Technical Specification Group Services and System Aspects **TSGS#25(04)0622**
Meeting #25, Palm Springs, USA

Source: **SA WG3**

Title: **9 CRs to 33.234: Various changes to WLAN Interworking Security (Rel-6)**

Document for: **Approval**

Agenda Item: **7.3.3**

The following CRs were 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-040622	33.234	010	-	Rel-6	Update referece to RFC3748 "Extensible Authentication Protocol (EAP)"	F	6.1.0	S3-040555	WLAN
SP-040622	33.234	011	-	Rel-6	References update	F	6.1.0	S3-040599	WLAN
SP-040622	33.234	012	-	Rel-6	Sending of temporary identities from WLAN UE	F	6.1.0	S3-040601	WLAN
SP-040622	33.234	013	-	Rel-6	Clarification on fast re-authentication procedure	F	6.1.0	S3-040603	WLAN
SP-040622	33.234	014	-	Rel-6	Correction of authentication procedure for WLAN UE split	F	6.1.0	S3-040610	WLAN
SP-040622	33.234	015	-	Rel-6	Modification of mechanism to restrict simultaneous WLAN sessions	C	6.1.0	S3-040668	WLAN
SP-040622	33.234	016	-	Rel-6	Wa interface security	C	6.1.0	S3-040669	WLAN
SP-040622	33.234	017	-	Rel-6	Introduction of protected result indications	F	6.1.0	S3-040670	WLAN
SP-040622	33.234	018	-	Rel-6	Tunnel authentication procedure in Wm interface	F	6.1.0	S3-040671	WLAN

3GPP TSG SA WG3 Security — S3#34 **S3-040555**

July 6 - 9, 2004, Acapulco, Mexico

CR-Form-v7

CHANGE REQUEST

⌘	**33.234**	**CR**	**010**	⌘ **rev**	**-**	⌘ Current version:	**6.1.0** ⌘

*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:	⌘	Update referece to RFC3748 "Extensible Authentication Protocol (EAP)"		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	09/07/2004
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:	⌘	Correct reference section
Summary of change:	⌘	Update refereces from RFC2284bis to RFC3748 “Extensible Authentication Protocol (EAP)” . RFC3748 obsoletes RFC2284bis
Consequences if not approved:	⌘	WLAN access specfciations would refference an obsolete RFC.

		Y	N		
Clauses affected:	⌘	2 - References			
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

*** START CHANGE***

2 References

[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] ~~draft-ietf-eap-rfc2284bis-06~~ rfc3748.txt, ~~October 2003~~June 2004: "~~PPP~~ Extensible Authentication Protocol (EAP)".

[4] draft-arkko-pppext-eap-aka-11, October 2003: "EAP AKA Authentication".

[5] draft-haverinen-pppext-eap-sim-12, October 2003: "EAP SIM Authentication".

*** END OF CHANGE***

3GPP TSG SA WG3 Security — S3#34 **_Tdoc ⌘S3-040599_**
Acapulco, Mexico 6 - 9 July 2004

CR-Form-v7

CHANGE REQUEST

⌘	**33.234**	**CR**	**011**	⌘ **rev**	**-**	⌘	Current version:	**6.1.0**	⌘

*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:	⌘	References update		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	21/06/2004
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:	⌘	Some references in TS 33.234 do not match the current status
Summary of change:	⌘	Internet drafts in references chapter are updated
Consequences if not approved:	⌘	Document versions referenced in TS 33.234 may be obsolete

Clauses affected:	⌘	2

Other specs affected: ⌘

Y	N		
	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] draft-ietf-eap-rfc2284bis-06.txt, October 2003: "PPP Extensible Authentication Protocol (EAP)".

[4] draft-arkko-pppext-eap-aka-~~11~~12, ~~October~~ April ~~2003~~2004: "~~EAP AKA Authentication~~ Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA) ". IETF Work in progress

[5] draft-haverinen-pppext-eap-sim-~~12~~13, ~~October~~ April 2003: "~~EAP SIM Authentication~~ 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-~~03~~08.txt, ~~October~~ June 2003: "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-~~01~~02.txt, ~~November~~ June ~~2003~~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-ikev2-13.txt, March 2004: "Internet Key Exchange (IKEv2) Protocol".

[30] RFC 2406, November 1998: "IP Encapsulating Security Payload (ESP)".

