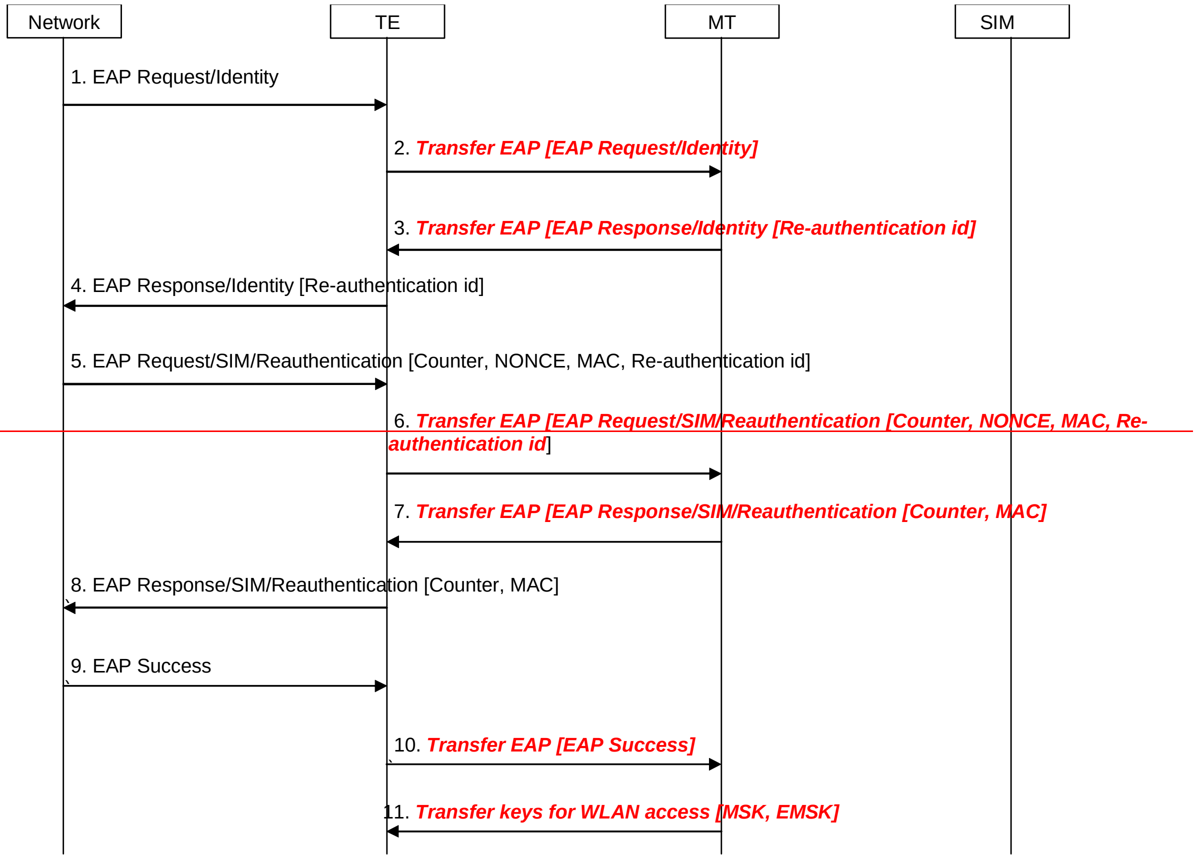
14. The TE sends the EAP packet received in message 13 to the UICC application using +CEAP AT command.

15. The MT performs the received +CEAP AT command (see TS 27.007 [38]).

16. After a successful EAP reauthentication, 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

6.7.4.2 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 184.


Network
TE
MT
SIM
1. EAP Request/Identity
2. Transfer EAP [EAP Request/Identity]
3. Transfer EAP [EAP Response/Identity [Re-authentication id]
4. EAP Response/Identity [Re-authentication id]
5. EAP Request/SIM/Reauthentication [Counter, NONCE, MAC, Re-authentication id]
6. Transfer EAP [EAP Request/SIM/Reauthentication [Counter, NONCE, MAC, Re-authentication id]
7. Transfer EAP [EAP Response/SIM/Reauthentication [Counter, MAC]
8. EAP Response/SIM/Reauthentication [Counter, MAC]
9. EAP Success
10. Transfer EAP [EAP Success]
11. Transfer keys for WLAN access [MSK, EMSK]

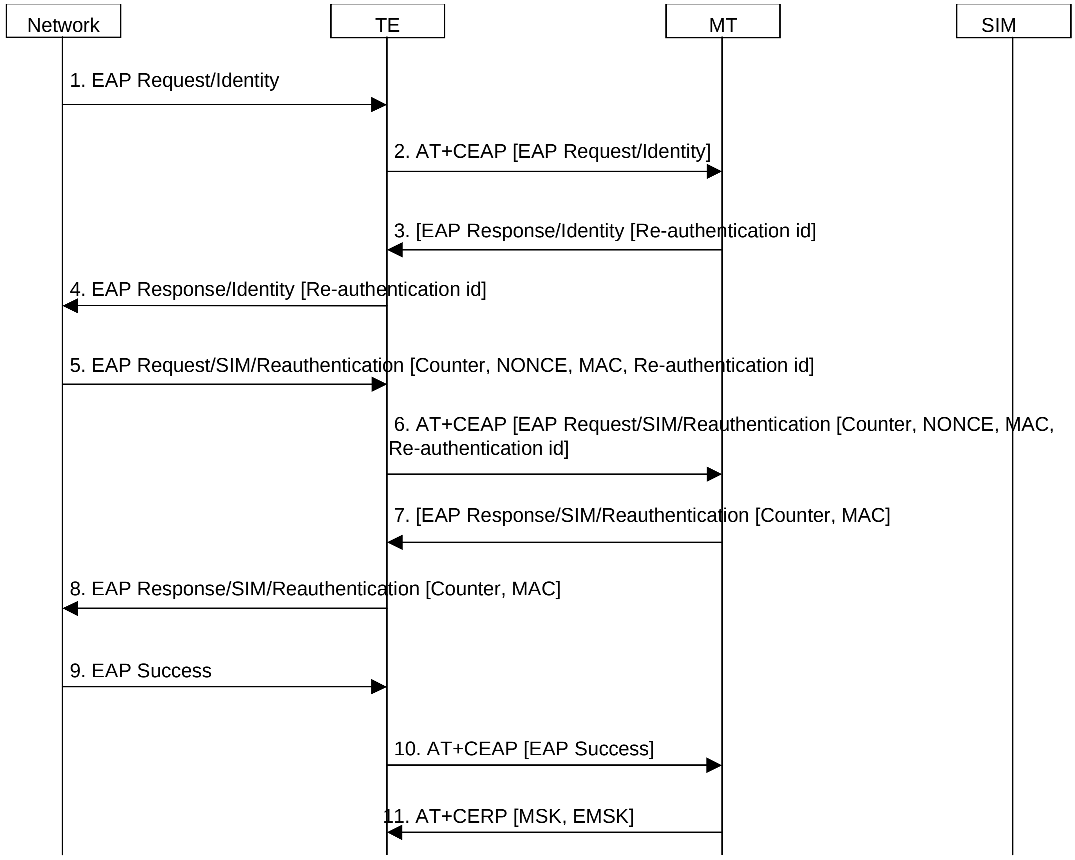

Network
TE
MT
SIM
1. EAP Request/Identity
2. AT+CEAP [EAP Request/Identity]
3. [EAP Response/Identity [Re-authentication id]
4. EAP Response/Identity [Re-authentication id]
5. EAP Request/SIM/Reauthentication [Counter, NONCE, MAC, Re-authentication id]
6. AT+CEAP [EAP Request/SIM/Reauthentication [Counter, NONCE, MAC, Re-authentication id]
7. [EAP Response/SIM/Reauthentication [Counter, MAC]
8. EAP Response/SIM/Reauthentication [Counter, MAC]
9. EAP Success
10. AT+CEAP [EAP Success]
11. AT+CERP [MSK, EMSK]

Figure 184: 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. ~~The TE forwards the message to the MT via the Bluetooth interface.~~

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~~MT~~ 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.

3GPP TSG SA WG3 Security ó S3#35 **Tdoc ⌘S3-040763**
October 5 ñ 8, 2004

St Paulís Bay, Malta

CR-Form-v7

CHANGE REQUEST

⌘	**33.234**	**CR**	**028**	⌘ **rev**	**-**	⌘ Current version:	**6.2.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects:	UICC apps⌘ □	ME ☒	Radio Access Network □	Core Network ☒

Title:	⌘	Passing keying material to the WLAN-AN during the Fast re-authentication procedure		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	23/06/2004
Category:	⌘	**F**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	(GSM Phase 2)
R96	(Release 1996)
R97	(Release 1997)
R98	(Release 1998)
R99	(Release 1999)
Rel-4	(Release 4)
Rel-5	(Release 5)
Rel-6	(Release 6)

Reason for change:	⌘	According to the current specification, the newly generated keying material after the fast re-authentication is not transmitted to the WLAN-AN. WLAN-AN cannot refresh the WEP key after the fast re-authentication procedure.
Summary of change:	⌘	It is necessary to pass the newly derived key materials from the AAA server to the WLAN AN with the EAP-success message after the Fast re-authentication procedure, so that WLAN AN stores the keying material to be used in communication with the authenticated WLAN-UE.
Consequences if not approved:	⌘	UE and WLAN AN will have different keying material after Fast re-authentication procedure. So communcation with the authenticated WLAN-UE is not possible.

Clauses affected:	⌘	6.1.4			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

*** BEGIN SET OF CHANGES ***

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.

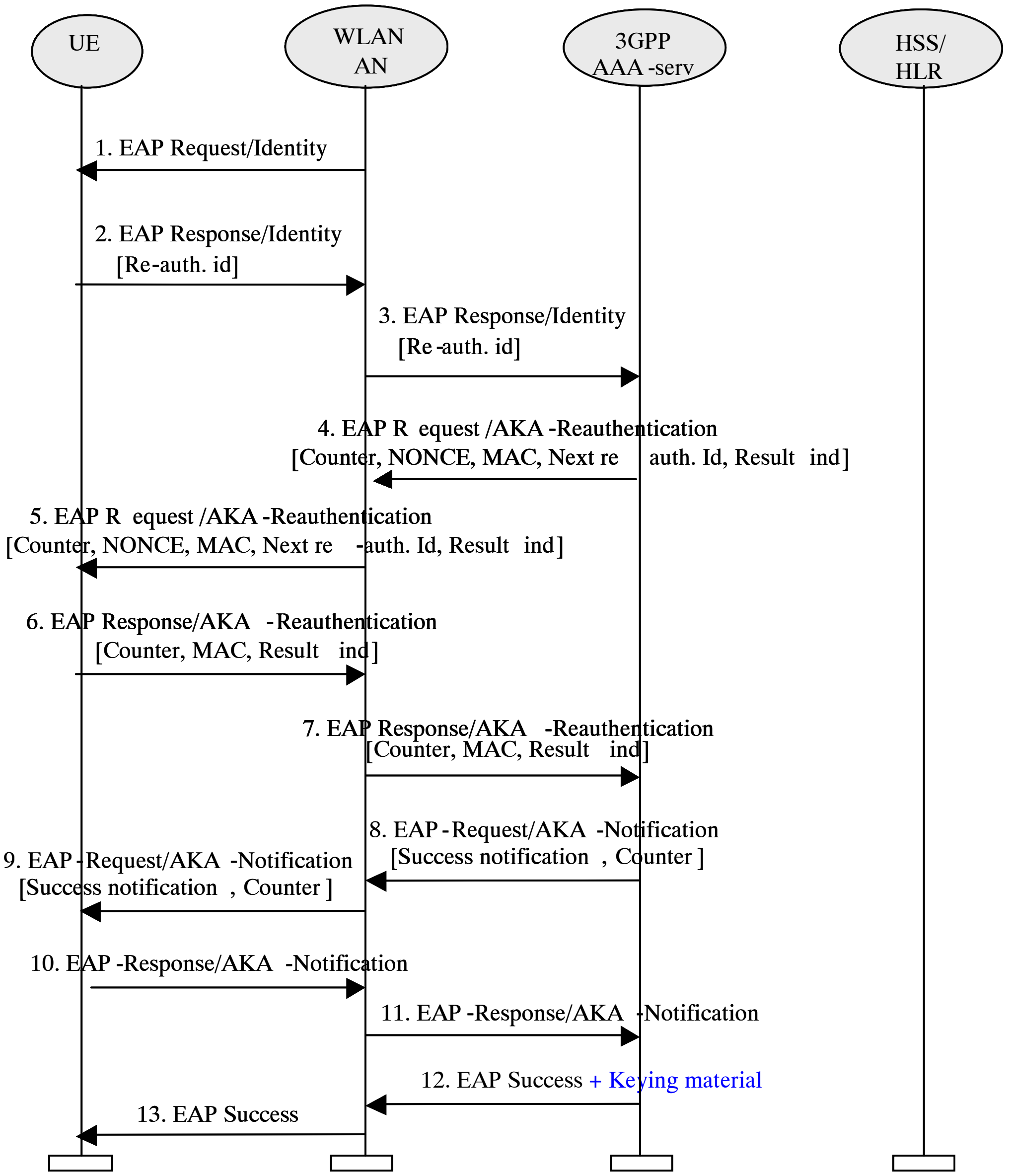

UE
WLAN AN
3GPP AAA -serv
HSS/ HLR
1. EAP Request/Identity
2. EAP Response/Identity [Re-auth. id]
3. EAP Response/Identity [Re-auth. id]
4. EAP Request /AKA -Reauthentication [Counter, NONCE, MAC, Next re-auth. Id, Result ind]
5. EAP Request /AKA -Reauthentication [Counter, NONCE, MAC, Next re-auth. Id, Result ind]
6. EAP Response/AKA -Reauthentication [Counter, MAC, Result ind]
7. EAP Response/AKA -Reauthentication [Counter, MAC, Result ind]
8. EAP-Request/AKA -Notification [Success notification , Counter]
9. EAP-Request/AKA -Notification [Success notification , Counter]
10. EAP -Response/AKA -Notification
11. EAP -Response/AKA -Notification
12. EAP Success + Keying material
13. EAP Success

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 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.
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.

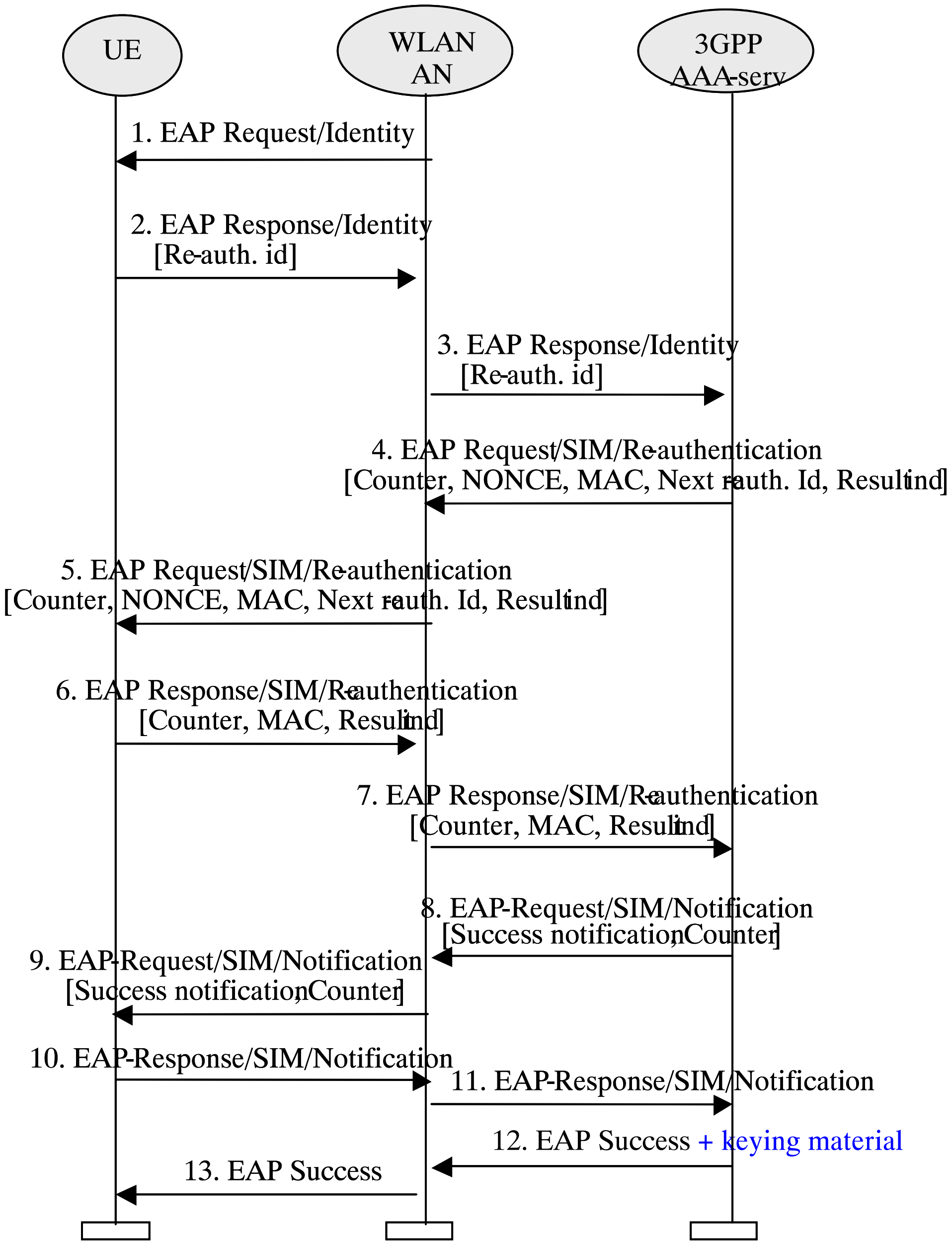

UE
WLAN AN
3GPP AAA-serv
1. EAP Request/Identity
2. EAP Response/Identity [Re-auth. id]
3. EAP Response/Identity [Re-auth. id]
4. EAP Request/SIM/Re-authentication [Counter, NONCE, MAC, Next re-auth. Id, Result ind]
5. EAP Request/SIM/Re-authentication [Counter, NONCE, MAC, Next re-auth. Id, Result ind]
6. EAP Response/SIM/Re-authentication [Counter, MAC, Result ind]
7. EAP Response/SIM/Re-authentication [Counter, MAC, Result ind]
8. EAP-Request/SIM/Notification [Success notification, Counter]
9. EAP-Request/SIM/Notification [Success notification, Counter]
10. EAP-Response/SIM/Notification
11. EAP-Response/SIM/Notification
12. EAP Success + keying material
13. EAP Success

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 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.

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.

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Security ó S3#35 **Tdoc ⌘S3-040837**
October 5 ñ 8, 2004, St Paulís Bay, Malta

CR-Form-v7

CHANGE REQUEST

⌘ **33.234 CR 029** ⌘ **rev 1** ⌘ Current version: **6.2.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Clarification on Deletion of Temporary IDs
Source:	⌘	SA WG3
Work item code:	⌘	WLAN
Date:	⌘	23/06/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Temporary IDs should not be deleted untill the EAP Authentication process completes, as the IDs are passed again in the EAP Authentication procedure to detect MITM attack.
Summary of change:	⌘	The same temporary IDs are used when the AAA server request again to detect MITM attack
Consequences if not approved:	⌘	If AAA server request for the ID again, then the WLAN-UE cannot pass the same ID as it marked as deleted.

Clauses affected:	⌘	5.1.6

Other specs Affected: ⌘

Y	N		
	X	Other core specifications	⌘
	X	Test specifications	
	X	O&M Specifications	

Other comments: ⌘

*** BEGIN SET OF CHANGES ***

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 ~~so that they can only be used once~~ as ì deletedî 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 scenario 3, 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).
An exception is when the full authentication is being performed for tunnel establishment in scenario 3, in which case the IMSI may be sent even if identity privacy support was activated by the home network. In this situation, the authentication exchange is performed in a protected tunnel which provides encryption and integrity protection, as well as replay protection.

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 pseudonyms, 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 pseudonym.

If identity privacy is used but the AAA server cannot identify the user by its pseudonym, the AAA server requests the user 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.

Editor's note: The use of PEAP with EAP/AKA and EAP/SIM is currently under consideration. If PEAP is used, the temporary identity privacy scheme provided by EAP/AKA and EAP/SIM is not needed.

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Security ó S3#35
October 5 ñ 8, 2004, St Paulís Bay, Malta

Tdoc ⌘S3-040765

CR-Form-v7

CHANGE REQUEST

⌘	**33.234**	**CR**	**030**	⌘ **rev**	**-** ⌘	Current version: **6.2.1** ⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Clarification on Protecting Re-authentication ID in FAST/FULL Re-Authentication procedure			
Source:	⌘	SA WG3			
Work item code:	⌘	WLAN	***Date:***	⌘	23/06/2004
Category:	⌘	**F**	***Release:***	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	As stated in the EAP SIM and EAP AKA drafts, the AAA server transmits the protected Re-authentication ID using encryption to the WLAN UE. But TS 33.234 does not clearly mention the protection of the re-authentication ID.
Summary of change:	⌘	As specified in the EAP SIM/AKA drafts, It is necessary to protect the re-authentication ID in the EAP authentication procedure.
Consequences if not approved:	⌘	Passing unprotected Re-authentication ID within EAP message will lead to attack against Identity privacy and also TS 33.234 not aligned with IETF drafts.

Clauses affected:	⌘	6.1				
		Y	**N**			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

*** BEGIN SET OF CHANGES ***

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 section 4.2. This form of authentication shall be based on EAP-AKA (ref. [4]), as described in section 6.1.1.1.

Editor's note: also see section 4.2.4 on WLAN-UE Functional Split.

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.