[31] draft-ietf-ipsec-ui-suites-~~05~~06.txt, April 2004: "Cryptographic Suites for IPsec". IETF Work in progress

[32] draft-ietf-ipsec-udp-encaps-~~08~~09.txt, ~~February~~ May 2004: "UDP Encapsulation of IPsec Packets". IETF Work in progress

[33] draft-ietf-ipsec-ikev2-algorithms-~~04~~05.txt, ~~September~~ April ~~2003~~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".

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Security — S3#34 **_Tdoc ⌘[H1]S3-040601_**
Acapulco, Mexico 6 – 9 July 2004

CR-Form-v7

CHANGE REQUEST

⌘	**33.234**	**CR**	**012**	⌘**rev**	**-**	⌘	Current version:	**6.1.0**	⌘

*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 temporary identities from WLAN UE		
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:	⌘	In EAP AKA/SIM internet drafts, it is stated that the WLAN UE can choose whether to use identity privacy support or not. And in the EAP AKA/SIM fast authentication procedure, it is stated that “4 … 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).” This means that when the AAA server has sent a temporary identity to the WLAN UE, the WLAN UE shall use the re-authentication id only once and mark it as deleted after use. There has been no mention about the case when pseudonym received in the last re-authentication procedure is not used in the next re-authentication attempt either because a re-authentication id is being sent or a permanent id is being requested by the AAA-Server. In these cases the unused pseudonym can be used in the next full re-authentication procedure.
Summary of change:	⌘	It should be stated in 33.234 that the WLAN UE must send a temporary identity whenever it is available and not used in the previous authentication. So a pseudonym received in the previous re-authentication procedure can be used in the full re-authentication procedure if it is not used in earlier re-authentication attempts.
Consequences if not approved:	⌘	WLAN UE may decide to send permanent user identity even if there is an unused temporary identity available, which can end up in passive or active attacks.

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. 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 — S3#34
Acapulco, Mexico 6 - 9 July 2004

Tdoc ⌘S3-040603

CR-Form-v7

CHANGE REQUEST

⌘	**33.234**	**CR**	**013**	⌘**rev**	**-**	⌘ Current version:	**6.1.0** ⌘

*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 fast re-authentication procedure		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	16/06/2004
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:	⌘	Fast re-authentication procedure is specified in TS 33.234. However, it is not clearly written how the re-use of keys is performed. This CR proposes to specify which keys are re-used and which ones are generated again in the process.
Summary of change:	⌘	The key derivation process for fast re-authentication is specified.
Consequences if not approved:	⌘	Misunderstanding of the fast re-authentication process and wrong selection of keys.

Clauses affected:	⌘	6.1.4				
		Y	**N**			
Other specs affected:	⌘	X		Other core specifications	⌘	24.234
			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.

*** END SET OF CHANGES ***

3GPP TSG- SA WG3 SECURITY Meeting #34
Acapulco, Mexico, July 6-9 2004

Tdoc ⌘S3-040610

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.234**	**CR**	**014**	⌘**rev**	**-** ⌘	Current version: **6.1.0** ⌘