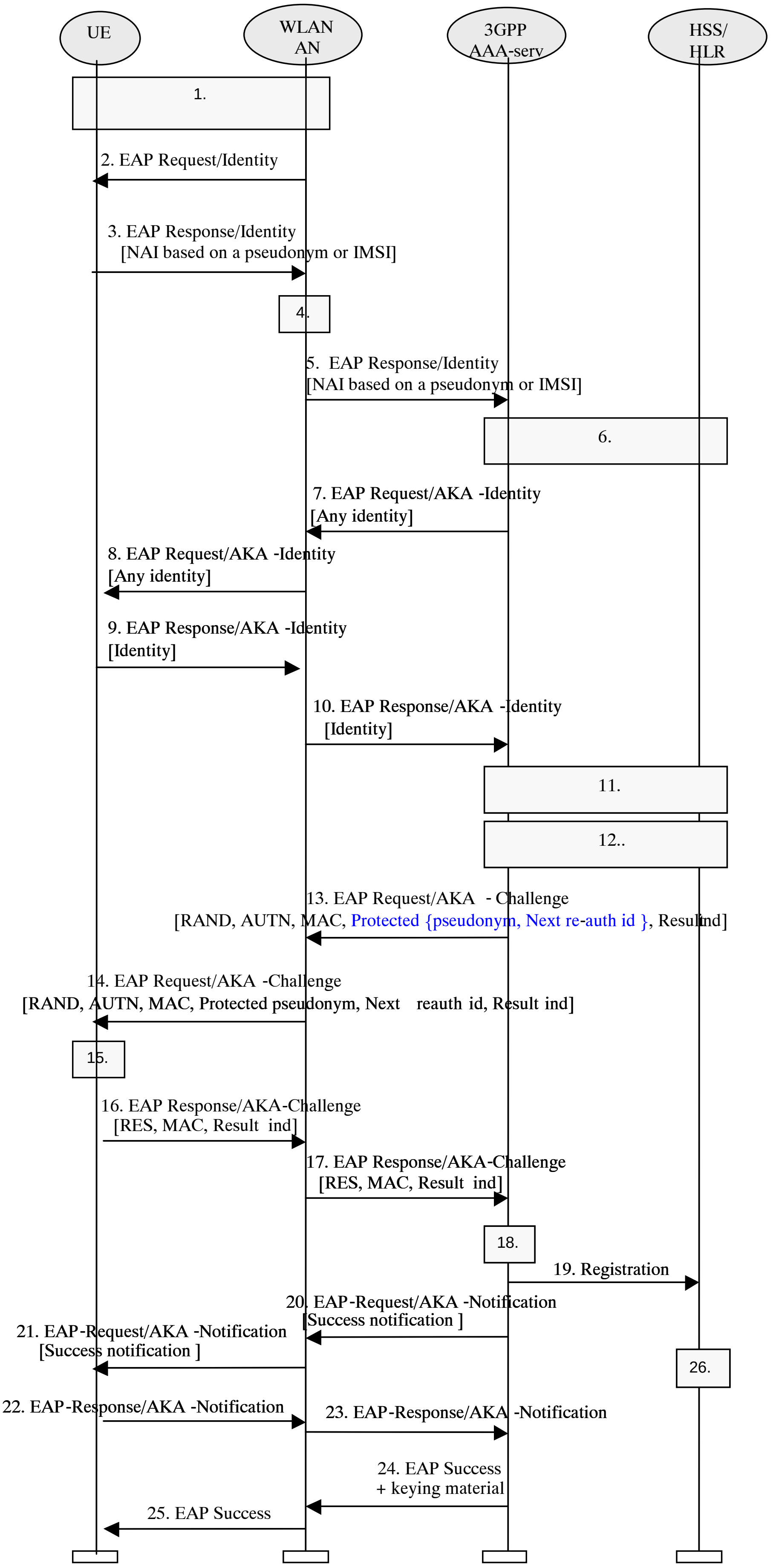

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity [NAI based on a pseudonym or IMSI]
4.
5. EAP Response/Identity [NAI based on a pseudonym or IMSI]
6.
7. EAP Request/AKA -Identity [Any identity]
8. EAP Request/AKA -Identity [Any identity]
9. EAP Response/AKA -Identity [Identity]
10. EAP Response/AKA -Identity [Identity]
11.
12..
13. EAP Request/AKA - Challenge [RAND, AUTN, MAC, Protected {pseudonym, Next re-auth id }, Result ind]
14. EAP Request/AKA -Challenge [RAND, AUTN, MAC, Protected pseudonym, Next reauth id, Result ind]
15.
16. EAP Response/AKA-Challenge [RES, MAC, Result ind]
17. EAP Response/AKA-Challenge [RES, MAC, Result ind]
18.
19. Registration
20. EAP-Request/AKA -Notification [Success notification]
21. EAP-Request/AKA -Notification [Success notification]
26.
22. EAP-Response/AKA -Notification
23. EAP-Response/AKA -Notification
24. EAP Success + keying material
25. EAP Success

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 RFC 2486. NAI contains either a temporary identifier (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 EAP/AKA [4].

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.

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 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 was received, then the WLAN-UE stores the pseudonym 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. 3GPP AAA Server checks the received MAC and compares XRES to the received RES. If successful, the AAA server shall compare the MAC address, VPLMN Identity and the WLAN radio 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 the old sessions (skip step 19).

19. Otherwise, the AAA server considers that the authentication exchange is related to a new scenario-2 session. In this case the AAA server shall contact the HSS for a decision. The AAA server shall inform to the HSS of the WLAN-UE's MAC address, the VPLMN Identity, as well as the identifier of the WLAN radio network used.

20. 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.

21. The WLAN AN forwards the message to the WLAN-UE.

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

23. 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

24. 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 EAP level). The WLAN-AN stores the keying material to be used in communication with the authenticated WLAN-UE.

25. 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.

26. If the same subscriber but different MAC address, or VPLMN identity or the radio network information is received than in any ongoing session, then the registration is related to a new scenario-2 session. The HSS shall close an old scenario-2 session by indicating to the 3GPP AAA server of the old session to terminate the session, based on the policy whether simultaneous sessions are not allowed, or whether the number of allowed sessions has been exceeded.

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 section 6.1.2.1. This authentication method satisfies the authentication requirements from section 4.2, without the need for a UICC with a USIM application

Editor's note: Also see section 4.2.4 on WLAN-UE split.

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.

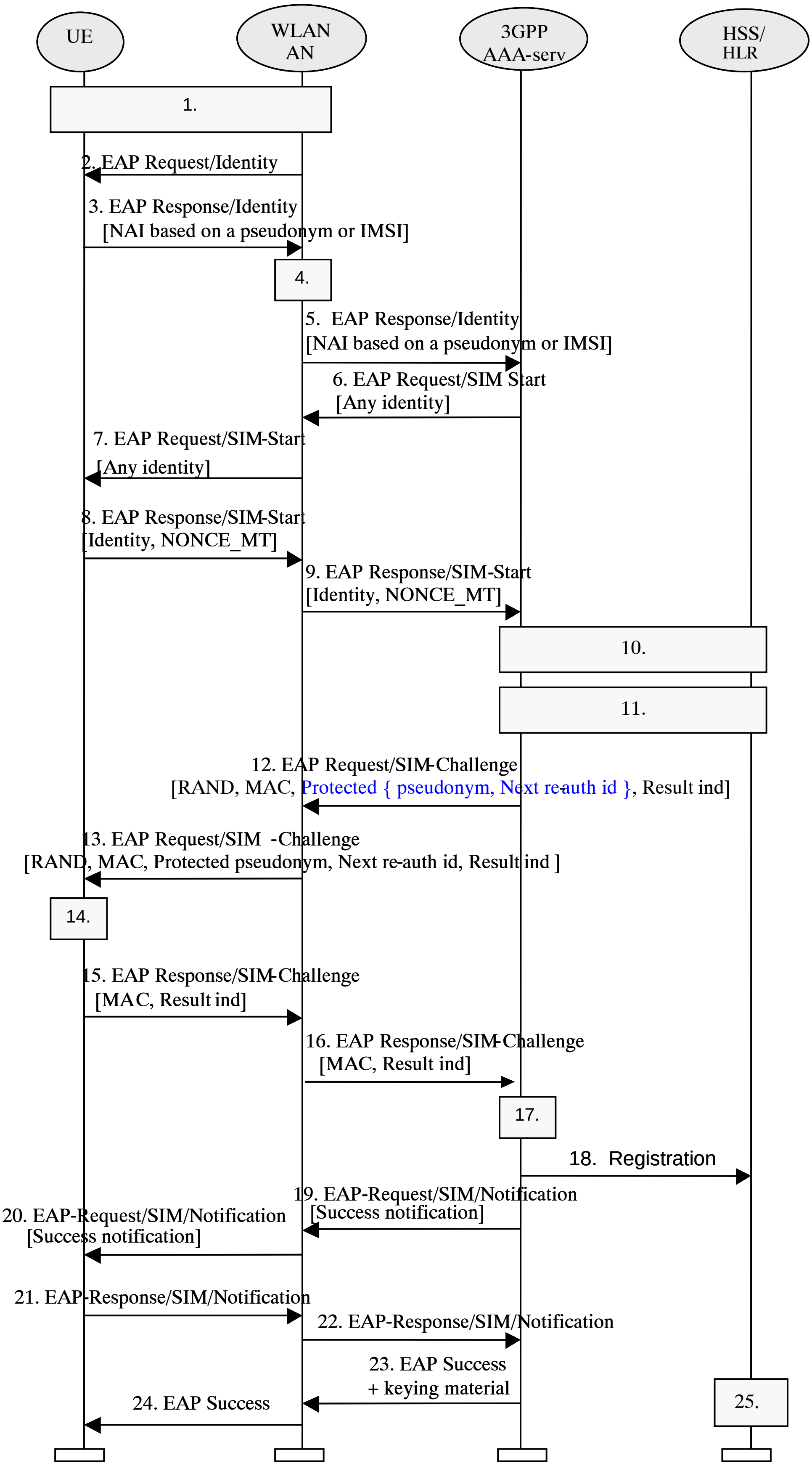

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity [NAI based on a pseudonym or IMSI]
4.
5. EAP Response/Identity [NAI based on a pseudonym or IMSI]
6. EAP Request/SIM Start [Any identity]
7. EAP Request/SIM-Start [Any identity]
8. EAP Response/SIM-Start [Identity, NONCE_MT]
9. EAP Response/SIM-Start [Identity, NONCE_MT]
10.
11.
12. EAP Request/SIM-Challenge [RAND, MAC, Protected { pseudonym, Next re-auth id }, Result ind]
13. EAP Request/SIM -Challenge [RAND, MAC, Protected pseudonym, Next re-auth id, Result ind]
14.
15. EAP Response/SIM-Challenge [MAC, Result ind]
16. EAP Response/SIM-Challenge [MAC, Result ind]
17.
18. Registration
19. EAP-Request/SIM/Notification [Success notification]
20. EAP-Request/SIM/Notification [Success notification]
21. EAP-Response/SIM/Notification
22. EAP-Response/SIM/Notification
23. EAP Success + keying material
24. EAP Success
25.

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 RFC 2486. NAI contains either a temporary identifier (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 EAP/SIM.

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 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.

    Although this step is presented after step 9 in this examples, 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).

11. The 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 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 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 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 was received, then the WLAN-UE stores the pseudonym for future authentications.

    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.

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

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. If successful, the AAA server shall compare the MAC address, VPLMN Identity and the WLAN radio 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 the old sessions (skip step 18).

18. Otherwise, the AAA server considers that the authentication exchange is related to a new scenario-2 session. In this case the AAA server shall contact the HSS/HLR for a decision. The AAA server shall inform the HSS/HLR of the WLAN-UEís MAC address, the VPLMN Identity, as well as the identifier of the WLAN radio network used.

19. 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.

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

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

22. 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.

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 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.

24. 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.

25. If the same subscriber but different MAC address, or VPLMN identity, or the radio network information is received than in any ongoing session, then the registration is related to a new scenario-2 session. The HSS/HLR shall close an old scenario-2 session by indicating to the 3GPP AAA server of the old session to terminate the session, based on whether simultaneous sessions are not allowed, or whether the number of allowed sessions has been exceeded.

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

Editors note: LS (S3-030187/ S1-030546) from SA1 has stated, "There are requests from operators for a secure SIM based WLAN authentication solution". SA3 has SA1 in an LS (S3-030306) if this request is confirmed. The input paper to SA3 on this can be found at: http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_28_Berlin/Docs/ZIP/S3-030198.zip

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.

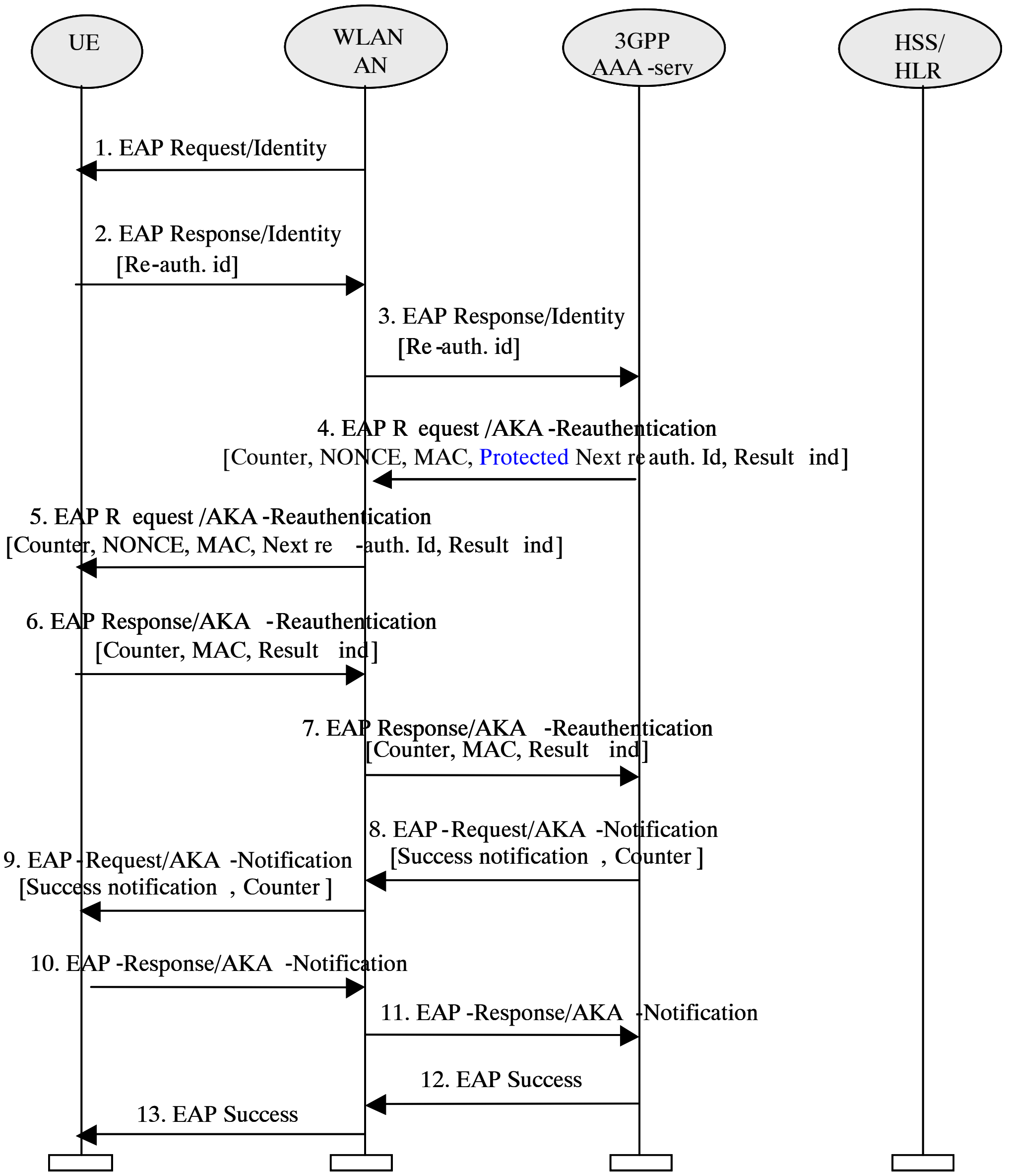

UE
WLAN AN
3GPP AAA -serv
HSS/ HLR
1. EAP Request/Identity
2. EAP Response/Identity [Re-auth. id]
3. EAP Response/Identity [Re -auth. id]
4. EAP R equest /AKA -Reauthentication [Counter, NONCE, MAC, Protected Next re auth. Id, Result ind]
5. EAP R equest /AKA -Reauthentication [Counter, NONCE, MAC, Next re -auth. Id, Result ind]
6. EAP Response/AKA -Reauthentication [Counter, MAC, Result ind]
7. EAP Response/AKA -Reauthentication [Counter, MAC, Result ind]
8. EAP -Request/AKA -Notification [Success notification , Counter]
9. EAP -Request/AKA -Notification [Success notification , Counter]
10. EAP -Response/AKA -Notification
11. EAP -Response/AKA -Notification
12. EAP Success
13. EAP Success

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.

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.
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.

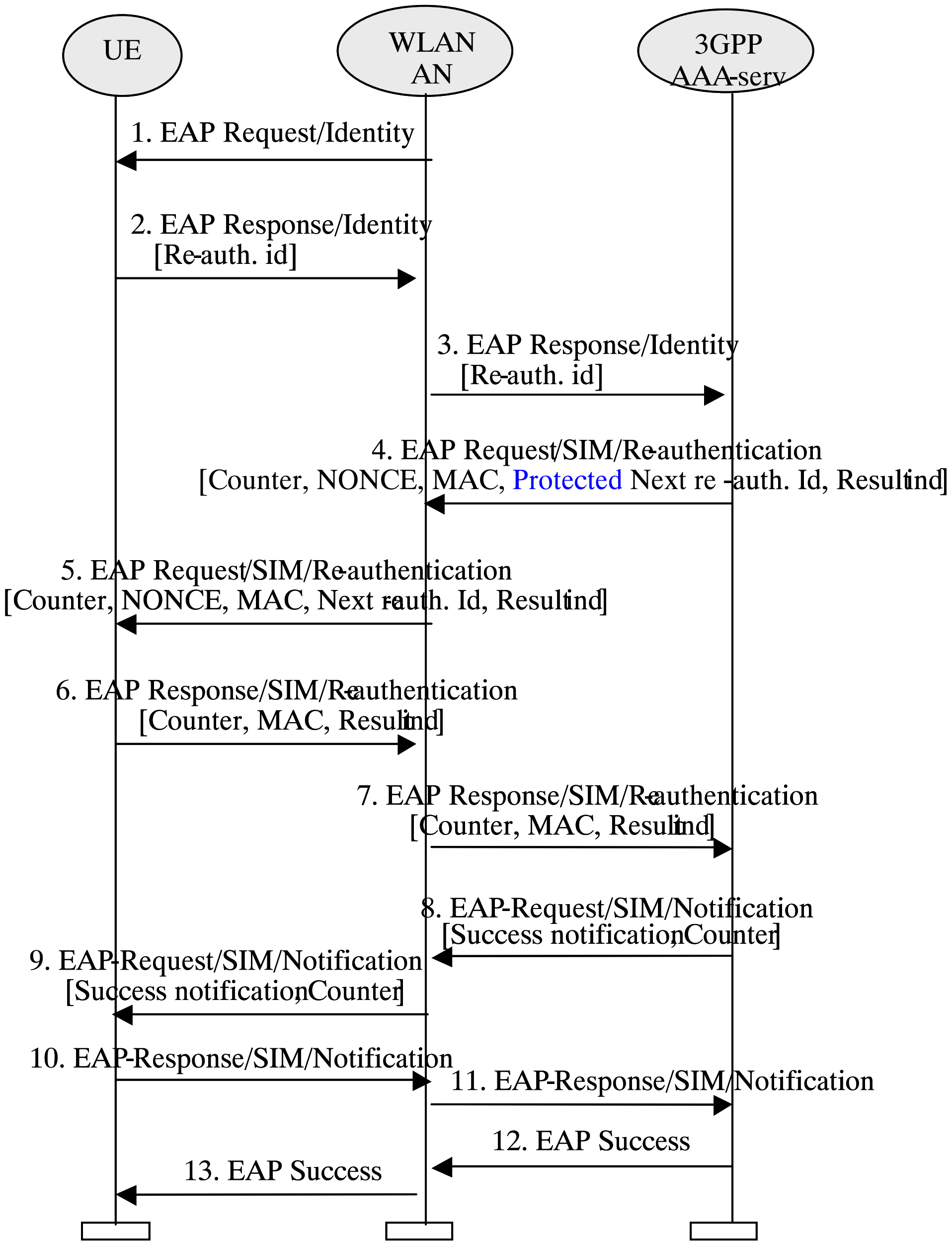

UE
WLAN AN
3GPP AAA-serv
1. EAP Request/Identity
2. EAP Response/Identity [Re-auth. id]
3. EAP Response/Identity [Re-auth. id]
4. EAP Request/SIM/Re-authentication [Counter, NONCE, MAC, Protected Next re -auth. Id, Result ind]
5. EAP Request/SIM/Re-authentication [Counter, NONCE, MAC, Next re-auth. Id, Result ind]
6. EAP Response/SIM/Re-authentication [Counter, MAC, Result ind]
7. EAP Response/SIM/Re-authentication [Counter, MAC, Result ind]
8. EAP-Request/SIM/Notification [Success notification, Counter]
9. EAP-Request/SIM/Notification [Success notification, Counter]
10. EAP-Response/SIM/Notification
11. EAP-Response/SIM/Notification
12. EAP Success
13. EAP Success

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.
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.
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.

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Security ó S3#35 **Tdoc ⌘S3-040766**
October 5 ñ 8, 2004, St Paulís Bay, Malta

CR-Form-v7

CHANGE REQUEST

⌘	**33.234**	**CR**	**031**	⌘ **rev**	**-**	⌘ Current version:	**6.2.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Assigning Remote IP Address to WLAN UE using IKEv2 configuration Payload		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	23/06/2004
Category:	⌘	**B**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Assignment of Remote IP address to WLAN-UE by PLMN is mentioned as necessary functionality and requirement, but the mechanism of obtaining Remote IP Address is not addressed.
Summary of change:	⌘	Add feature on assigning Remote IP address to the WLAN UE
Consequences if not approved:	⌘	No method defined for WLAN UE to obtain the Remote IP address during the tunnel setup Procedure.

Clauses affected:	⌘	6.1.5.1, 6.1.5.2			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

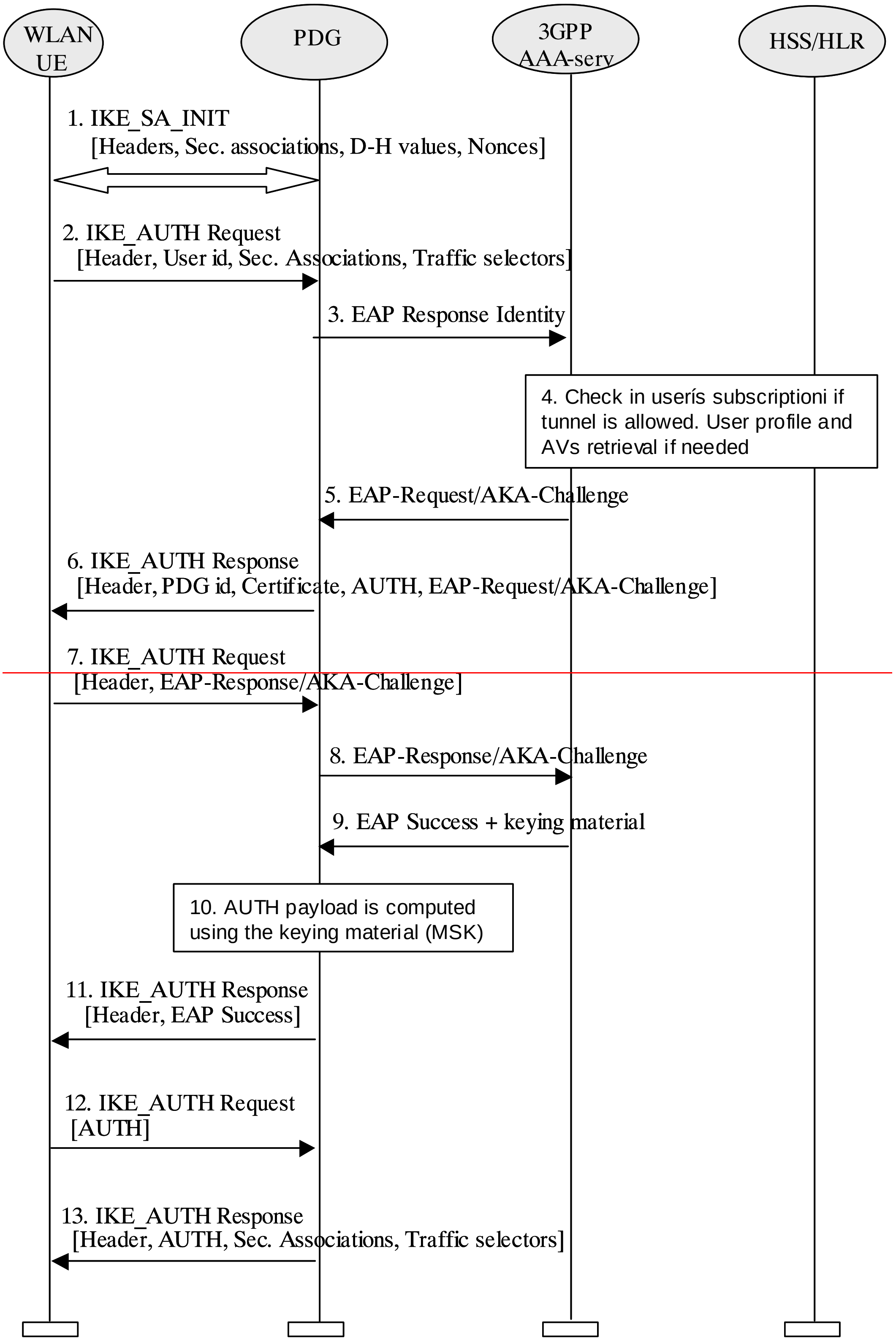
*** BEGIN SET OF CHANGES ***

6.1.5.1 Tunnel full authentication and authorization

The tunnel end point in the network is the PDG. 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 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 AAA server over Diameter (the opposite for messages sent from the AAA server). 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 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 AAA server is certain that no intermediate node has modified or changed the user identity.