*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 □

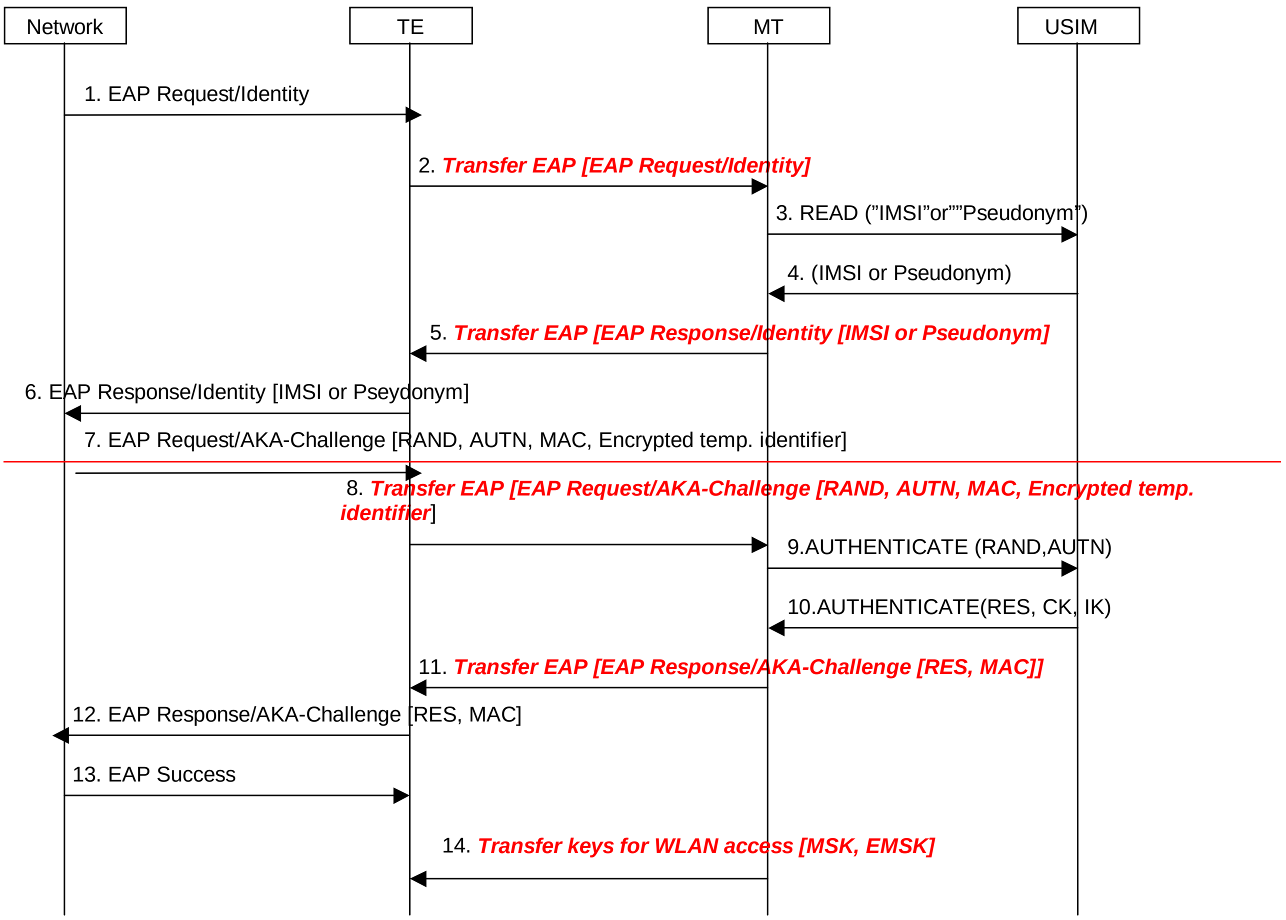
Title:	⌘	Correction of authentication procedure for WLAN UE split		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	08/07/2004
Category:	⌘	**F**	***Release:*** ⌘	Rel-6
		Use one of the following categories: ***F** (correction)* ***A** (corresponds to a correction in an earlier release)* ***B** (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 current TS describes the authentication procedures for WLAN UE split interworking. Some steps in the procedure are unnecessary and should be avoided to save resource on the MT. In particular, after the TE receives the EAP success message , the TE does not inform the MT . This means that the MT generates the MSK/EMSK and sends these keys to the TE without any indication from the TE. However, if there is an authentication failure, it is unnecessary that the MT generates these keys.
Summary of change:	⌘	Add a message between the TE and MT to indicate the authentication result to the MT.
Consequences if not approved:	⌘	MT will do unnecessary work in the authentication failure case

Clauses affected:	⌘	6.7.1, 6.7.2, 6.7.3, 6.7.4			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

6.7.1 Full authentication with EAP AKA

The process is shown in figure 11.


Network
TE
MT
USIM
1. EAP Request/Identity
2. Transfer EAP [EAP Request/Identity]
3. READ (”IMSI”or””Pseudonym”)
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 keys for WLAN access [MSK, EMSK]