WLAN UE
PDG
3GPP AAA-serv
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request
[Header, User id, Sec. Associations, Traffic selectors]
3. EAP Response Identity
4. Check in userís subscriptioni if tunnel is allowed. User profile and AVs retrieval if needed
5. EAP-Request/AKA-Challenge
6. IKE_AUTH Response
[Header, PDG id, Certificate, AUTH, EAP-Request/AKA-Challenge]
7. IKE_AUTH Request
[Header, EAP-Response/AKA-Challenge]
8. EAP-Response/AKA-Challenge
9. EAP Success + keying material
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response
[Header, EAP Success]
12. IKE_AUTH Request
[AUTH]
13. IKE_AUTH Response
[Header, AUTH, Sec. Associations, Traffic selectors]

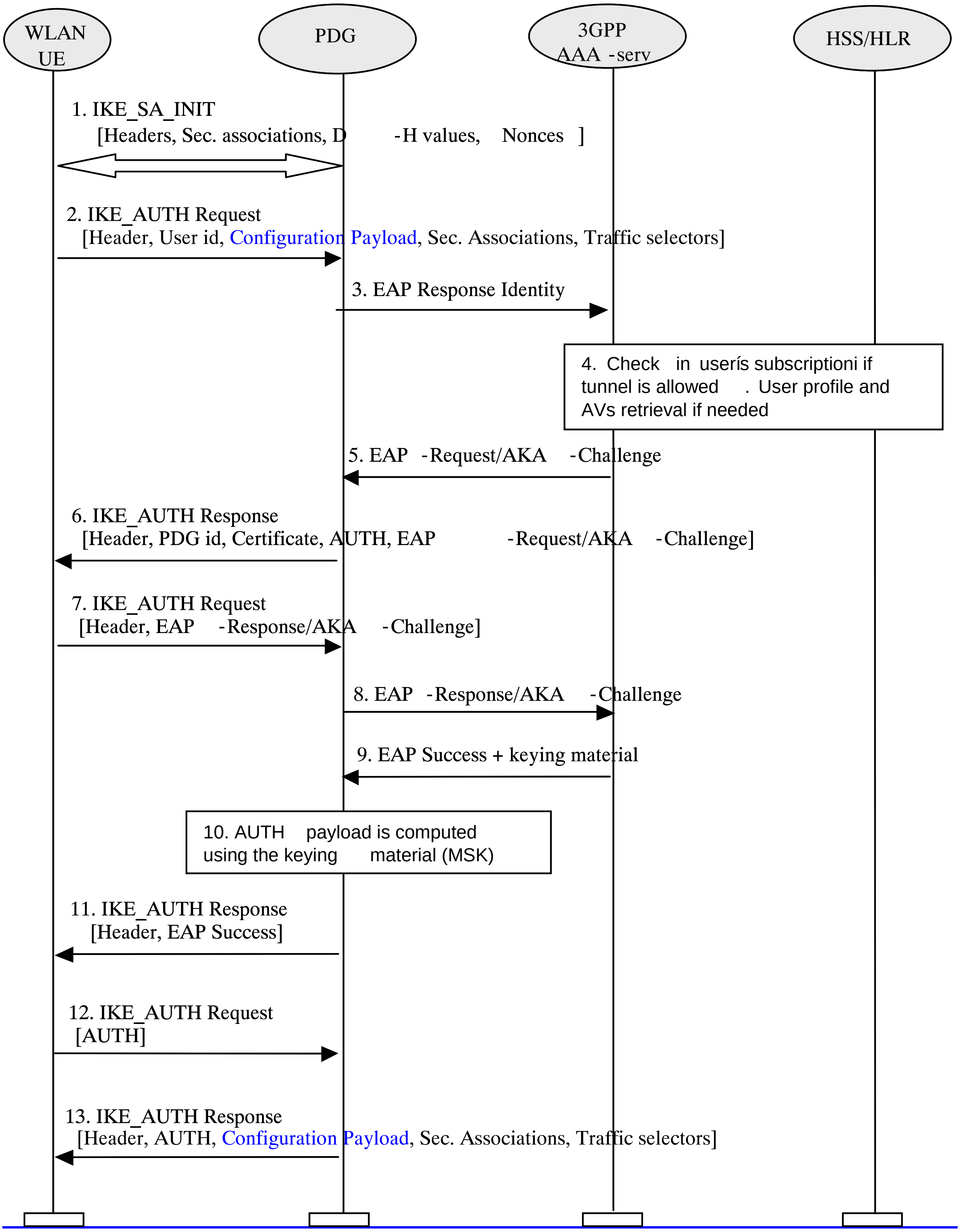

WLAN UE
PDG
3GPP AAA -serv
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec. associations, D -H values, Nonces]
2. IKE_AUTH Request
[Header, User id, Configuration Payload, Sec. Associations, Traffic selectors]
3. EAP Response Identity
4. Check in userís subscriptioni if tunnel is allowed . User profile and AVs retrieval if needed
5. EAP -Request/AKA -Challenge
6. IKE_AUTH Response
[Header, PDG id, Certificate, AUTH, EAP -Request/AKA -Challenge]
7. IKE_AUTH Request
[Header, EAP -Response/AKA -Challenge]
8. EAP -Response/AKA -Challenge
9. EAP Success + keying material
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response
[Header, EAP Success]
12. IKE_AUTH Request
[AUTH]
13. IKE_AUTH Response
[Header, AUTH, Configuration Payload, Sec. Associations, Traffic selectors]

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

Editors note: The control of simultaneous sessions in the EAP authentication has to be possible as in WLAN access authentication. Nevertheless, it is needed to study in detail how the parameters to perform this control have to be transferred in EAP/IKEv2. For example, the VPLMN id could be included in the NAI (see TS 23.234 [13], section 5.3.4)

Editors' note: W-APN should be sent in this step, because in TS 23.234 [13], there is following sentence; "The WLAN-UE shall include the W-APN and the user identity in the initial tunnel establishment request." One possibility is to include the W-APN in the IDr parameter in the IKE_AUTH phase, but this has to be studied in detail.

3. The PDG sends the EAP Response identity message to the 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 ref. [37]. This will help the AAA server to distinguish between authentications for WLAN access and authentications for tunnel setup.

4. The AAA server shall fetch the user profile and authentication vectors from HSS/HLR (if these parameters are not available in the 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. The AAA server checks in userís subscription if he/she is authorized to establish the tunnel.

   In this sequence diagram, it is assumed that the user has a USIM and EAP-AKA will be used. For EAP SIM there is no difference from the IKEv2-EAP relationship point of view, but only for the EAP SIM mechanism itself, which is explained in this technical specification

5. The 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 AAA server (EAP-Request/AKA-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 to the AAA server.

9. When all checks are successful, the AAA server sends 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-AAA server) is implemented using Diameter, the MSK shall be encapsulated in the EAP-Master-Session-Key parameter, as defined in ref. [23].

Editor's note: Registration procedure, including transport of parameters needed to perform simultaneous access control, should be performed in order to update registration status in HSS and fetch the necessary data to the AAA server, but this still needs to be studied in detail.

10. 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.

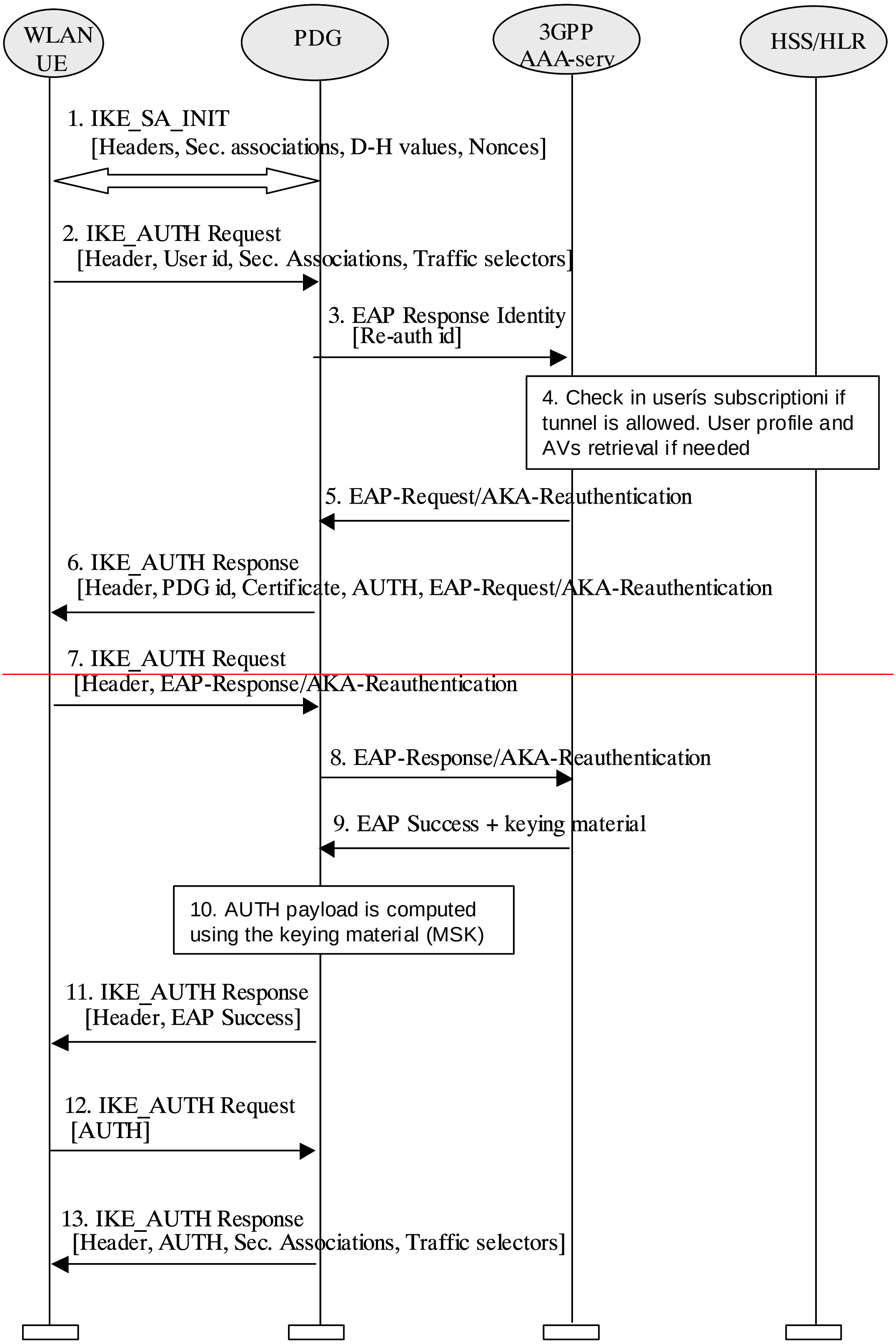
12. The WLAN-UE shall take its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the PDG.

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

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.


WLAN UE
PDG
3GPP AAA-serv
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request
[Header, User id, Sec. Associations, Traffic selectors]
3. EAP Response Identity
[Re-auth id]
4. Check in userís subscriptioni if tunnel is allowed. User profile and AVs retrieval if needed
5. EAP-Request/AKA-Reauthentication
6. IKE_AUTH Response
[Header, PDG id, Certificate, AUTH, EAP-Request/AKA-Reauthentication
7. IKE_AUTH Request
[Header, EAP-Response/AKA-Reauthentication
8. EAP-Response/AKA-Reauthentication
9. EAP Success + keying material
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response
[Header, EAP Success]
12. IKE_AUTH Request
[AUTH]
13. IKE_AUTH Response
[Header, AUTH, Sec. Associations, Traffic selectors]

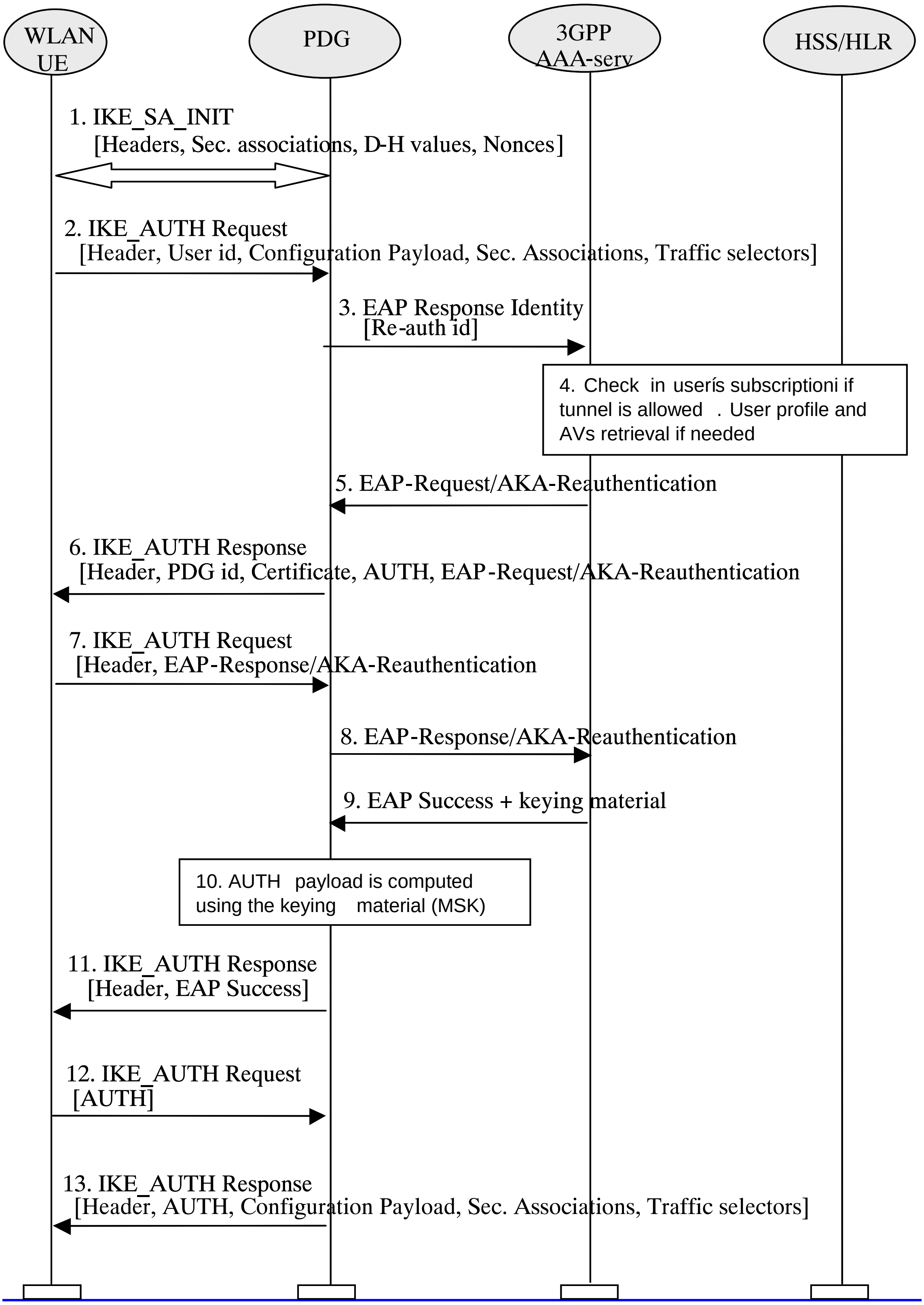

WLAN UE
PDG
3GPP AAA-serv
HSS/HLR
1. IKE_SA_INIT [Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request [Header, User id, Configuration Payload, Sec. Associations, Traffic selectors]
3. EAP Response Identity [Re-auth id]
4. Check in userís subscriptioni if tunnel is allowed . User profile and AVs retrieval if needed
5. EAP-Request/AKA-Reauthentication
6. IKE_AUTH Response [Header, PDG id, Certificate, AUTH, EAP-Request/AKA-Reauthentication
7. IKE_AUTH Request [Header, EAP-Response/AKA-Reauthentication
8. EAP-Response/AKA-Reauthentication
9. EAP Success + keying material
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response [Header, EAP Success]
12. IKE_AUTH Request [AUTH]
13. IKE_AUTH Response [Header, AUTH, Configuration Payload, Sec. Associations, Traffic selectors]

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 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. 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 EAP Response identity message 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 shall fetch the user profile and authentication vectors from HSS/HLR (if these parameters are not available in the AAA server) and determines the EAP method (SIM or AKA) to be used, according to the user subscription. The AAA server checks in userís subscription if he/she is authorized to establish the tunnel.

   In this sequence diagram, it is assumed that the user has a USIM and EAP-AKA will be used. For EAP SIM there is no difference from the IKEv2-EAP relationship point of view, but only for the EAP SIM mechanism itself, which is explained in this technical specification.

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

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 AAA server (EAP-Request/AKA-Reauthentication is included in order to start the EAP procedure over IKEv2.

7. 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.

8. The PDG forwards the EAP-Response/AKA-Reauthentication message to the AAA server.

9. When all checks are successful, the AAA server sends 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].

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

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Security ó S3#35 **Tdoc ⌘*S3-040861***
October 5 ñ 8, 2004, St Paulís Bay, Malta

CR-Form-v7

CHANGE REQUEST

⌘	**33.234**	**CR**	**033**	⌘	**rev**	**1**	⌘	Current version:	**6.2.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘ Tunnel Establishment Procedure		
Source:	⌘ SA WG3		
Work item code:	⌘ WLAN	***Date:***	⌘ 23/06/2004
Category:	⌘ **F**	***Release:***	⌘ Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change: ⌘ According to the current specification, PDG shall generate the EAP-RESPONSE Identity which will add an additional requirement for PDG and also to align with the IKEv2 draft and IEEE standards (802.1x and 802.11i), the procedure for tunnel establishment need to be modified.

Summary of change: ⌘ It is nessary to modify the procedure of tunnel establishment to align with the current specification and with IETF and IEEE standards.

Consequences if not approved: ⌘ TS 33.234 is not aligned with current IETF specifications and the IEEE standards.

Clauses affected: ⌘ 6.1.5.1 and 6.1.5.2

		Y	N		
Other specs Affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments: ⌘

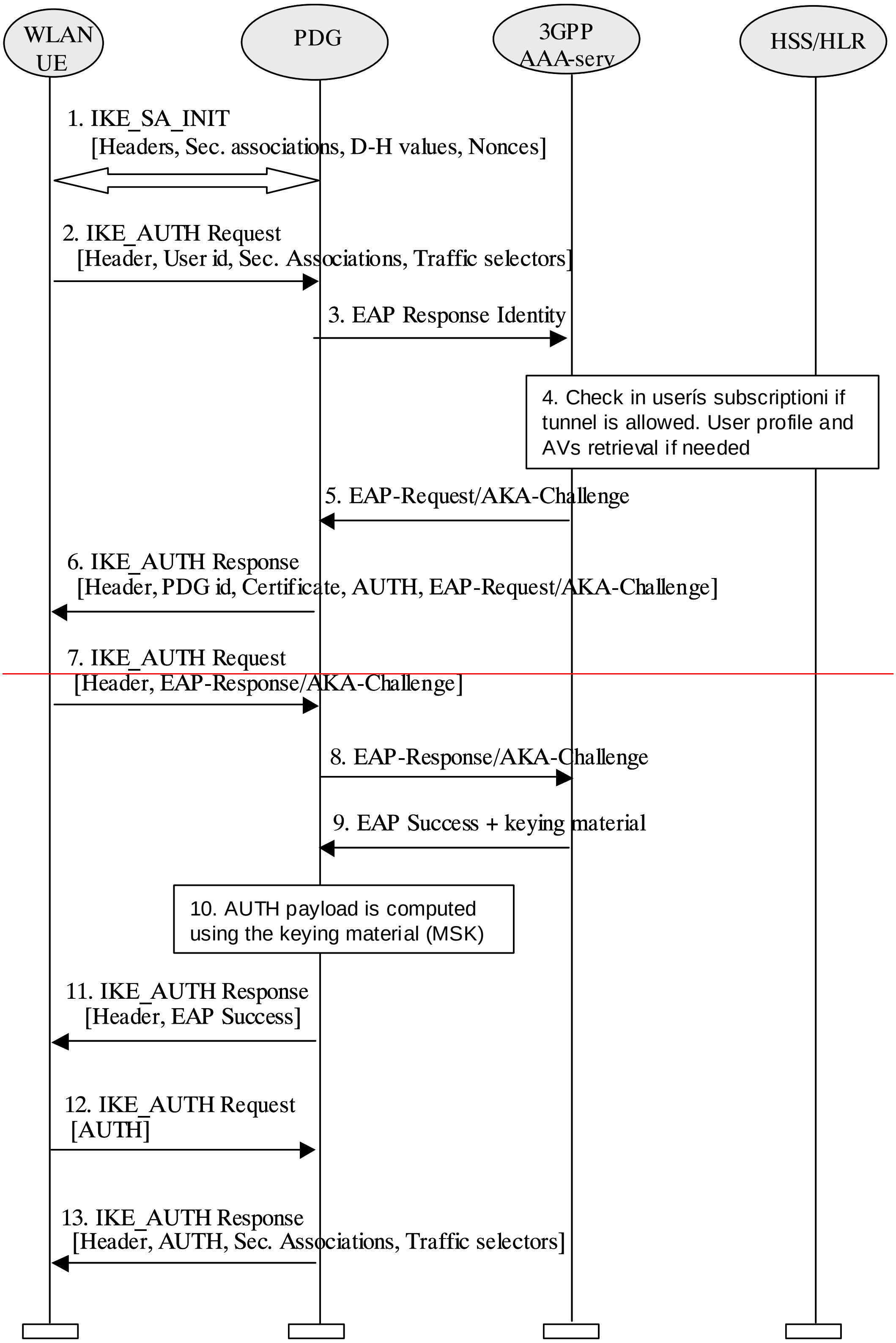
*** BEGIN SET OF CHANGES ***

6.1.5.1 Tunnel full authentication and authorization

The tunnel end point in the network is the PDG. 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 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 AAA server over Diameter (the opposite for messages sent from the AAA server).

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 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 AAA server is certain that no intermediate node has modified or changed the user identity.


WLAN UE
PDG
3GPP AAA-serv
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request
[Header, User id, Sec. Associations, Traffic selectors]
3. EAP Response Identity
4. Check in userís subscriptioni if tunnel is allowed. User profile and AVs retrieval if needed
5. EAP-Request/AKA-Challenge
6. IKE_AUTH Response
[Header, PDG id, Certificate, AUTH, EAP-Request/AKA-Challenge]
7. IKE_AUTH Request
[Header, EAP-Response/AKA-Challenge]
8. EAP-Response/AKA-Challenge
9. EAP Success + keying material
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response
[Header, EAP Success]
12. IKE_AUTH Request
[AUTH]
13. IKE_AUTH Response
[Header, AUTH, Sec. Associations, Traffic selectors]

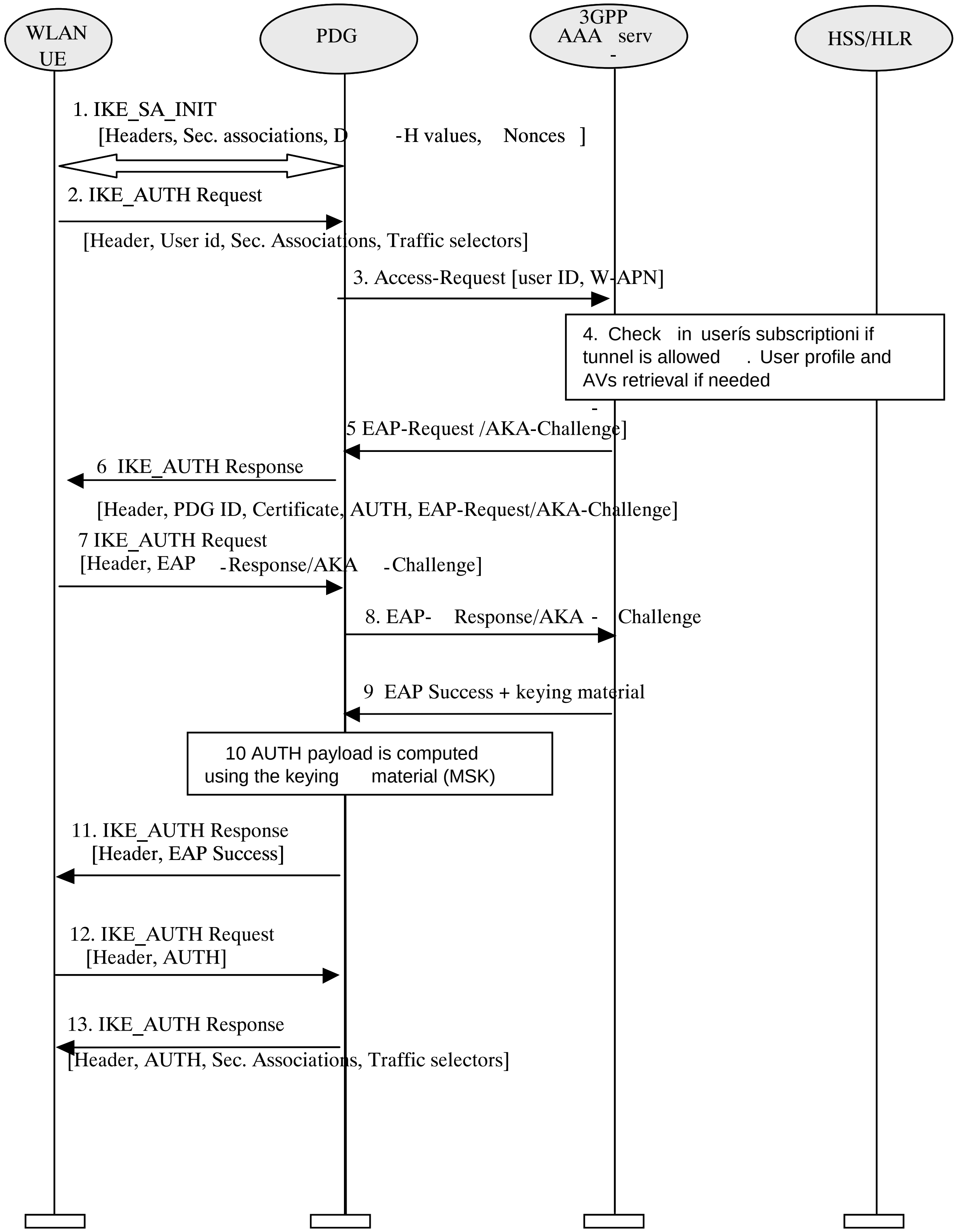

WLAN UE
PDG
3GPP AAA serv -
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec. associations, D -H values, Nonces]
2. IKE_AUTH Request
[Header, User id, Sec. Associations, Traffic selectors]
3. Access-Request [user ID, W-APN]
4. Check in userís subscriptioni if tunnel is allowed . User profile and AVs retrieval if needed
5 EAP-Request /AKA-Challenge]
6 IKE_AUTH Response
[Header, PDG ID, Certificate, AUTH, EAP-Request/AKA-Challenge]
7 IKE_AUTH Request
[Header, EAP -Response/AKA -Challenge]
8. EAP- Response/AKA - Challenge
9 EAP Success + keying material
10 AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response
[Header, EAP Success]
12. IKE_AUTH Request
[Header, AUTH]
13. IKE_AUTH Response
[Header, AUTH, Sec. Associations, Traffic selectors]

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 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).

Editors note: The control of simultaneous sessions in the EAP authentication has to be possible as in WLAN access authentication. Nevertheless, it is needed to study in detail how the parameters to perform this control have to be transferred in EAP/IKEv2. For example, the VPLMN id could be included in the NAI (see TS 23.234 [13], section 5.3.4)

Editors' note: W-APN should be sent in this step, because in TS 23.234 [13], there is following sentence; "The WLAN-UE shall include the W-APN and the user identity in the initial tunnel establishment request." One possibility is to include the W-APN in the IDr parameter in the IKE_AUTH phase, but this has to be studied in detail.

3. The PDG sends the Access Request ~~EAP Response identity~~ message with an empty EAP AVP to the AAA server, containing the user identity and W-APN. 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 shall fetch the user profile and authentication vectors from HSS/HLR (if these parameters are not available in the 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. The AAA server checks in userís subscription if he/she is authorized to establish the tunnel.

   In this sequence diagram, it is assumed that the user has a USIM and EAP-AKA will be used. For EAP SIM there is no difference from the IKEv2-EAP relationship point of view, but only for the EAP SIM mechanism itself, which is explained in this technical specification

5. The 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 AAA server (EAP-Request/AKA-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 to the AAA server.

9. When all checks are successful, the AAA server sends 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-AAA server) is implemented using Diameter, the MSK shall be encapsulated in the EAP-Master-Session-Key parameter, as defined in ref. [23].

Editor's note: Registration procedure, including transport of parameters needed to perform simultaneous access control, should be performed in order to update registration status in HSS and fetch the necessary data to the AAA server, but this still needs to be studied in detail.

10. 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.

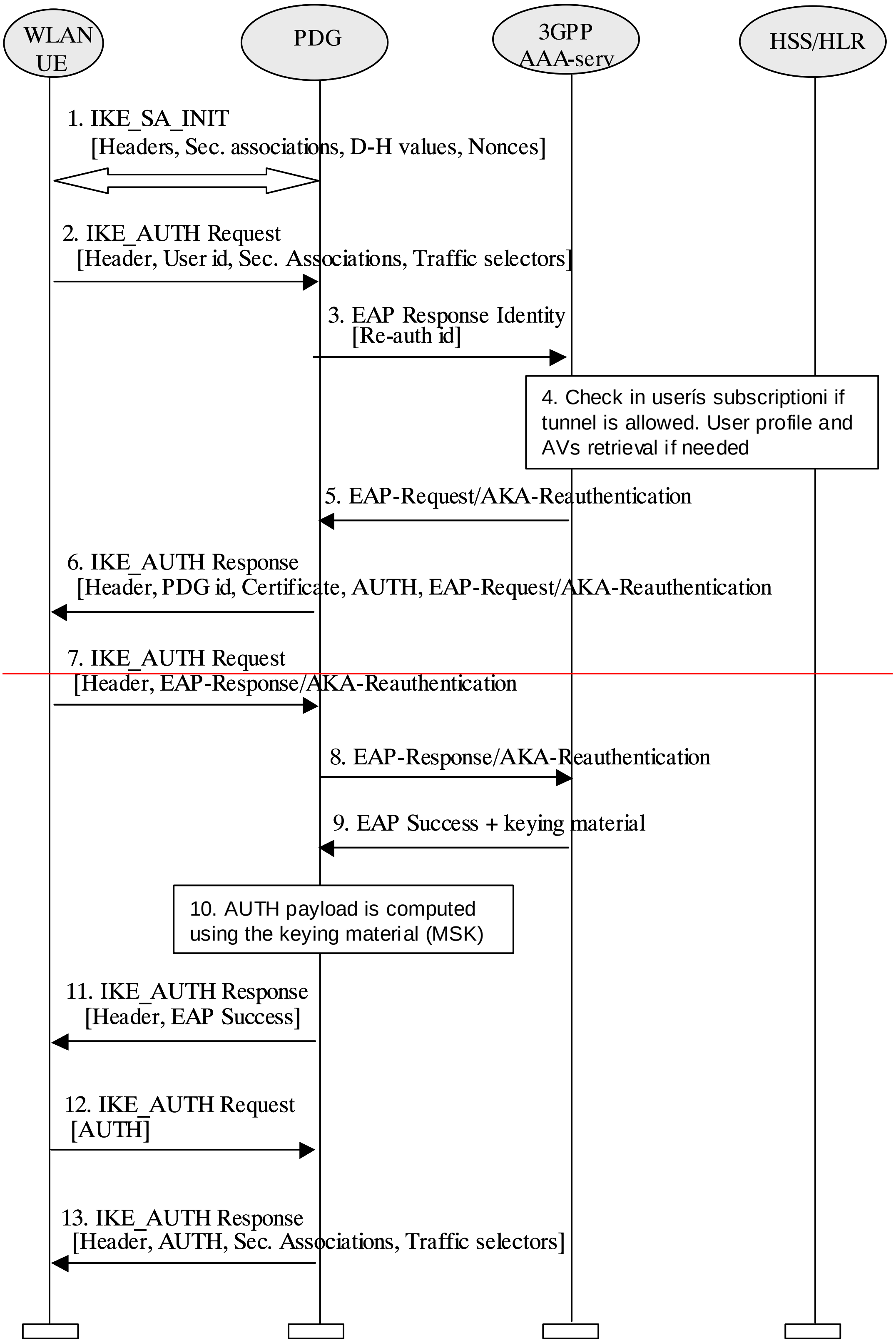
12. The WLAN-UE shall take its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the PDG.

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. This AUTH parameter is sent to the WLAN-UE together with the security associations and rest of IKEv2 parameters and the IKEv2 negotiation terminates.

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.


WLAN UE
PDG
3GPP AAA-serv
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request
[Header, User id, Sec. Associations, Traffic selectors]
3. EAP Response Identity
[Re-auth id]
4. Check in userís subscriptioni if tunnel is allowed. User profile and AVs retrieval if needed
5. EAP-Request/AKA-Reauthentication
6. IKE_AUTH Response
[Header, PDG id, Certificate, AUTH, EAP-Request/AKA-Reauthentication
7. IKE_AUTH Request
[Header, EAP-Response/AKA-Reauthentication
8. EAP-Response/AKA-Reauthentication
9. EAP Success + keying material
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response
[Header, EAP Success]
12. IKE_AUTH Request
[AUTH]
13. IKE_AUTH Response
[Header, AUTH, Sec. Associations, Traffic selectors]

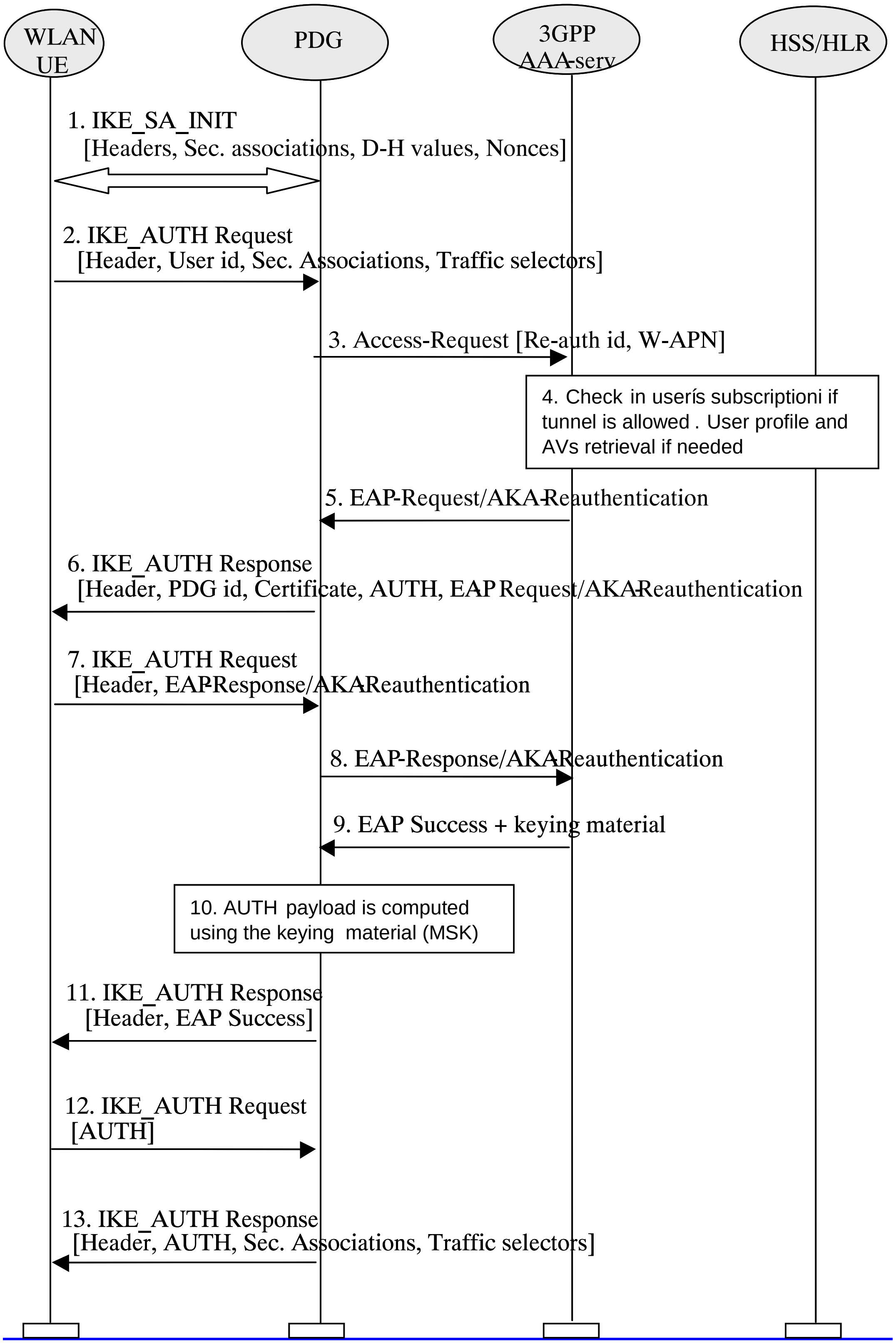

WLAN UE
PDG
3GPP AAA-serv
HSS/HLR
1. IKE_SA_INIT [Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request [Header, User id, Sec. Associations, Traffic selectors]
3. Access-Request [Re-auth id, W-APN]
4. Check in userís subscriptioni if tunnel is allowed . User profile and AVs retrieval if needed
5. EAP-Request/AKA-Reauthentication
6. IKE_AUTH Response [Header, PDG id, Certificate, AUTH, EAP Request/AKA-Reauthentication
7. IKE_AUTH Request [Header, EAP-Response/AKA-Reauthentication
8. EAP-Response/AKA-Reauthentication
9. EAP Success + keying material
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response [Header, EAP Success]
12. IKE_AUTH Request [AUTH]
13. IKE_AUTH Response [Header, AUTH, Sec. Associations, Traffic selectors]

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 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.

3. The PDG sends the Access Request ~~EAP Response identity~~ message with an empty EAP AVP to the AAA server, containing the re-authentication identity and W-APN. 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 shall fetch the user profile and authentication vectors from HSS/HLR (if these parameters are not available in the AAA server) and determines the EAP method (SIM or AKA) to be used, according to the user subscription. The AAA server checks in userís subscription if he/she is authorized to establish the tunnel.

   In this sequence diagram, it is assumed that the user has a USIM and EAP-AKA will be used. For EAP SIM there is no difference from the IKEv2-EAP relationship point of view, but only for the EAP SIM mechanism itself, which is explained in this technical specification.

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

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 AAA server (EAP-Request/AKA-Reauthentication is included in order to start the EAP procedure over IKEv2.

7. 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.

8. The PDG forwards the EAP-Response/AKA-Reauthentication message to the AAA server.

9. When all checks are successful, the AAA server sends 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].

10. 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. This AUTH parameter is sent to the WLAN-UE together with the security associations and rest of IKEv2 parameters and the IKEv2 negotiation terminates.

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Security ó SA3#35 **S3-040771**

October 5-8, 2004, St Paul's Bay, Malta

CR-Form-v7

CHANGE REQUEST

⌘	**33.234**	**CR**	**036**	⌘ **rev**	**-**	⌘	Current version:	**6.2.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Deletion of inconclusive text on A5/2 countermeasures		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	28/09/2004
Category:	⌘	**F**	***Release:*** ⌘	Rel-6
		Use one of the following categories: ***F** (correction)* ***A** (corresponds to a correction in an earlier release)* ***B** (addition of feature),* ***C** (functional modification of feature)* ***D** (editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.		*Use one of the following releases:* *2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)*

Reason for change:	⌘	There is text in Annex C.3.5 which mentions ongoing discussions, without coming to conclusions. Such text is inappropriate in a complete specification.
Summary of change:	⌘	Deletion of inappropriate text.
Consequences if not approved:	⌘	Inappropriate text in specification.

Clauses affected:	⌘	C.3.5			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘	-			

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.

~~It should also be noted that in order to alleviate the security problem with the A5/2 attack new terminals are required cf. the discussion on the Special RAND or that a USIM is used instead of a SIM. The exact terminal and network requirements on how to alleviate the A5/2 issues are currently studied in 3GPP and it is proposed that those requirements shall also apply to WLAN and 3G interworking for consistency reasons. So, for example, if the special RAND mechanism is adopted then special RANDs should be sent to WLAN AAA servers to prohibit the use of all A5 and GEA algorithms. When the GSM device implements the special RAND mechanism, this will protect against a man-in-the-middle exploiting a weakness in any GSM algorithm in order to masquerade as a WLAN client or eavesdrop the WLAN communications.~~

3GPP TSG SA WG3 Security ó SA3#35 **S3-040842**

October 5-8, 2004, St Paul's Bay, Malta

CR-Form-v7

CHANGE REQUEST

⌘	**33.234**	**CR**	**037**	⌘	**rev**	**1**	⌘	Current version:	**6.2.1**	⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Alignment of IPsec profile with RFC2406		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	28/09/2004
Category:	⌘	**F**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The current profile of IPSec ESP in section 6.6 of TS 33.234 contradicts the specification of IPSec ESP in RFC2406. RC2406 states in section 3.2: ìNote that although both confidentiality and authentication are optional, at least one of these services MUST be selected hence both algorithms MUST NOT be simultaneously NULL.î. An editors' note is removed.
Summary of change:	⌘	(Message) authentication must not be switched off. Update of reference to IKEv2. Removal of editors' note.
Consequences if not approved:	⌘	Non-conformance with RFC2406.

Clauses affected:	⌘	2.2, 6.6				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘	-				

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] draft-arkko-pppext-eap-aka-12, April 2004: "Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA)". IETF Work in progress

[5] draft-haverinen-pppext-eap-sim-13, April 2004: "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)". IETF Work in progress

[6] IEEE Std 802.11i/D7.0, October 2003: "Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security".

[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] draft-ietf-ipsec-ikev2-1~~4~~6.txt, ~~May~~ September 2004: "Internet Key Exchange (IKEv2) Protocol".

[30] RFC 2406, November 1998: "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-mariblanca-aaa-eap-lla-01.txt, June 2004: "EAP lower layer attributes for AAA protocols".

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 ~~security~~ confidentiality protection ~~(confidentiality and/or integrity)~~ in the tunnel ~~(for example high trust between the 3GPP network operator and the WLAN access provider)~~. This means that the transform IDs for encryption ENCR_NULL ~~and NONE for integrity~~ shall be allowed to negotiate, as specified in ref. [29]. Integrity protection shall always be used, i.e. the authentication algorithm [30] shall not be NULL.

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

~~Editor's note: An example of a profile of IPSec ESP, which may be useful to study when writing this section, can be found in TS 33.210, section 5.3. Future editions of this specification will define additional profiles.~~

3GPP TSG SA WG3 Security ó S3#36
Shenzhen, China 23 - 26 November 2004

Tdoc ⌘S3-041153

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**040**	⌘**rev**	**2**	⌘	Current version:	**6.2.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects:	UICC apps⌘ ☐	ME ☒	Radio Access Network ☐	Core Network ☒

Title:	⌘	Control of simultaneous sessions in WLAN 3GPP IP access		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	20/10/2004
Category:	⌘	**C**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	A mechanism to control simultaneous sessions in WLAN 3GPP IP access (formerly called scenario 3) is needed in order to prevent fraud situations, for example where the user gives access to its (U)SIM from several devices that authenticate on behalf of the user and get access to the 3GPP network.
Summary of change:	⌘	This paper reflects the changes needed in the TS 33.234 to introduce the mechanism. It basically consists of having a flag for every W-APN in the 3GPP AAA server to indicate if it is already active or not, i.e. if an IKE security association has already been set up or not. If a certain W-APN is active and a new W-APN setup request is received in the AAA server, the request is rejected.
Consequences if not approved:	⌘	Potential fraud situations may happen, where a user gives access to this (U)SIM to several devices.

Clauses affected:	⌘	3.1, 5.7 (new), 6.1.5.1, 6.1.5.2				
		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	23.234, 24.234
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

*** BEGIN SET OF CHANGES ***

3.1 Definitions

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

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**.**

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.

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

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

5.7 Simultaneous access control

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 allow only one IKEv2 security associations per W-APN. With this mechanism, it is avoided that two or more devices 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). The AAA server shall keep a flag (e.g. active yes/no) for every W-APN and check this flag when a IKE SA establishment attempt is received. If the W-APN is already active, the AAA server will instruct the PDG to delete the old IKE SA and proceed to establish the new IKE SA.