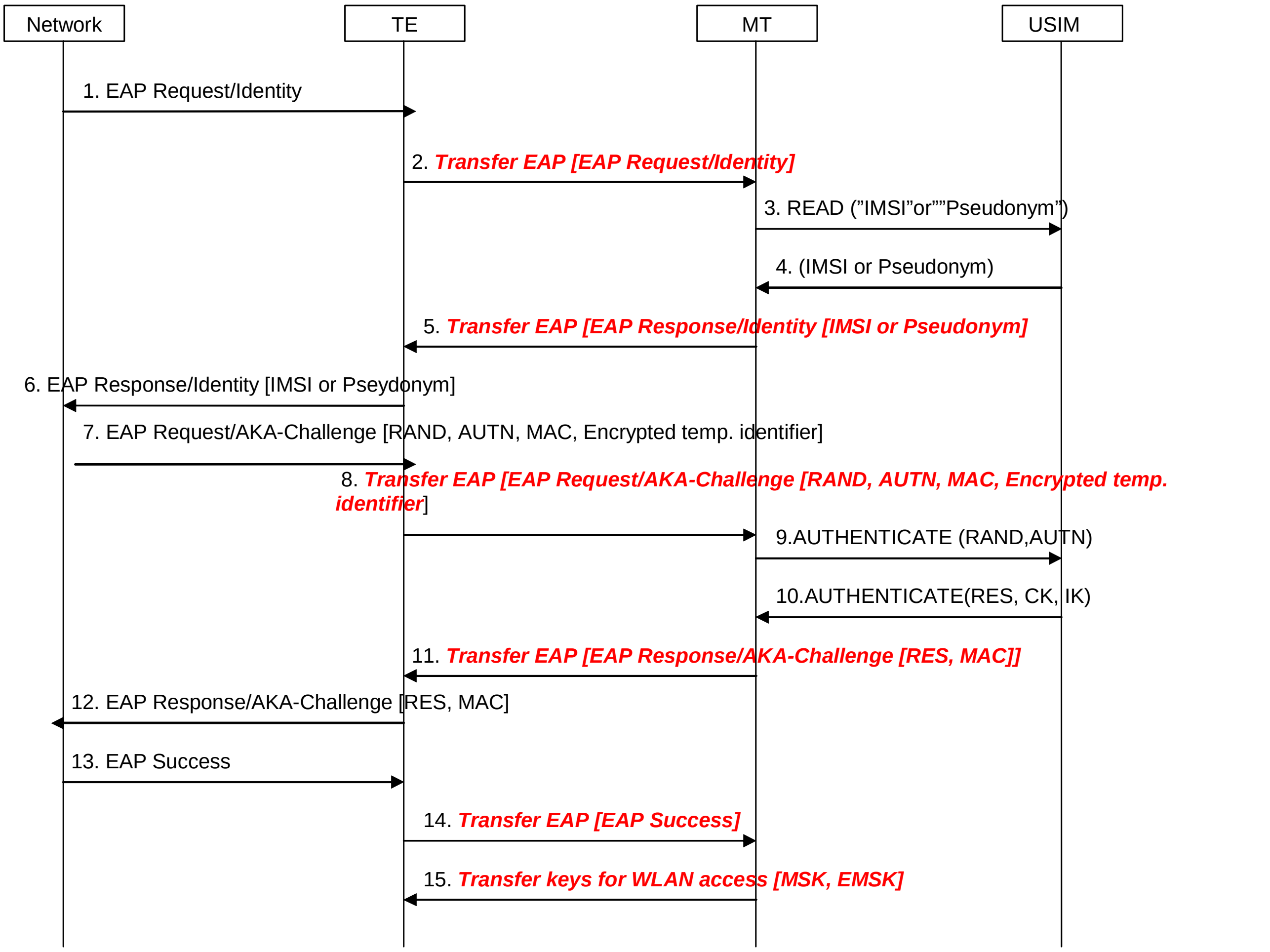

Network
TE
MT
USIM
1. EAP Request/Identity
2. Transfer EAP [EAP Request/Identity]
3. READ (”IMSI”or””Pseudonym”)
4. (IMSI or Pseudonym)
5. Transfer EAP [EAP Response/Identity [IMSI or Pseudonym]
6. EAP Response/Identity [IMSI or Pseydonym]
7. EAP Request/AKA-Challenge [RAND, AUTN, MAC, Encrypted temp. 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]

Figure 11: 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.

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.

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.

9. The MT requests authentication vectors from the USIM.

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 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.