*** END SET OF CHANGES ***

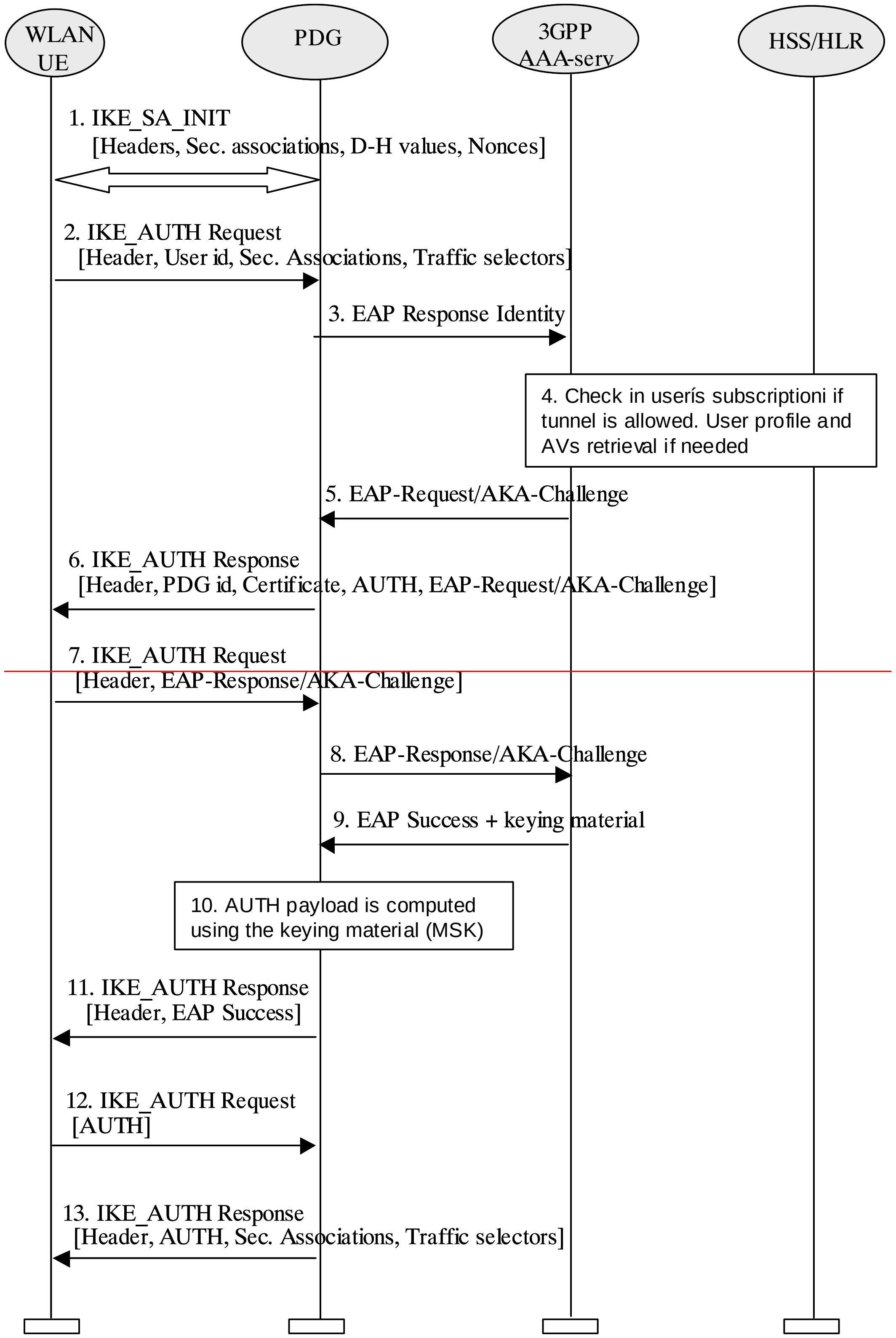
*** BEGIN SET OF CHANGES ***

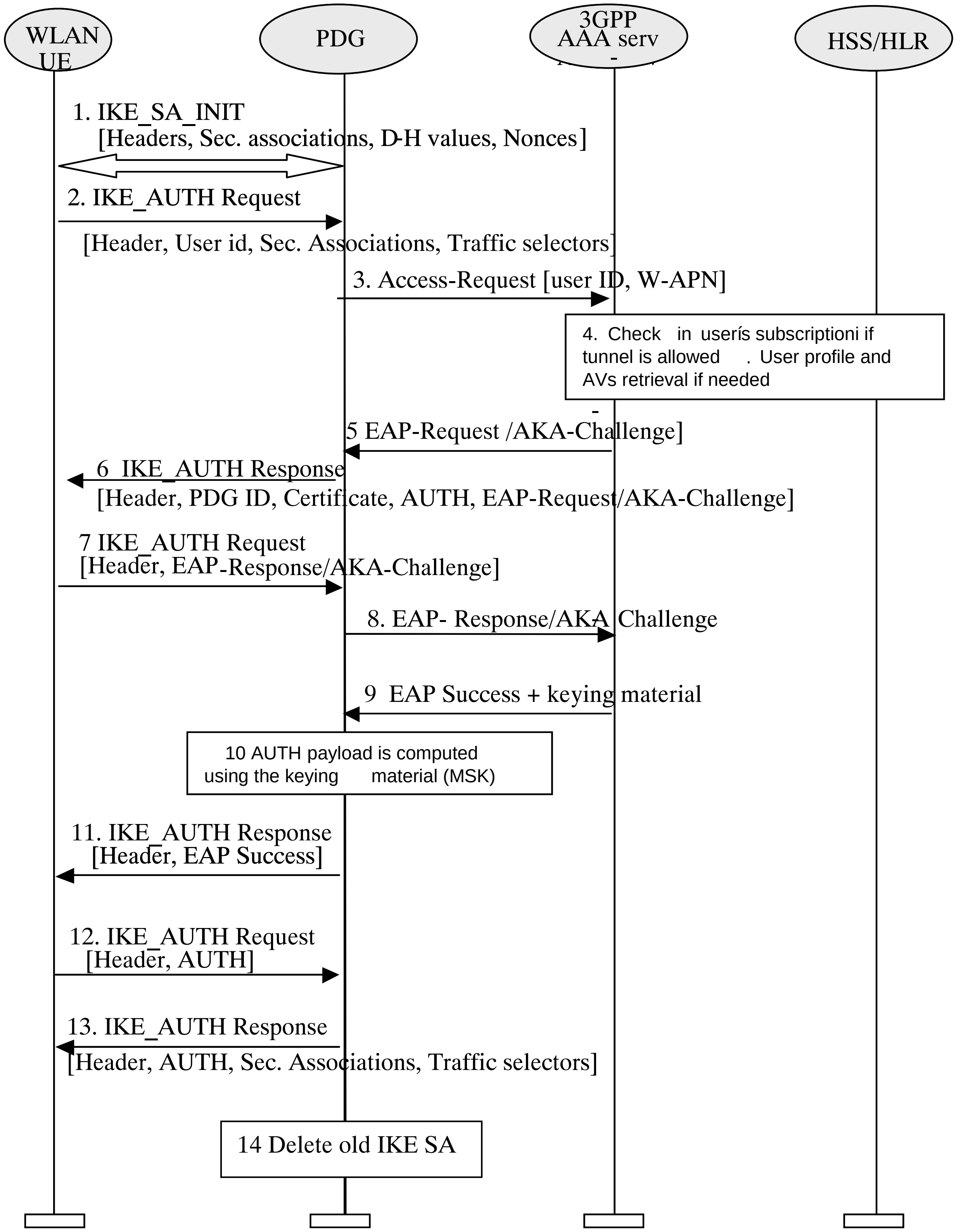
6.1.5.1 Tunnel full authentication and authorization

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 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 AAA server over Diameter (the opposite for messages sent from the AAA server).

The sequence diagram is shown in this chapter. 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 AAA server to request the user identity again using the EAP AKA or EAP SIM specific methods (as specified in ref. [4] and [5]), because the AAA server is certain that no intermediate node has modified or changed the user identity.


WLAN UE
PDG
3GPP AAA-serv
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request
[Header, User id, Sec. Associations, Traffic selectors]
3. EAP Response Identity
4. Check in userís subscriptioni if tunnel is allowed. User profile and AVs retrieval if needed
5. EAP-Request/AKA-Challenge
6. IKE_AUTH Response
[Header, PDG id, Certificate, AUTH, EAP-Request/AKA-Challenge]
7. IKE_AUTH Request
[Header, EAP-Response/AKA-Challenge]
8. EAP-Response/AKA-Challenge
9. EAP Success + keying material
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response
[Header, EAP Success]
12. IKE_AUTH Request
[AUTH]
13. IKE_AUTH Response
[Header, AUTH, Sec. Associations, Traffic selectors]


WLAN UE
PDG
3GPP AAA serv -
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request
[Header, User id, Sec. Associations, Traffic selectors]
3. Access-Request [user ID, W-APN]
4. Check in userís subscriptioni if tunnel is allowed . User profile and AVs retrieval if needed
5 EAP-Request /AKA-Challenge]
6 IKE_AUTH Response
[Header, PDG ID, Certificate, AUTH, EAP-Request/AKA-Challenge]
7 IKE_AUTH Request
[Header, EAP-Response/AKA-Challenge]
8. EAP- Response/AKA Challenge
9 EAP Success + keying material
10 AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response
[Header, EAP Success]
12. IKE_AUTH Request
[Header, AUTH]
13. IKE_AUTH Response
[Header, AUTH, Sec. Associations, Traffic selectors]
14 Delete old IKE SA

Sequence of events:

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 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 ref [14], containing the IMSI or the pseudonym. The identity in NAI format generated from the IMSI is described in ref. [4] and [5], depending on the type of EAP method to be used (EAP SIM or EAP AKA).

~~Editors note: The control of simultaneous sessions in the EAP authentication has to be possible as in WLAN access authentication. Nevertheless, it is needed to study in detail how the parameters to perform this control have to be transferred in EAP/IKEv2. For example, the VPLMN id could be included in the NAI (see TS 23.234 [13], section 5.3.4)~~

Editors' note: W-APN should be sent in this step, because in TS 23.234 [13], there is following sentence; "The WLAN-UE shall include the W-APN and the user identity in the initial tunnel establishment request." One possibility is to include the W-APN in the IDr parameter in the IKE_AUTH phase, but this has to be studied in detail.

3. The PDG sends the Access Request ~~EAP Response identity~~ ~~message~~ with an empty EAP AVP to the AAA server, containing the user identity and W-APN. The PDG shall include a parameter indicating that the authentication is being performed for tunnel establishment, as indicated in ref. [32]. This will help the AAA server to distinguish between authentications for WLAN access and authentications for tunnel setup.

4. The AAA server shall fetch the user profile and authentication vectors from HSS/HLR (if these parameters are not available in the 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. The AAA server checks in userís subscription if he/she is authorized to establish the tunnel.

   In this sequence diagram, it is assumed that the user has a USIM and EAP AKA will be used. For EAP SIM there is no difference from the IKEv2-EAP relationship point of view, but only for the EAP SIM mechanism itself, which is explained in this technical specification

5. The 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 AAA server (EAP-Request/AKA-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 to the AAA server

9. When all checks are successful, the AAA server sends 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-AAA server) is implemented using Diameter, the MSK shall be encapsulated in the EAP-Master-Session-Key parameter, as defined in [23]

   If the W-APN is not active, the AAA server will mark it as ìactiveî.

   If the AAA server detects that the W-APN is active in other PDG, it will send an indication to that PDG requesting to delete the IKE SA of the W-APN.

Editors note: Registration procedure, including transport of parameters needed to perform simultaneous access control, should be performed in order to update registration status in HSS and fetch the necessary data to the AAA server, but this still needs to be studied in detail.

10. 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. This AUTH parameter is sent to the WLAN UE together with the security associations and rest of 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 ref. [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.

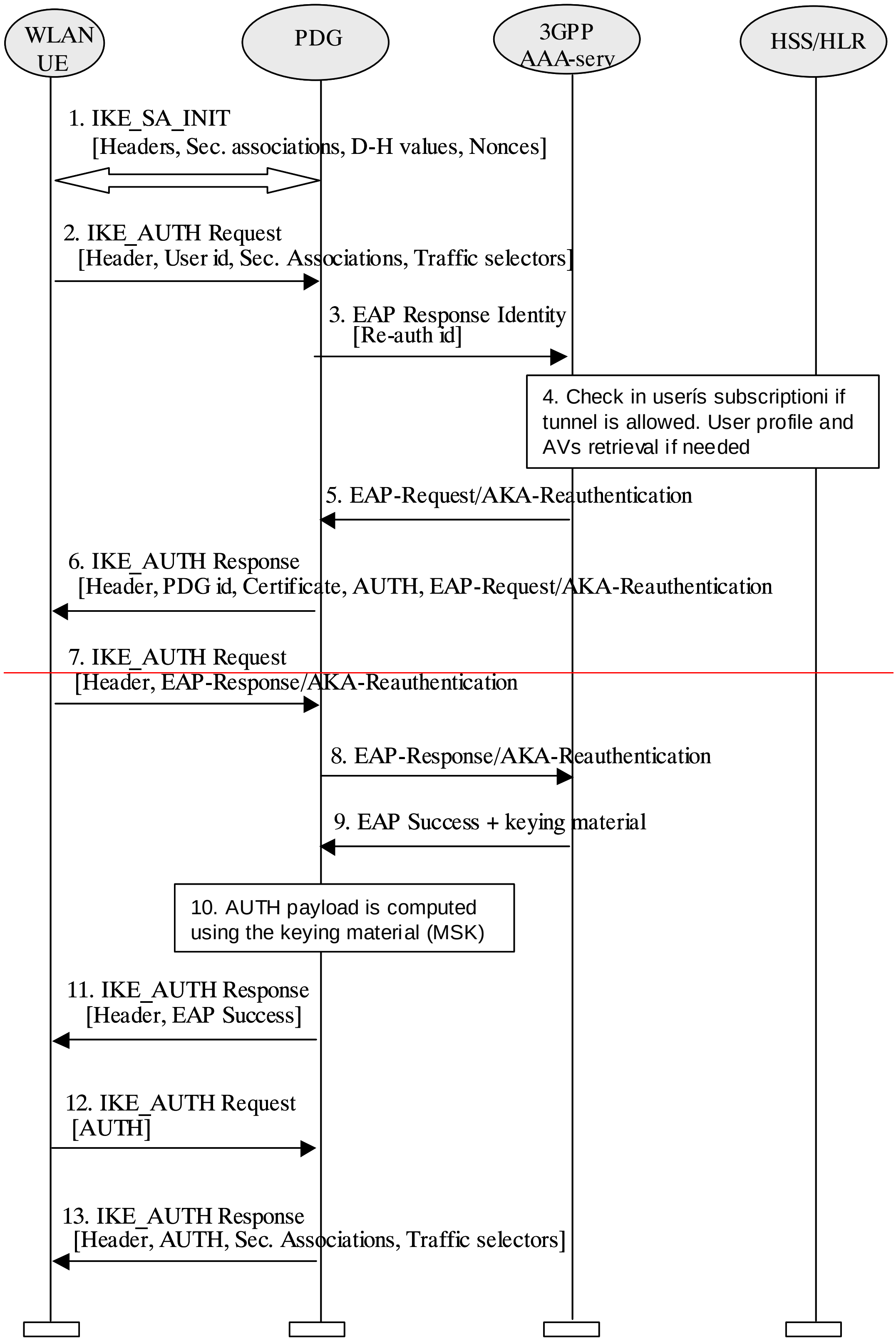
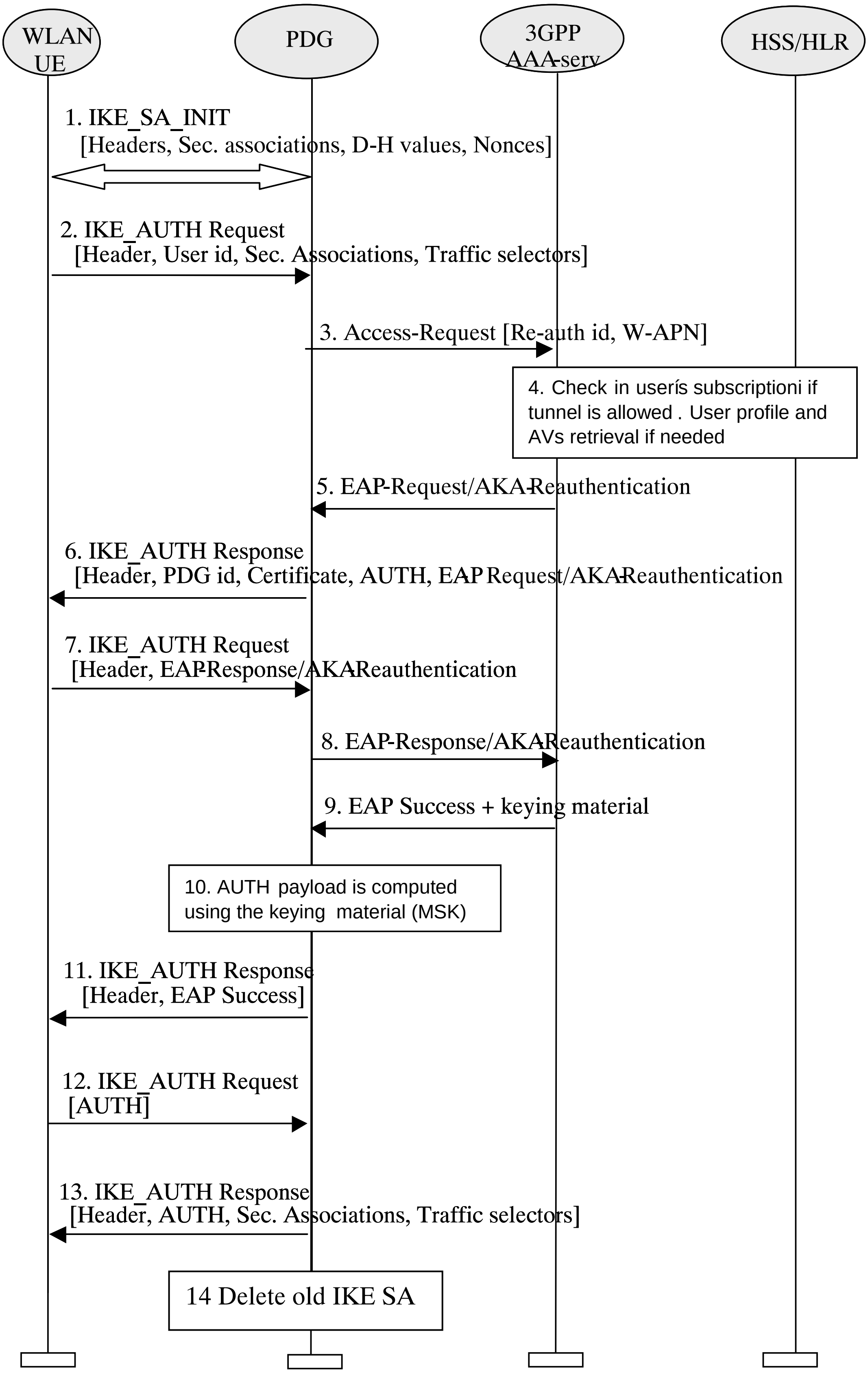

WLAN UE
PDG
3GPP AAA-serv
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request
[Header, User id, Sec. Associations, Traffic selectors]
3. EAP Response Identity
[Re-auth id]
4. Check in userís subscriptioni if tunnel is allowed. User profile and AVs retrieval if needed
5. EAP-Request/AKA-Reauthentication
6. IKE_AUTH Response
[Header, PDG id, Certificate, AUTH, EAP-Request/AKA-Reauthentication
7. IKE_AUTH Request
[Header, EAP-Response/AKA-Reauthentication
8. EAP-Response/AKA-Reauthentication
9. EAP Success + keying material
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response
[Header, EAP Success]
12. IKE_AUTH Request
[AUTH]
13. IKE_AUTH Response
[Header, AUTH, Sec. Associations, Traffic selectors]

Figure 7B: Tunnel fast re-authentication and authorization


WLAN UE
PDG
3GPP AAA-serv
HSS/HLR
1. IKE_SA_INIT
[Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request
[Header, User id, Sec. Associations, Traffic selectors]
3. Access-Request [Re-auth id, W-APN]
4. Check in userís subscriptioni if tunnel is allowed . User profile and AVs retrieval if needed
5. EAP-Request/AKA-Reauthentication
6. IKE_AUTH Response
[Header, PDG id, Certificate, AUTH, EAP Request/AKA-Reauthentication
7. IKE_AUTH Request
[Header, EAP-Response/AKA-Reauthentication
8. EAP-Response/AKA-Reauthentication
9. EAP Success + keying material
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response
[Header, EAP Success]
12. IKE_AUTH Request
[AUTH]
13. IKE_AUTH Response
[Header, AUTH, Sec. Associations, Traffic selectors]
14 Delete old IKE SA

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 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.

3. The PDG sends the Access Request ~~EAP Response identity~~ message with an empty EAP AVP to the AAA server, containing the re-authentication identity and W-APN. 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 shall fetch the user profile and authentication vectors from HSS/HLR (if these parameters are not available in the AAA server) and determines the EAP method (SIM or AKA) to be used, according to the user subscription. The AAA server checks in userís subscription if he/she is authorized to establish the tunnel.

   In this sequence diagram, it is assumed that the user has a USIM and EAP AKA will be used. For EAP SIM there is no difference from the IKEv2-EAP relationship point of view, but only for the EAP SIM mechanism itself, which is explained in this technical specification.

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

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 AAA server (EAP-Request/AKA-Reauthentication is included in order to start the EAP procedure over IKEv2.

7. 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.

8. The PDG forwards the EAP-Response/AKA-Reauthentication message to the AAA server.

9. When all checks are successful, the AAA server sends 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].

   If the W-APN is not active, the AAA server will mark it as ìactiveî.

   If the AAA server detects that the W-APN is active in other PDG, it will send an indication to that PDG requesting to delete the IKE SA of the W-APN.

10. 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. This AUTH parameter is sent to the WLAN UE together with the security associations and rest of 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 to the WLAN UE an INFORMATIONAL exchange with a Delete payload, as specified in ref. [29], in order to delete the old IKE SA in WLAN UE.

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Security ó S3#36 *Tdoc ⌘S3-041109*
Shenzhen, China 23 - 26 November 2004

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**041**	⌘**rev**	**1**	⌘	Current version:	**6.2.1**	⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network □

Title:	⌘	Completion of definition and abbreviations		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	23/11/2004
Category:	⌘	**D**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Some features and new chapters have been in different SA3 meetings to TS 33.234, but the definitions and abbreviations chapters have not been modified accordingly. This CR updates these chapters
Summary of change:	⌘	New abbreviations and definitions are added.
Consequences if not approved:	⌘	Lack of content consistency in TS 33.234

Clauses affected:	⌘	3.1, 3.2			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

*** BEGIN SET OF CHANGES ***

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.

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.

Editors note: This WLAN-UE definition needs to be reflected in related specifications.

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

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Security ó S3#36
Shenzhen, China 23 - 26 November 2004

Tdoc ⌘S3-041110

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**042**	⌘**rev**	**1**	⌘	Current version:	**6.2.1** ⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Fallback from re-authentication to full authentication		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	25/11/2004
Category:	⌘	**F**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Currently in TS 33.234 it is described how to force a re-authentication process from a full authentication (sending a re-authentication identity from the AAA server), but it is not clearly described how to request again a full authentication when re-authentications have been started
Summary of change:	⌘	It is indicated in the TS that, in order to be able to perform a full authentication after a re-authentication, the AAA server has to issue a pseudonym together with a re-authentication id. The AAA server, when it decides to have full authentication, will reject the re-authentication identity and request the pseudonym
Consequences if not approved:	⌘	Fallback from fast re-authentication to full authentication may be performed using the permanent user identity (IMSI), which is not desirable from identity privacy perspective. The fallback process is not currently described properly in the TS and implementations may vary.

Clauses affected:	⌘	2, 6.1.4.2 (new)				
		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	24.234
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

*** BEGIN SET OF CHANGES ***

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] draft-arkko-pppext-eap-aka-~~12~~13, ~~April~~ October 2004: "Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA)". IETF Work in progress

[5] draft-haverinen-pppext-eap-sim-~~13~~14, ~~April~~ October 2004: "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)". IETF Work in progress

[6] IEEE Std 802.11i/D7.0, October 2003: "Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security".

[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] draft-ietf-ipsec-ikev2-14.txt, May 2004: "Internet Key Exchange (IKEv2) Protocol".

[30] RFC 2406, November 1998: "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-mariblanca-aaa-eap-lla-01.txt, June 2004: "EAP lower layer attributes for AAA protocols".

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

6.1.4.2 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 ref. [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 ref. [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 ref, [5].

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Security ó S3#36
Shenzhen, China 23 - 26 November 2004

Tdoc ⌘S3-040947

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**043**	⌘ **rev**	**-**	⌘	Current version:	**6.2.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects:	UICC apps⌘	□	ME	☒	Radio Access Network	□	Core Network ☒

Title:	⌘	Clarification on the use of IMSI in WLAN 3GPP IP access		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	29/10/2004
Category:	⌘	**F**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F (correction)
A (corresponds to a correction in an earlier release)
B (addition of feature),
C (functional modification of feature)
D (editorial modification)
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The identity privacy handling for WLAN 3GPP IP access (formerly called scenario 3) says that the IMSI is valid to be used even if identity privacy support is used by the home network. This may lead to a inconsistent situation where the home network is issuing temporary identities and the WLAN UE using the IMSI to identify the user.
Summary of change:	⌘	It is clarified that the sending of IMSI in WLAN 3GPP IP access is more secure than in WLAN direct IP access (formerly called scenario 2) because of the protection provided in an IKEv2 exchange. However, it is stated that if temporary identities are being issued by the home network, they shall be used by the WLAN UE.
Consequences if not approved:	⌘	The overriding of the temporary identities by the WLAN UE and use of the IMSI instead may lead to the security risks exposed in the NOTE in the affected chapter.

Clauses affected:	⌘	5.1.6				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

*** BEGIN SET OF CHANGES ***

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 so that they can only be used once. 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 scenario 3, 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).

~~An exception is when the full authentication is being performed for tunnel establishment in scenario 3, in which case the IMSI may be sent even if identity privacy support was activated by the home network.~~ 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 ~~this situation~~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 pseudonyms, 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 pseudonym.

If identity privacy is used but the AAA server cannot identify the user by its pseudonym, the AAA server requests the user 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.

Editor's note: The use of PEAP with EAP/AKA and EAP/SIM is currently under consideration. If PEAP is used, the temporary identity privacy scheme provided by EAP/AKA and EAP/SIM is not needed.

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Security ó S3#36
Shenzhen, China 23 - 26 November 2004

Tdoc ⌘S3-041138

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**044**	⌘**rev**	**2**	⌘ Current version:	**6.2.1** ⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Clarification on the use of MAC addresses		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	26/11/2004
Category:	⌘	**C**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Ericsson submitted CR S3-040750 in SA3#35 meeting, together with a discussion paper in which the use of the MAC address of a device to control simultaneous sessions was questioned. This CR introduces the necessary changes in TS 33.234 according to the conclusions of the discussion paper. Basically, the conclusions is that the AAA server can trust in the MAC address only in one situation in scenario 2: when the MAC addresses if in the authentication requests are being received from the same WLAN access network. In scenario 3, the MAC address cannot be trusted and hence it doesnít help to detect simultaneous accesses. It hasnít been identified an alternative mechanism to the use of the MAC address in scenario 2.
Summary of change:	⌘	Clarification of the use of the MAC address in different chapters. A new chapter is created in order to introduce the simultaneous session control issue. A mistake is corrected in the pictures as well.
Consequences if not approved:	⌘	Trusting in the MAC addresses may make the AAA server believe that there are no simultaneous sessions while in reality there are.

Clauses affected:	⌘	5.7 (new), 6.1.1, 6.1.2				
		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	24.234
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

*** BEGIN SET OF CHANGES ***

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 userís 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.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

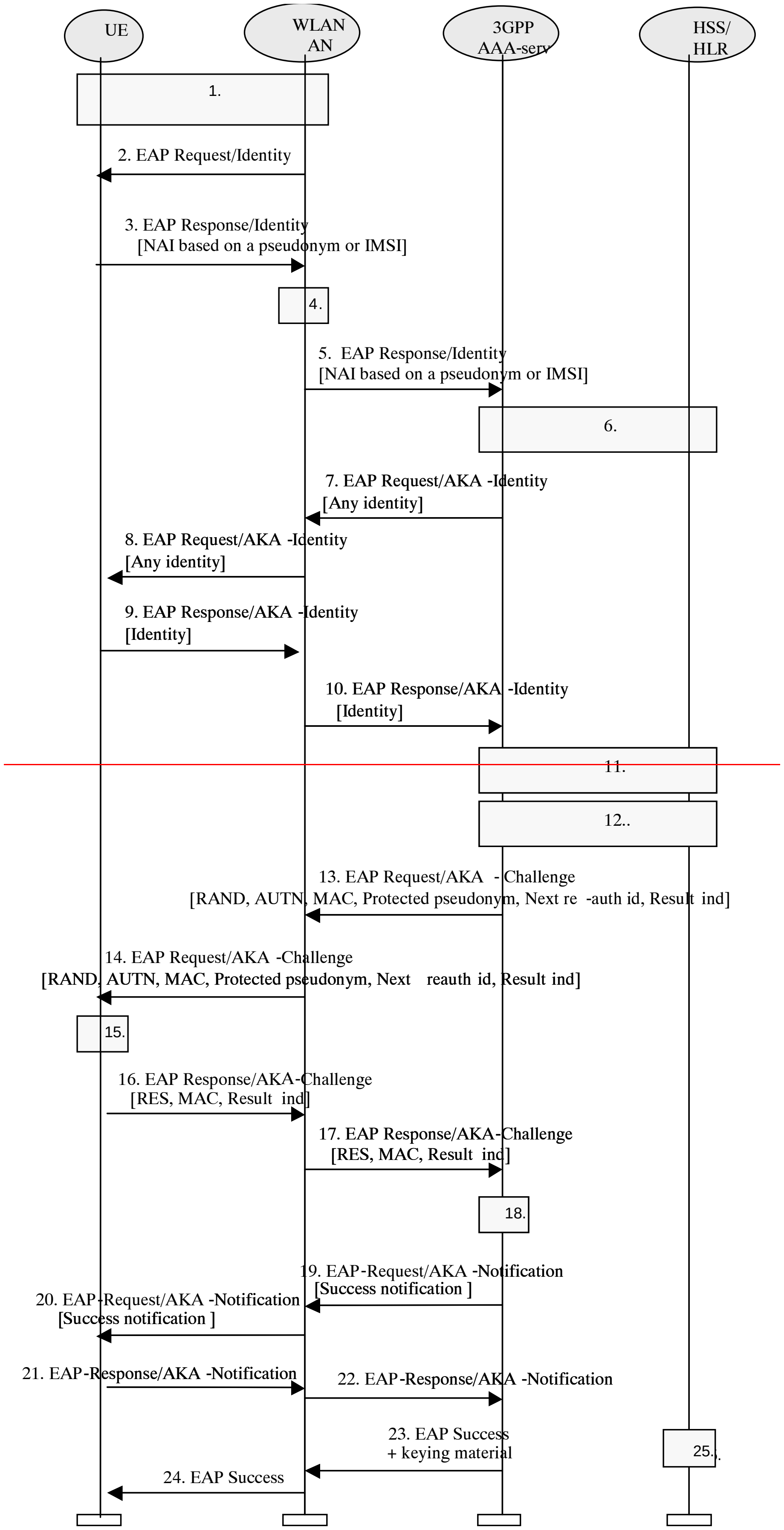
6.1.1 USIM-based WLAN Access Authentication

USIM based authentication is a proven solution that satisfies the authentication requirements from section 4.2. This form of authentication shall be based on EAP-AKA (ref. [4]), as described in section 6.1.1.1.

Editor's note: also see section 4.2.4 on WLAN-UE Functional Split.

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.


UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity [NAI based on a pseudonym or IMSI]
4.
5. EAP Response/Identity [NAI based on a pseudonym or IMSI]
6.
7. EAP Request/AKA -Identity [Any identity]
8. EAP Request/AKA -Identity [Any identity]
9. EAP Response/AKA -Identity [Identity]
10. EAP Response/AKA -Identity [Identity]
11.
12..
13. EAP Request/AKA - Challenge [RAND, AUTN, MAC, Protected pseudonym, Next re -auth id, Result ind]
14. EAP Request/AKA -Challenge [RAND, AUTN, MAC, Protected pseudonym, Next reauth id, Result ind]
15.
16. EAP Response/AKA-Challenge [RES, MAC, Result ind]
17. EAP Response/AKA-Challenge [RES, MAC, Result ind]
18.
19. EAP-Request/AKA -Notification [Success notification]
20. EAP-Request/AKA -Notification [Success notification]
21. EAP-Response/AKA -Notification
22. EAP-Response/AKA -Notification
23. EAP Success + keying material
25..
24. EAP Success

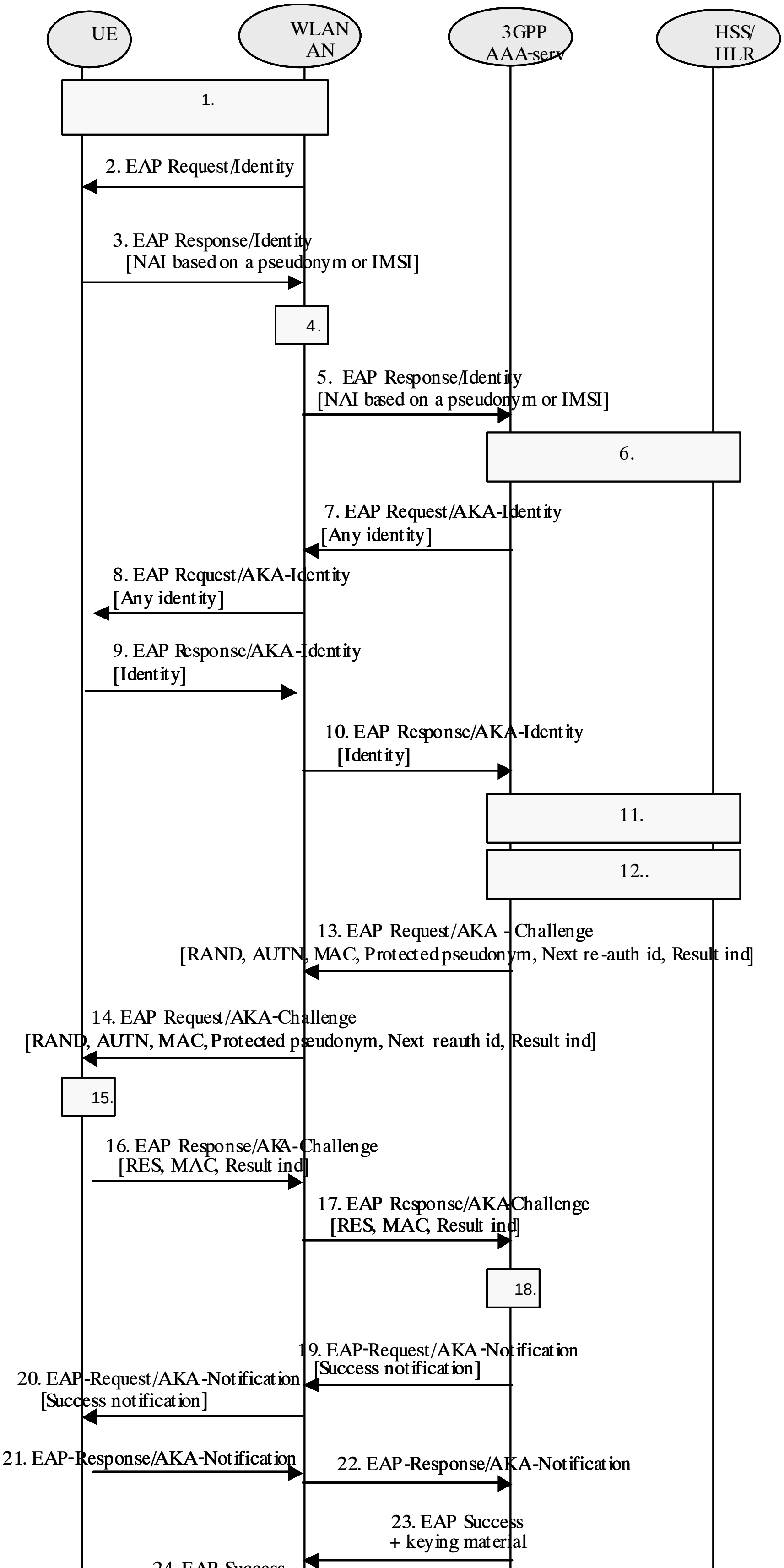

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity [NAI based on a pseudonym or IMSI]
4.
5. EAP Response/Identity [NAI based on a pseudonym or IMSI]
6.
7. EAP Request/AKA-Identity [Any identity]
8. EAP Request/AKA-Identity [Any identity]
9. EAP Response/AKA-Identity [Identity]
10. EAP Response/AKA-Identity [Identity]
11.
12..
13. EAP Request/AKA - Challenge [RAND, AUTN, MAC, Protected pseudonym, Next re-auth id, Result ind]
14. EAP Request/AKA-Challenge [RAND, AUTN, MAC, Protected pseudonym, Next reauth id, Result ind]
15.
16. EAP Response/AKA-Challenge [RES, MAC, Result ind]
17. EAP Response/AKA-Challenge [RES, MAC, Result ind]
18.
19. EAP-Request/AKA-Notification [Success notification]
20. EAP-Request/AKA-Notification [Success notification]
21. EAP-Response/AKA-Notification
22. EAP-Response/AKA-Notification
23. EAP Success + keying material
24. EAP Success
25..

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 RFC 2486. NAI contains either a temporary identifier (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 EAP/AKA [4].

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.

   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 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 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 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 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 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 was received, then the WLAN-UE stores the pseudonym 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 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. The exception in this process is 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. In that case the authentication process continues normally.

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.

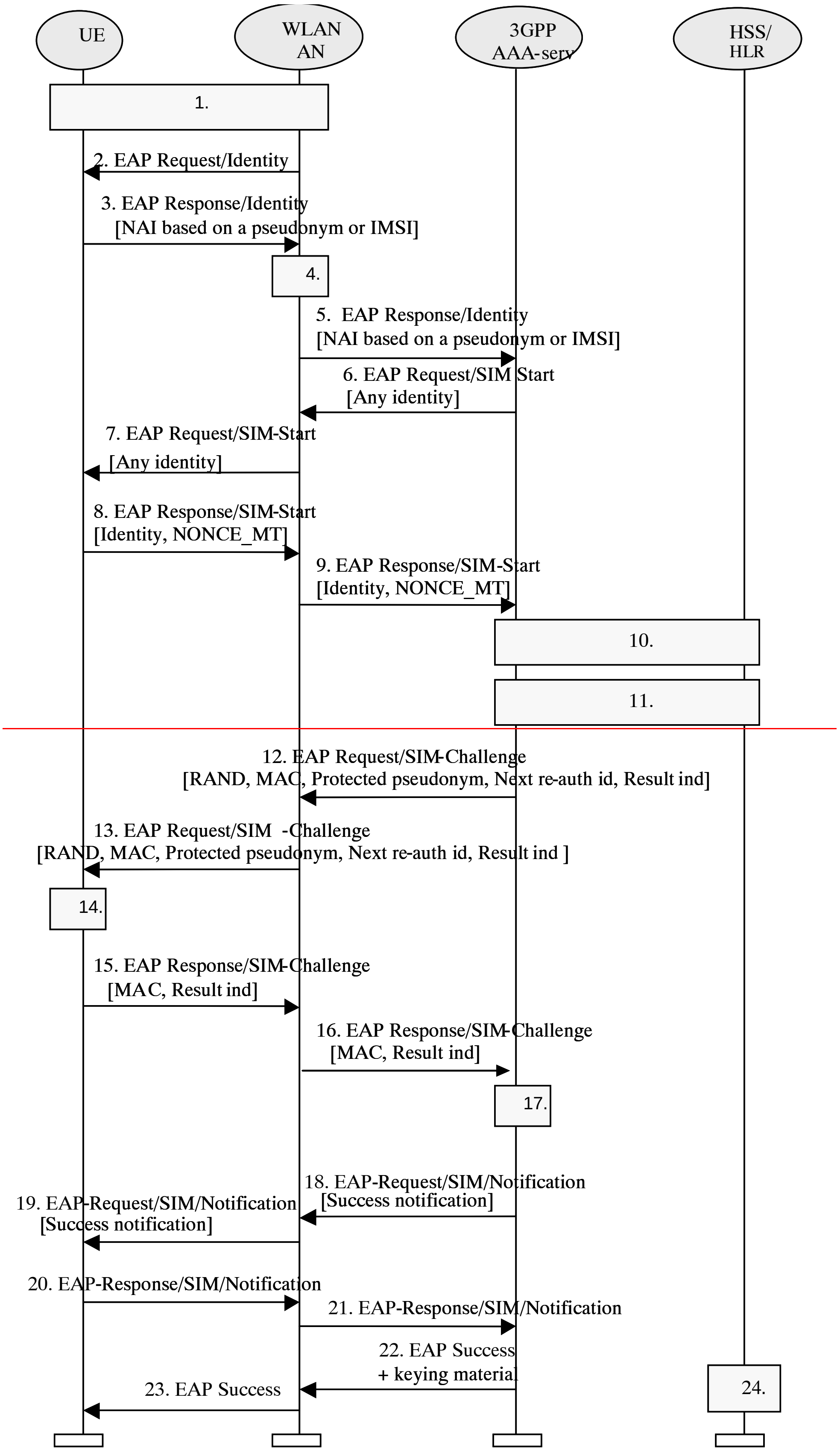
6.1.2 GSM SIM based WLAN Access authentication

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 section 6.1.2.1. This authentication method satisfies the authentication requirements from section 4.2, without the need for a UICC with a USIM application

Editor's note: Also see section 4.2.4 on WLAN UE split.

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.


UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity [NAI based on a pseudonym or IMSI]
4.
5. EAP Response/Identity [NAI based on a pseudonym or IMSI]
6. EAP Request/SIM Start [Any identity]
7. EAP Request/SIM-Start [Any identity]
8. EAP Response/SIM-Start [Identity, NONCE_MT]
9. EAP Response/SIM-Start [Identity, NONCE_MT]
10.
11.
12. EAP Request/SIM-Challenge [RAND, MAC, Protected pseudonym, Next re-auth id, Result ind]
13. EAP Request/SIM -Challenge [RAND, MAC, Protected pseudonym, Next re-auth id, Result ind]
14.
15. EAP Response/SIM-Challenge [MAC, Result ind]
16. EAP Response/SIM-Challenge [MAC, Result ind]
17.
18. EAP-Request/SIM/Notification [Success notification]
19. EAP-Request/SIM/Notification [Success notification]
20. EAP-Response/SIM/Notification
21. EAP-Response/SIM/Notification
22. EAP Success + keying material
23. EAP Success
24.

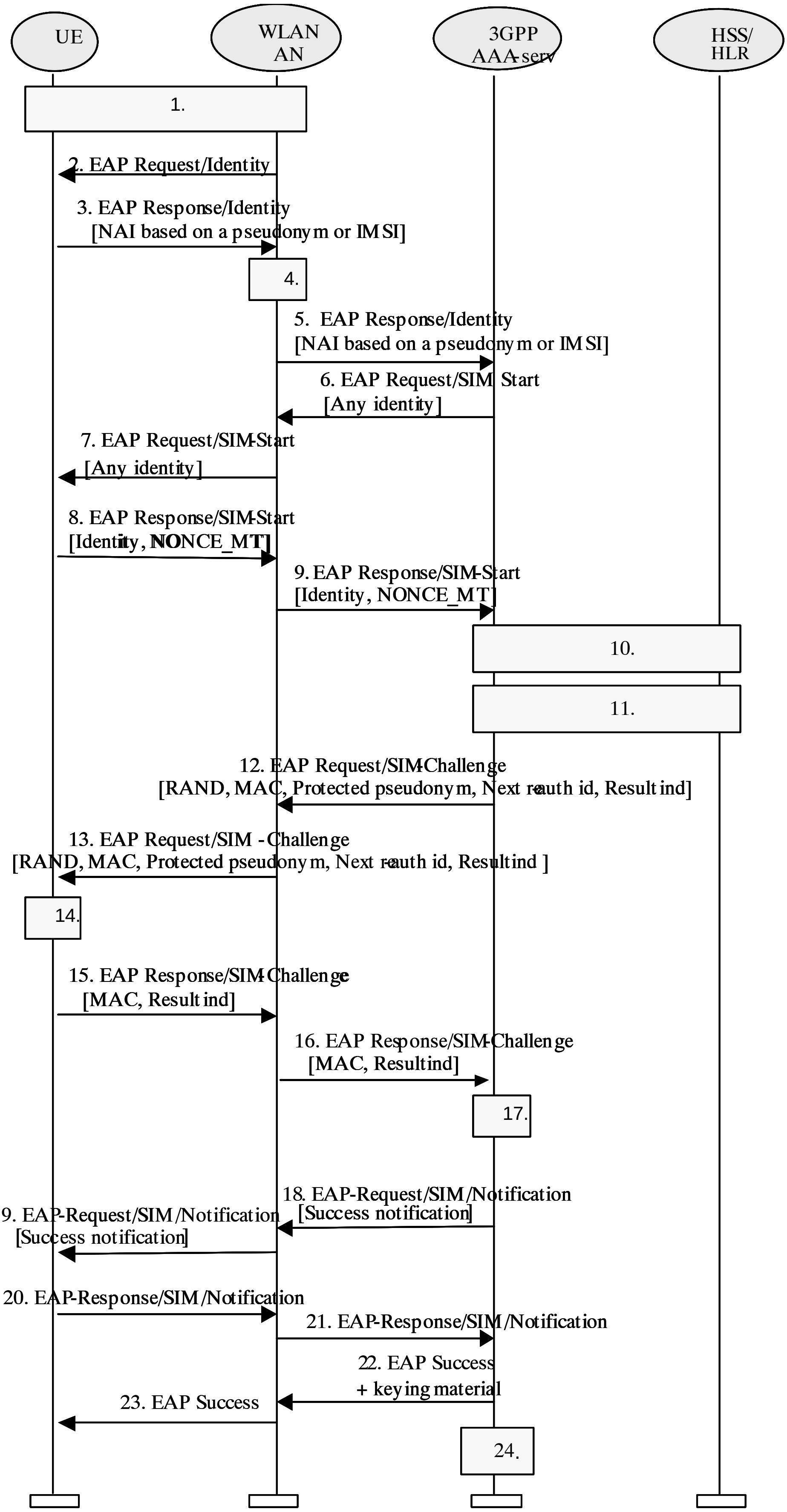

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity [NAI based on a pseudonym or IMSI]
4.
5. EAP Response/Identity [NAI based on a pseudonym or IMSI]
6. EAP Request/SIM Start [Any identity]
7. EAP Request/SIM-Start [Any identity]
8. EAP Response/SIM-Start [Identity, NONCE_MT]
9. EAP Response/SIM-Start [Identity, NONCE_MT]
10.
11.
12. EAP Request/SIM-Challenge [RAND, MAC, Protected pseudonym, Next re-auth id, Result ind]
13. EAP Request/SIM - Challenge [RAND, MAC, Protected pseudonym, Next re-auth id, Resultind]
14.
15. EAP Response/SIM-Challenge [MAC, Result ind]
16. EAP Response/SIM-Challenge [MAC, Resultind]
17.
18. EAP-Request/SIM/Notification [Success notification]
19. EAP-Request/SIM/Notification [Success notification]
20. EAP-Response/SIM/Notification
21. EAP-Response/SIM/Notification
22. EAP Success + keying material
23. EAP Success
24.