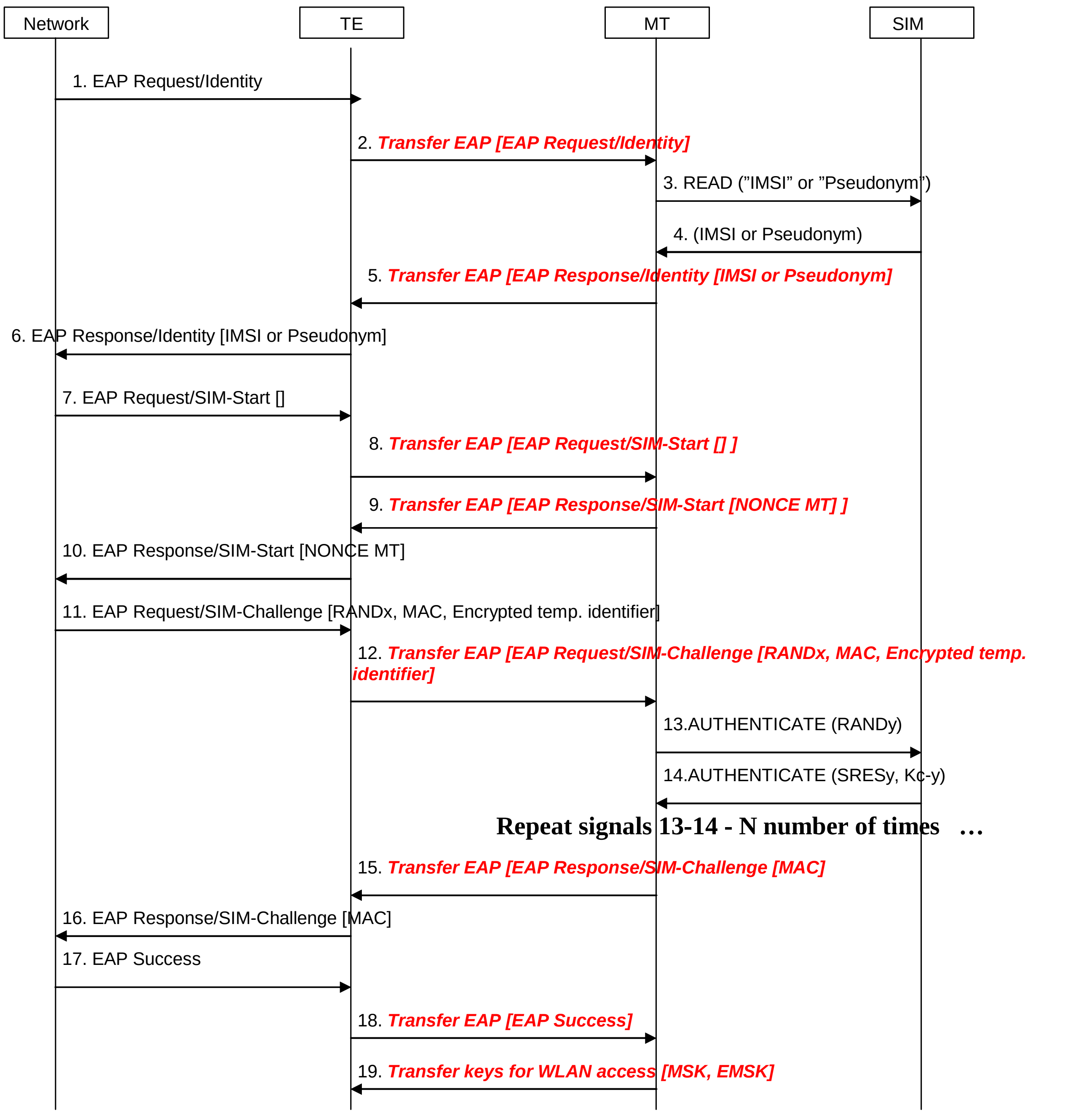
13. If both checks are correct, the network will send an EAP success message to the TE.

14 TE forwards the EAP success to the MT as a success indication.

~~14~~15. After receiving the success indication, ~~T~~the MT will derive according to ref. [4] the Master Session Key and Extended Master Session Key (MSK and EMSK) and send them to the TE. The TE uses them for security purposes, for example for WLAN link layer security

6.7.2 Full authentication with EAP SIM

The process is shown in figure 12, and it’s 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 (”IMSI” or ”Pseudonym”)
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 …
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]