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 RFC 2486. NAI contains either a temporary identifier (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 EAP/SIM.

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 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.

    Although this step is presented after step 9 in this examples, 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 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 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.

11. The 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 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 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 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 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 was received, then the WLAN-UE stores the pseudonym 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 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 whether simultaneous sessions are not allowed, or whether the number of allowed sessions has been exceeded. The exception in this process is 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. In that case the authentication process continues normally.

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.

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Security ó S3#36
Shenzhen, China 23 - 26 November 2004

Tdoc ⌘S3-040949

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**045**	⌘ **rev**	**-**	⌘	Current version:	**6.2.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □   ME ☒ Radio Access Network □   Core Network ☒

Title:	⌘	Clarifications and corrections on the use of pseudonyms		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	29/10/2004
Category:	⌘	**F**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	TS 33.234 still contains some chapters in which the word ìpseudonymî and ìtemporary identityî are used inconsistently.
Summary of change:	⌘	The words ìpseudonymî and ìtemporary identityî are replaced or changed where necessary. Some additional clarifications are added.
Consequences if not approved:	⌘	The WLAN UE or the AAA server may only consider the pseudonyms where in fact they should consider any temporary identity (re-authentication identity or pseudonym)

Clauses affected:	⌘	5.1.6, 6.1.1.1, 6.1.2.1, 6.4.1, 6.4.2, 6.4.4				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

*** BEGIN SET OF CHANGES ***

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 so that they can only be used once. 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 scenario 3, 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).

An exception is when the full authentication is being performed for tunnel establishment in scenario 3, in which case the IMSI may be sent even if identity privacy support was activated by the home network. In this situation, the authentication exchange is performed in a protected tunnel which provides encryption and integrity protection, as well as replay protection.

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 ~~pseudonyms~~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 ~~pseudonym~~temporary identity.

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

~~pseudonym~~re-authentication identity, the AAA server shall request~~s~~ the ~~user~~ WLAN UE to send its ~~permanent identity~~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.

Editor's note: The use of PEAP with EAP/AKA and EAP/SIM is currently under consideration. If PEAP is used, the temporary identity privacy scheme provided by EAP/AKA and EAP/SIM is not needed.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

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.

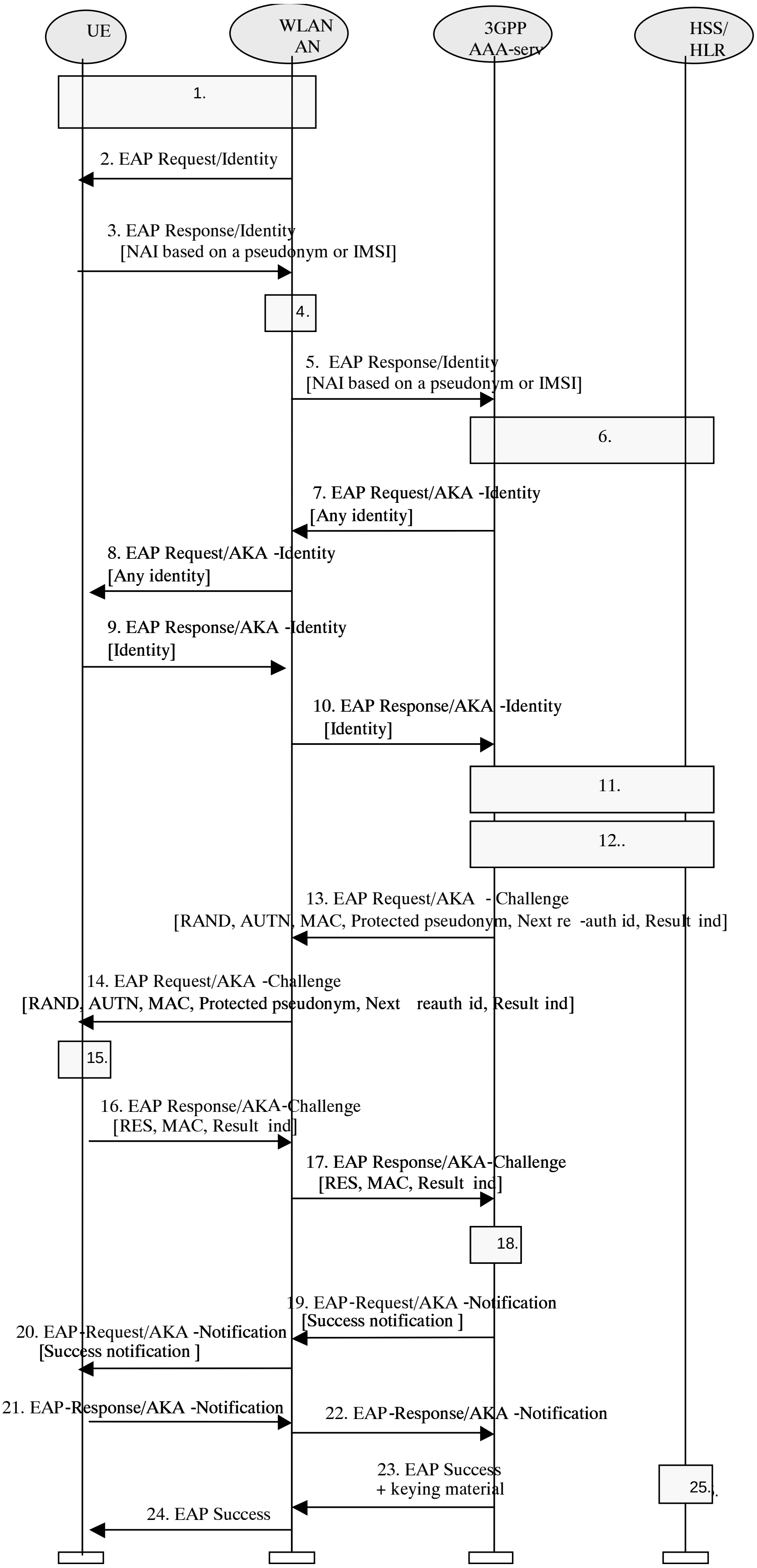

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity [NAI based on a pseudonym or IMSI]
4.
5. EAP Response/Identity [NAI based on a pseudonym or IMSI]
6.
7. EAP Request/AKA -Identity [Any identity]
8. EAP Request/AKA -Identity [Any identity]
9. EAP Response/AKA -Identity [Identity]
10. EAP Response/AKA -Identity [Identity]
11.
12..
13. EAP Request/AKA - Challenge [RAND, AUTN, MAC, Protected pseudonym, Next re -auth id, Result ind]
14. EAP Request/AKA -Challenge [RAND, AUTN, MAC, Protected pseudonym, Next reauth id, Result ind]
15.
16. EAP Response/AKA-Challenge [RES, MAC, Result ind]
17. EAP Response/AKA-Challenge [RES, MAC, Result ind]
18.
19. EAP-Request/AKA -Notification [Success notification]
20. EAP-Request/AKA -Notification [Success notification]
21. EAP-Response/AKA -Notification
22. EAP-Response/AKA -Notification
23. EAP Success + keying material
24. EAP Success
25..

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 RFC 2486. NAI contains either a ~~temporary identifier~~ ~~(~~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 EAP/AKA [4].

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.

   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 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 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 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 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 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 ~~was~~ were received, then the WLAN-UE stores the ~~pseudonym~~ 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 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.

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.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

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.

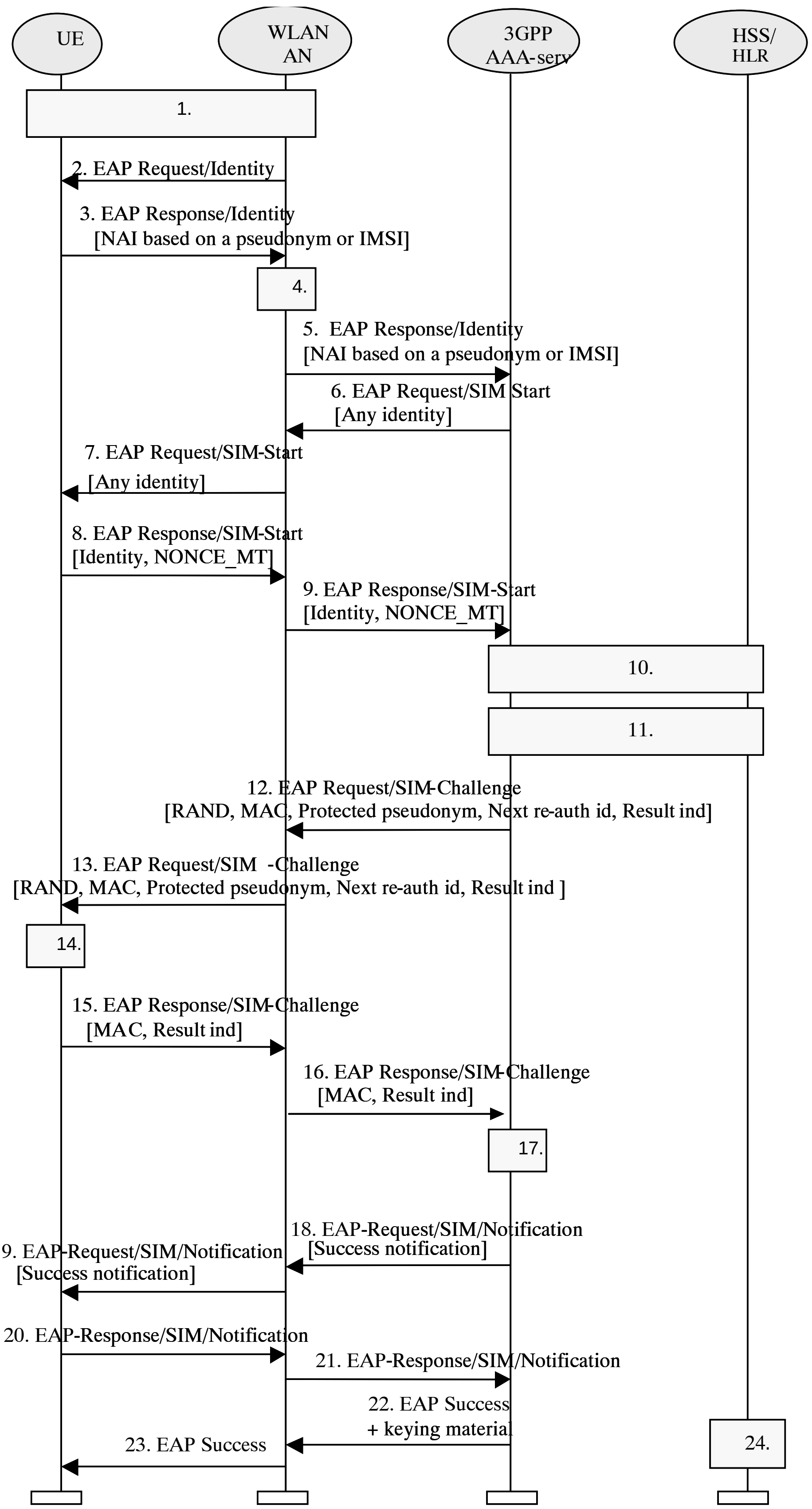

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity [NAI based on a pseudonym or IMSI]
4.
5. EAP Response/Identity [NAI based on a pseudonym or IMSI]
6. EAP Request/SIM Start [Any identity]
7. EAP Request/SIM-Start [Any identity]
8. EAP Response/SIM-Start [Identity, NONCE_MT]
9. EAP Response/SIM-Start [Identity, NONCE_MT]
10.
11.
12. EAP Request/SIM-Challenge [RAND, MAC, Protected pseudonym, Next re-auth id, Result ind]
13. EAP Request/SIM -Challenge [RAND, MAC, Protected pseudonym, Next re-auth id, Result ind]
14.
15. EAP Response/SIM-Challenge [MAC, Result ind]
16. EAP Response/SIM-Challenge [MAC, Result ind]
17.
18. EAP-Request/SIM/Notification [Success notification]
19. EAP-Request/SIM/Notification [Success notification]
20. EAP-Response/SIM/Notification
21. EAP-Response/SIM/Notification
22. EAP Success + keying material
23. EAP Success
24.

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 RFC 2486. NAI contains either a ~~temporary identifier~~ ~~(~~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 EAP/SIM.

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 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.

    Although this step is presented after step 9 in this examples, 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 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 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.

11. The 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 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 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 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 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 ~~was~~ were received, then the WLAN-UE stores the ~~pseudonym~~ 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 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 whether simultaneous sessions are not allowed, or whether the number of allowed sessions has been exceeded.

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.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

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 ~~pseudonym~~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.

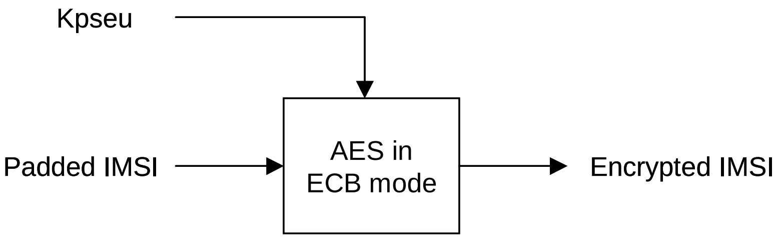
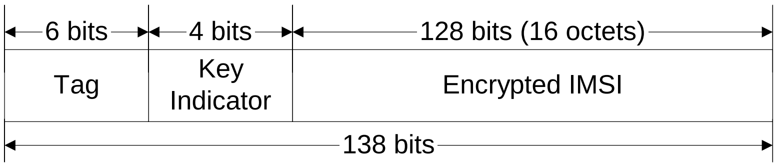


Figure 8: Encrypted IMSI generation

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.



6 bits	4 bits	128 bits (16 octets)
Tag	Key Indicator	Encrypted IMSI
138 bits		

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 identityTag 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 ~~pseudonym~~ 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.

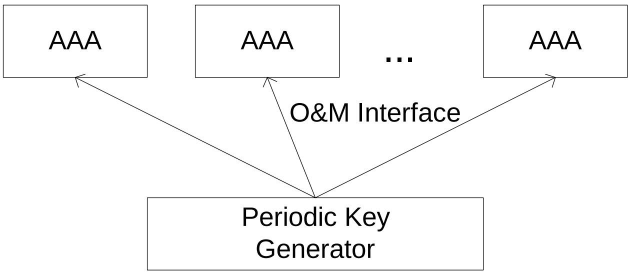


Figure 10: Key configuration via O&M

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

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

6.4.4 Acknowledged Limitations

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

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Security ó S3#36 **Tdoc ⌘S3-040958**
November 23 ñ 26, 2004

Shenzhen, China

CR-Form-v7

CHANGE REQUEST

⌘ **33.234 CR 047** ⌘**rev** **-** ⌘ Current version: **6.2.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Wn Reference Point Description		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	09/11/2004
Category:	⌘	**D**	***Release:*** ⌘	Rel-6

Use one of the following categories:
- ***F*** *(correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(addition of feature),*
- ***C*** *(functional modification of feature)*
- ***D*** *(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	To define the Wn interface in the TS 33.234, as the Rel-6 is going to freeze.
Summary of change:	⌘	To define the Wn interface which interface the WAG and the WLAN-AN network.
Consequences if not approved:	⌘	TS 33.234 will contain editorial notes in reference points description clause and does not contain description on Wn interface.

Clauses affected:	⌘	4.1.5				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

*** BEGIN SET OF CHANGES ***

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 ñ 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. ~~The definition of this reference point is for further study.~~

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.

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Security ó S3#36 ***Tdoc ⌘S3-040959***
November 23 ñ 26, 2004

Shenzhen, China

CR-Form-v7

CHANGE REQUEST

⌘ **33.234 CR 048** ⌘**rev** **-** ⌘ Current version: **6.2.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Removal of word ìscenarioî			
Source:	⌘	SA WG3			
Work item code:	⌘	WLAN	***Date:***	⌘	09/11/2004
Category:	⌘	**F**	***Release:***	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	In SA3#35 meeting, LS S3-040701from SA2 recommends to replace the work ìscenarioî with an alternate word in TS 33.234, because it is just the term to distinguish possible steps in developing/deploying I-WLAN.
Summary of change:	⌘	To replace the word ìscenarioî with alternate words simailar to TS 23.234 and TS 22.234.
Consequences if not approved:	⌘	TS 33.234 is not aligned with the TS 22.234 and TS 23.234

Clauses affected:	⌘	3.1, 4.1.1, 4.1.2, 4.1.3, 5.1.1, 5.1.6, 5.1.8, 5.2.1, 5.2.2, 5.3.1, 6.1.5, 6.2.1, 6.2.2, 6.3.1, 6.3.2, 6.5, Annex E				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

*** BEGIN SET OF CHANGES ***

3.1 Definitions

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

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.

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.

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

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

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

4.1.1 Non roaming WLAN interworking Reference Model

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

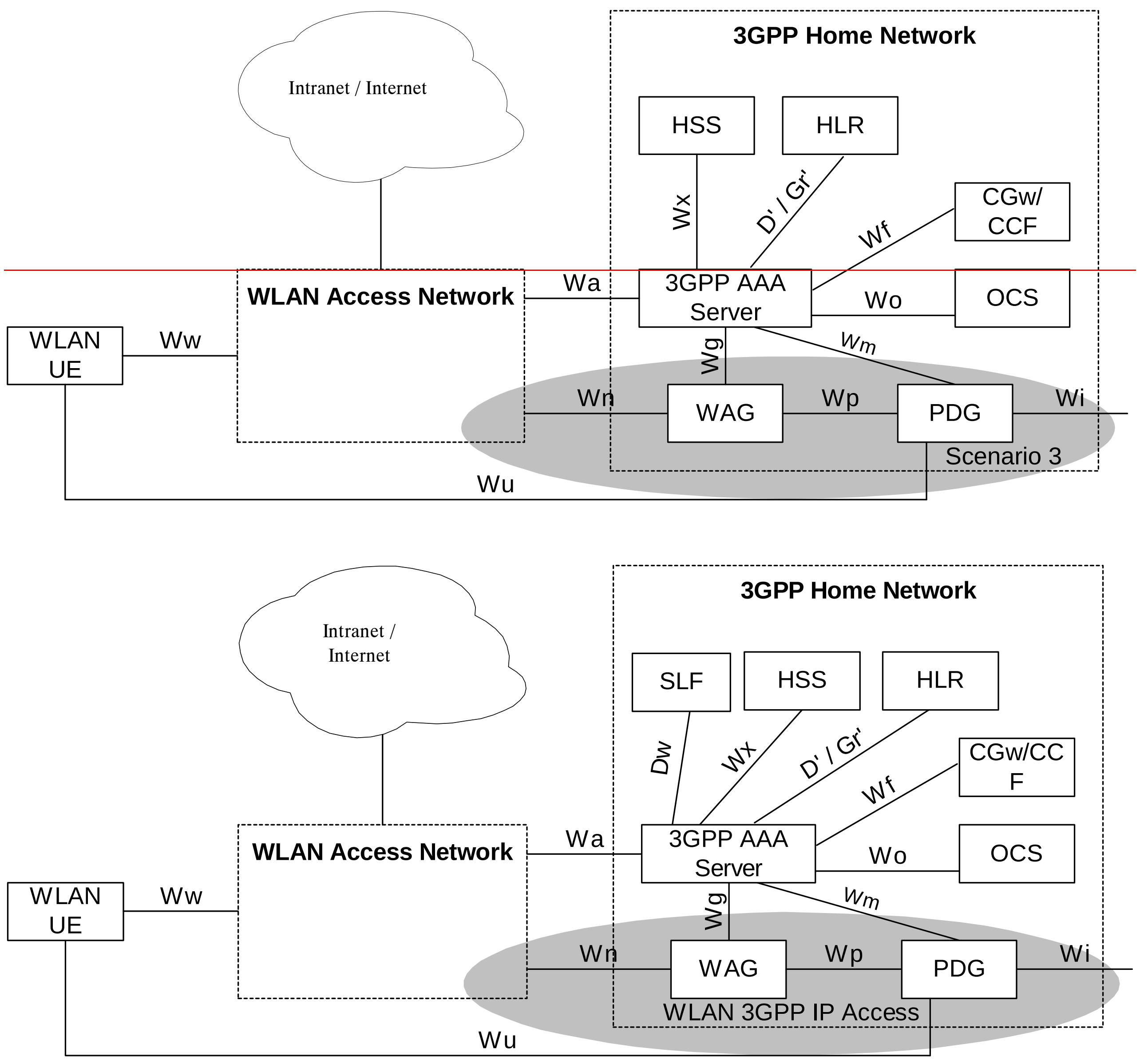
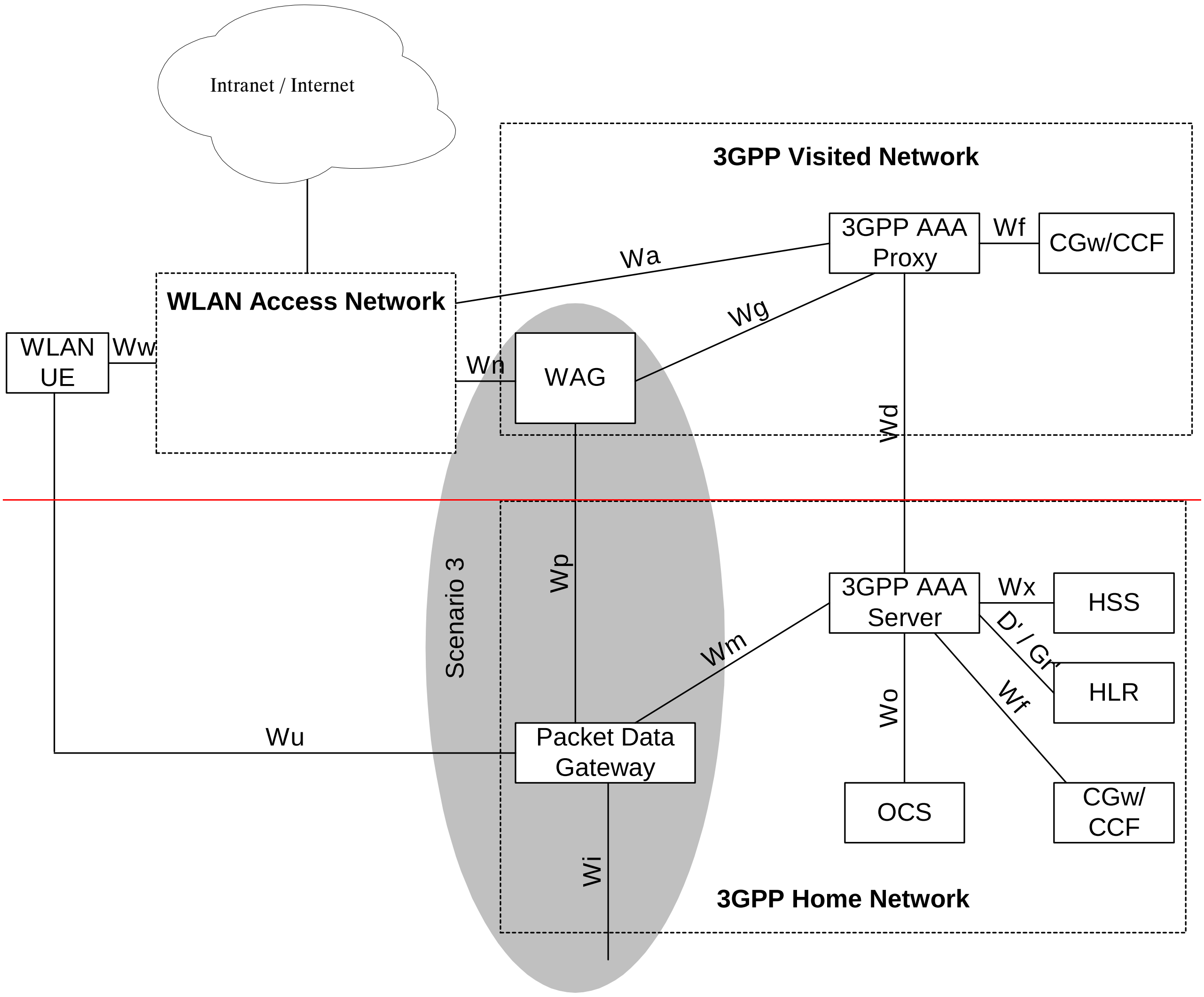


Figure 1: Non-roaming reference model (the shaded area refers to ~~scenario 3~~WLAN 3GPP IP Access functionality)

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).