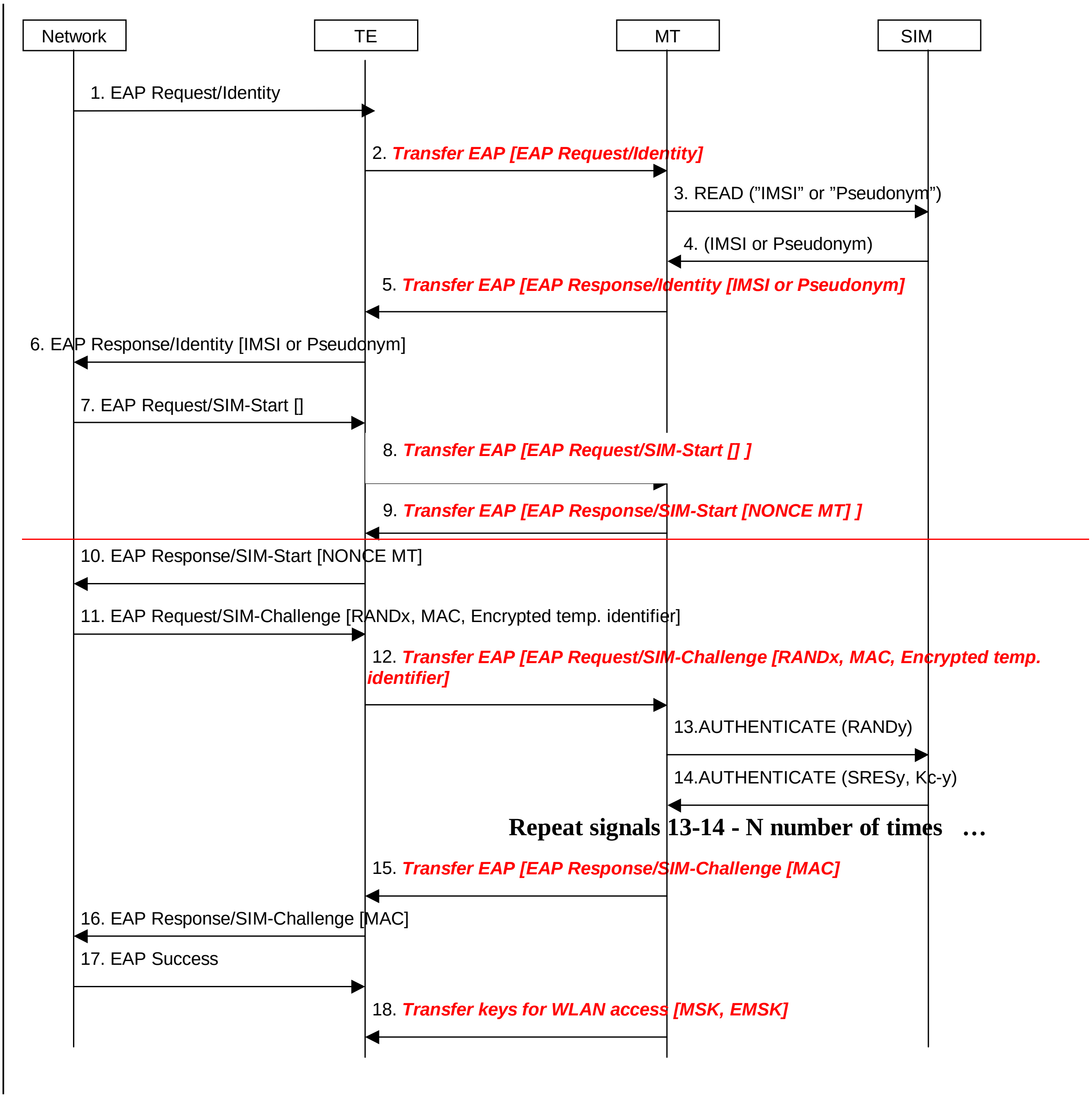

Network
TE
MT
SIM
1. EAP Request/Identity
2. Transfer EAP [EAP Request/Identity]
3. READ ("IMSI" or "Pseudonym")
4. (IMSI or Pseudonym)
5. Transfer EAP [EAP Response/Identity [IMSI or Pseudonym]
6. EAP Response/Identity [IMSI or Pseudonym]
7. EAP Request/SIM-Start []
8. Transfer EAP [EAP Request/SIM-Start []]
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 …
15. Transfer EAP [EAP Response/SIM-Challenge [MAC]
16. EAP Response/SIM-Challenge [MAC]
17. EAP Success
18. Transfer keys for WLAN access [MSK, EMSK]

Figure 12: 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 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.

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.

9. The MT generates a NONCE and sends it to the TE.

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.

13. The MT extracts the RAND and sends it to the SIM for key calculation.

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).

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. TE forwards the EAP success to the MT as a success indication

~~18~~19. After receiving the success indication, ~~T~~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, which will use them for other security purposes, for example WLAN link layer security.

6.7.3 Fast re-authentication with EAP AKA

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 13.