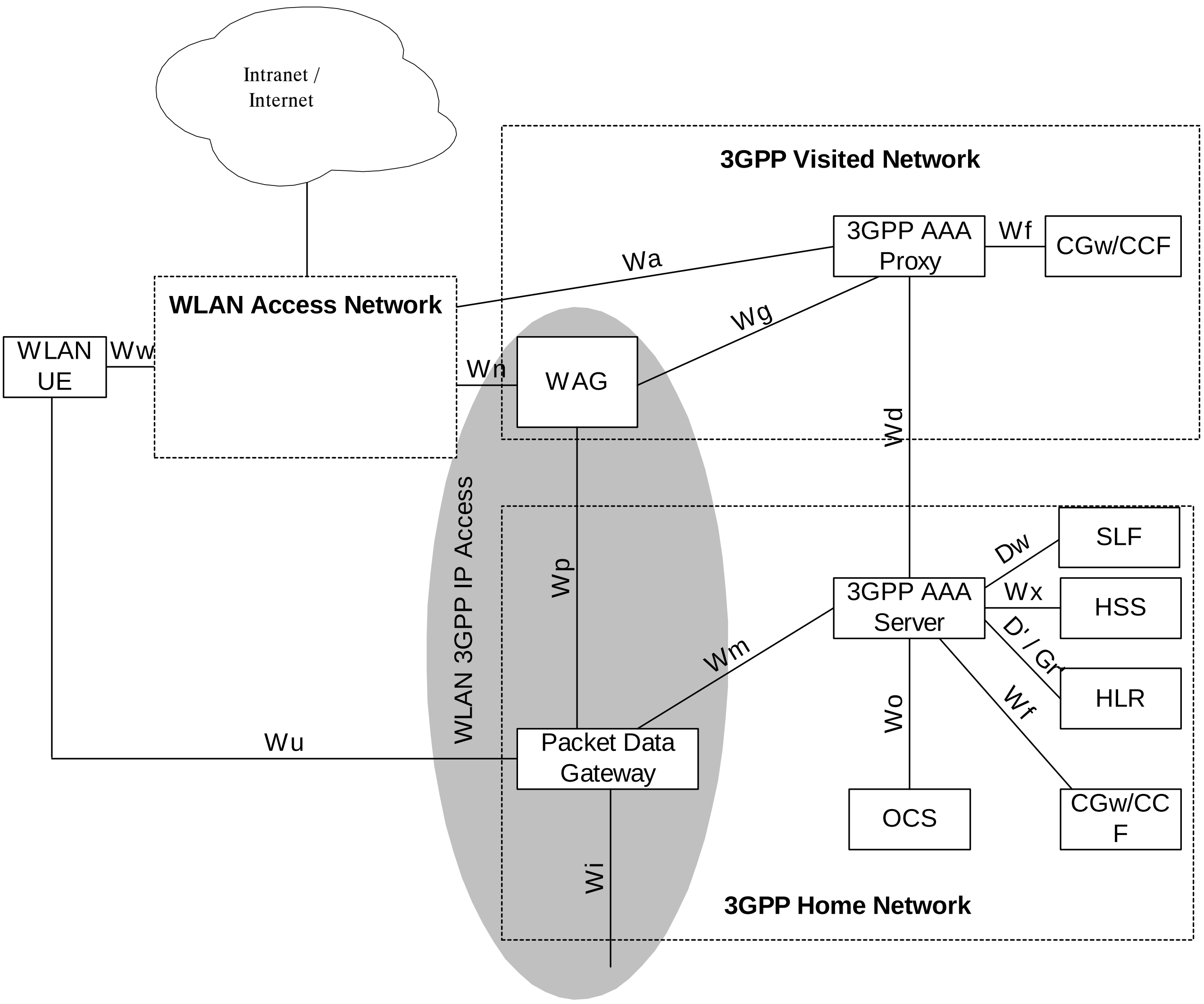
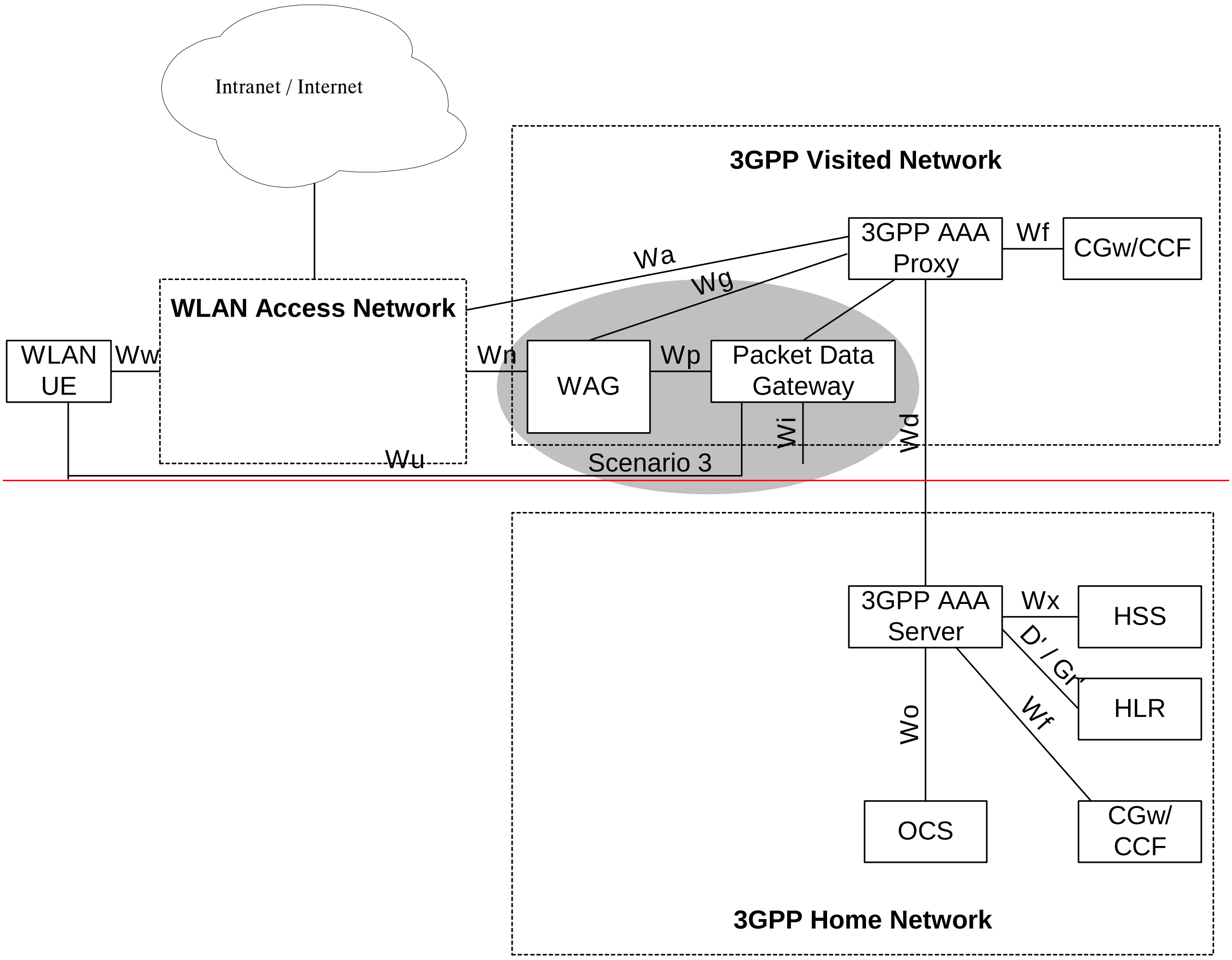


Figure 2: Roaming reference model - 3GPP PS based services provided via the 3GPP Home Network (the shaded area refers to ~~scenario 3~~WLAN 3GPP IP Access functionality)

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 PDGW).


Intranet / Internet
3GPP Visited Network
3GPP AAA Proxy
Wf
CGw/CCF
Wa
Wg
WLAN Access Network
WLAN UE
Ww
Wn
WAG
Wp
Packet Data Gateway
Wi
Wd
Wu
Scenario 3
3GPP AAA Server
Wx
HSS
D' / Gr'
HLR
Wf
Wo
OCS
CGw/ CCF
3GPP Home Network

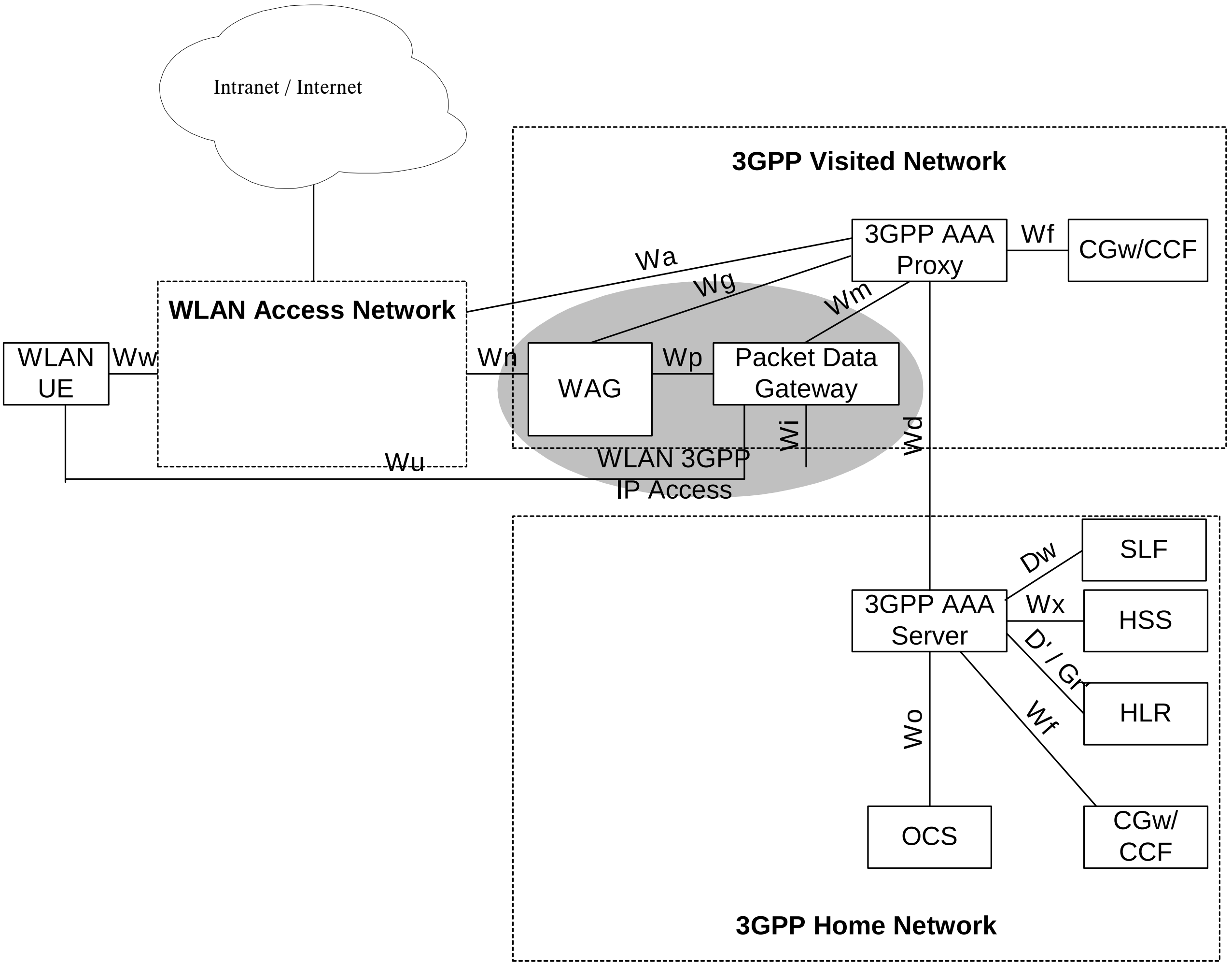


Figure 3: Roaming reference model - 3GPP PS based services provided via the 3GPP Visited Network (the shaded area refers to ~~scenario 3~~WLAN 3GPP IP Access functionality)

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

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~~W~~ 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 ~~scenario 3~~WLAN 3GPP IP Access are to be independent of the link layer security in ~~scenario 2~~WLAN Direct IP Access.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

5.1.1 End to End WLAN Access Authentication (~~Scenario 2~~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]).

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

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 so that they can only be used once. 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 ~~scenario 3~~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).

An exception is when the full authentication is being performed for tunnel establishment in ~~scenario 3~~WLAN 3GPP IP Access, in which case the IMSI may be sent even if identity privacy support was activated by the home network. In this situation, the authentication exchange is performed in a protected tunnel which provides encryption and integrity protection, as well as replay protection.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

5.1.8 Security Association Management for UE-initiated tunnels (~~Scenario 3~~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.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

5.2 Confidentiality protection

5.2.1 Confidentiality protection in ~~scenario 2~~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 ~~scenario 3~~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 ~~scenario 2~~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 ~~scenario 3~~WLAN 3GPP IP Access

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

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

6.1.5 Mechanisms for the set up of UE-initiated tunnels (~~Scenario 3~~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.
- 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.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

6.2 Confidentiality mechanisms

6.2.1 Confidentiality mechanisms in ~~scenario 2~~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 ~~scenario 3~~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.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

6.3 Integrity mechanisms

6.3.1 Integrity mechanisms in ~~scenario 2~~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 ~~scenario 3~~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.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

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 (~~scenario 3~~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].

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

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

Editor's note: The discussion on the security mechanisms for the set up of UE-initiated tunnels is still ongoing. The text in section 6.1.5 reflects the current working assumption of SA3. Alternatives still under discussion in SA3 are contained in this Annex. They may be replace the current working assumption in section 6.1.5 of the main body if problems with the working assumptions arise. Otherwise, this annex will be removed before the TS is submitted for approval.

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.

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Security ó S3#36
Shenzhen, China, 23-26 November 2004

S3-041108

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**049**	⌘**rev**	**1**	⌘	Current version:	**6.2.1**	⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects:	UICC apps⌘	□	ME	☒	Radio Access Network	□	Core Network	□

Title:	⌘	Correction of WRAP to CCMP		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	25/11/2004
Category:	⌘	**F**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	In TS 33.234, three WLAN link layer encryption protocol are mentioned, WEP, TKIP and WRAP. But this is the old description of WLAN security specfication IEEE802.11i. WRAP is deleted in final version of IEEE802.11i, only CCMP is left.So we should delete corresponding contents of WRAP in TS33.234 to align with IEEE specification.
Summary of change:	⌘	Delete corresponding contents of WRAP, and replace with CCMP in TS33.234.
Consequences if not approved:	⌘	Not in line with reference IEEE specification.

Clauses affected:	⌘	A.1.3				
		Y	**N**			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

********** START OF CHANGE **********

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 ~~Wireless Robust Authenticated Protocol (WRAP)~~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 (~~WRAP~~CCMP) but very much better than WEP.

~~WRAP (AES)~~

~~The Wireless Robust Authenticated Protocol (WRAP) is the long-term solution and is based on the Advanced Encryption Standard (AES). AES is a block cipher that can be used in different modes of operation. In 802.11i, two modes have been discussed: Offset Codebook (OCB) and Counter-mode with CBC-MAC (CCM). These two modes use AES differently to provide encryption and message integrity. OCB is a mode that provides both encryption and integrity in one run. CCM uses the Counter-mode for encryption and CBC-MAC for integrity. It is currently undecided if both or only one of the modes will be included in the final 802.11i spec. Both modes have been submitted to NIST as proposed block cipher modes.~~

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

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.

********** END OF CHANGE **********

3GPP TSG SA WG3 Security ó S3#36
Shenzhen, China, 23-26 November 2004

S3-041155

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.234**	**CR**	**050**	⌘ **rev**	**1** ⌘	Current version:	**6.2.1** ⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network □

Title:	⌘	Removal of resolved editors' notes		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	26/11/2004
Category:	⌘	**D**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	In TS 33.234, many of the Editors' notes have been resolved and should be removed from the specification.
Summary of change:	⌘	Delete resolved Editors' Notes.
Consequences if not approved:	⌘	Outdated editors information left in the TS

Clauses affected:	⌘	4.2.2, 4.2.4.2, 4.2.6, 5.1.6, 5.4, 6.1.3, 6.1.5, 6.6, Annex E				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

********** FIRST CHANGE **********

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.

~~Editors note: LS (S3-030166) sent to IEEE 802.11 task group i on their requirements over key length and entropy of keying material~~

- 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.

********** NEXT CHANGE **********

4.2.4.2 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. If this is the case, then the following requirements shall be satisfied:

- Any local interface shall be protected against eavesdropping, attacks on security-relevant information. This protection may be provided by physical or cryptographic means.
- The endpoints of a local interface should be authenticated and authorised. The authorisation may be implicit in the security set-up.
- 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.

~~Editors note: It was agreed at SA3#31 that for WLAN interworking, modification of EAP parameters on the Bluetooth interface will cause EAP to fail in the network or on the USIM. It was therefore agreed to remove the "undetected modification" requirement from this TS.~~

********** NEXT CHANGE **********

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 PDGW 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 scenario 3 are to be independent of the link layer security in scenario 2.

~~Editor's note: The independence requirement is not for security reasons. If the solution developed implies significant inefficiencies then this would be reported to SA WG2 for possible revision of this independence requirement.~~

********** NEXT CHANGE **********

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 so that they can only be used once. 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 scenario 3, 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).

An exception is when the full authentication is being performed for tunnel establishment in scenario 3, in which case the IMSI may be sent even if identity privacy support was activated by the home network. In this situation, the authentication exchange is performed in a protected tunnel which provides encryption and integrity protection, as well as replay protection.

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 pseudonyms, 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 pseudonym.

If identity privacy is used but the AAA server cannot identify the user by its pseudonym, the AAA server requests the user 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.

~~Editor's note: The use of PEAP with EAP/AKA and EAP/SIM is currently under consideration. If PEAP is used, the temporary identity privacy scheme provided by EAP/AKA and EAP/SIM is not needed.~~

********** NEXT CHANGE **********

5.4 ~~Visibility and configurability~~ Void

~~Editor's note: This section shall contain what the subscriber shall be able to configure and what is visible for the subscriber regarding the actual protection the subscriber is provided with.~~

********** NEXT CHANGE **********

6.1.3 EAP support in Smart Cards

~~Editors note: LS (S3-030187/ S1-030546) from SA1 has stated, "There are requests from operators for a secure SIM based WLAN authentication solution". SA3 has SA1 in an LS (S3-030306) if this request is confirmed. The input paper to SA3 on this can be found at: http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_28_Berlin/Docs/ZIP/S3-030198.zip~~

********** NEXT CHANGE **********

6.1.5 Mechanisms for the set up of UE-initiated tunnels (Scenario 3)

- 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.
- 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.

~~Editor's note: The discussion on the security mechanisms for the set up of UE-initiated tunnels is still ongoing in SA3. The text in this section reflects the current working assumption of SA3. Alternatives still under discussion in SA3 are contained in Annex E. They may replace the current working assumption in this section if problems with the working assumption arise. Otherwise, Annex E will be removed before the TS is submitted for approval. The above points on the use of IKEv2 are dependent on the analysis of the open issues on legacy VPN clients and key management; in particular, the use of EAP-AKA and EAP-SIM will be studied.~~

********** NEXT CHANGE **********

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 security protection (confidentiality and/or integrity) in the tunnel (for example high trust between the 3GPP network operator and the WLAN access provider). This means that transform IDs for encryption ENCR_NULL and NONE for integrity shall be allowed to negotiate, as specified in ref. [29]

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

~~Editor's note: An example of a profile of IPSec ESP, which may be useful to study when writing this section, can be found in TS 33.210, section 5.3. Future editions of this specification will define additional profiles.~~

********** NEXT CHANGE **********

Annex E: (informative): Alternative Mechanisms for the set up of UE-initiated tunnels (Scenario 3)

~~Editor's note: The discussion on the security mechanisms for the set up of UE-initiated tunnels is still ongoing. The text in section 6.1.5 reflects the current working assumption of SA3. Alternatives still under discussion in SA3 are contained in this Annex. They may be replace the current working assumption in section 6.1.5 of the main body if problems with the working assumptions arise. Otherwise, this annex will be removed before the TS is submitted for approval.~~

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.

********** END OF CHANGES **********