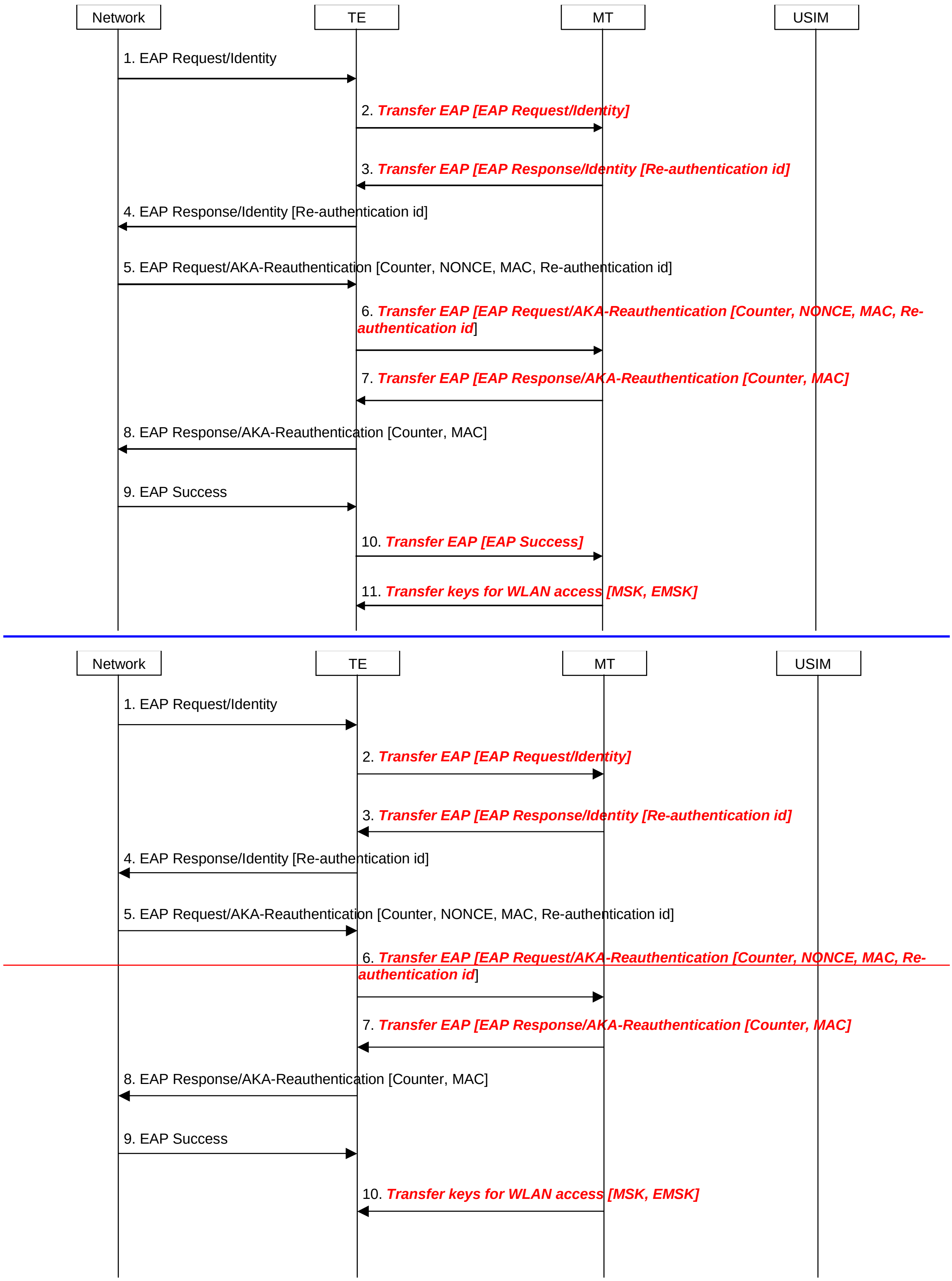

Network
TE
MT
USIM
1. EAP Request/Identity
2. Transfer EAP [EAP Request/Identity]
3. Transfer EAP [EAP Response/Identity [Re-authentication id]
4. EAP Response/Identity [Re-authentication id]
5. EAP Request/AKA-Reauthentication [Counter, NONCE, MAC, Re-authentication id]
6. Transfer EAP [EAP Request/AKA-Reauthentication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

Figure 13: Fast re-authentication with EAP AKA

1. The network sends a EAP request identity message.

2. 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.

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

6. The TE transfers the message to the MT with the parameters.

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 with the Counter received from the network.

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. TE forwards the EAP success to the MT as a success indication.

~~10~~11. After receiving the success indication, ~~T~~the MT sends the new calculated MSK and EMSK and sends them to the TE.

6.7.4 Fast re-authentication with EAP SIM

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 14.

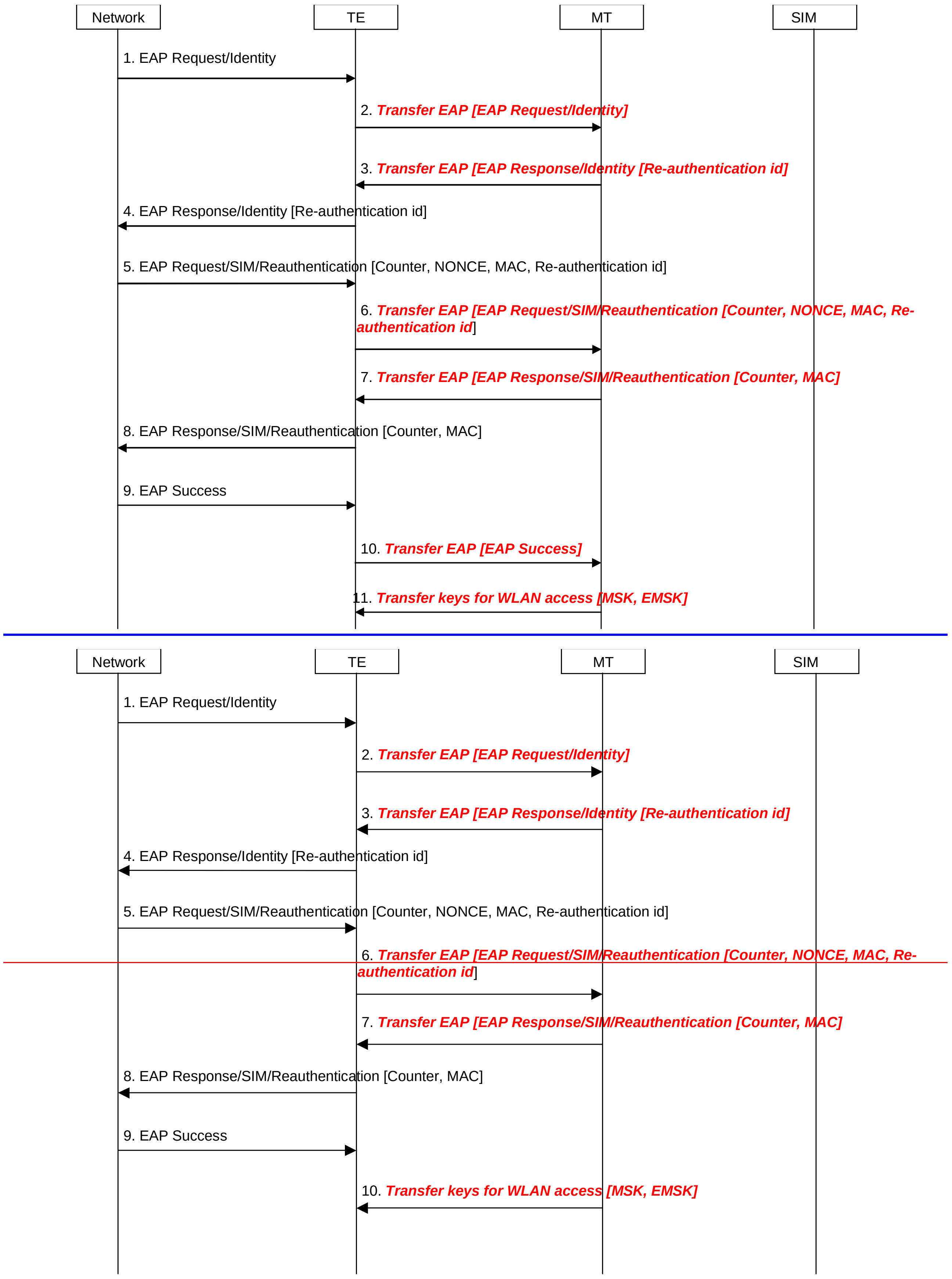

Network
TE
MT
SIM
1. EAP Request/Identity
2. Transfer EAP [EAP Request/Identity]
3. Transfer EAP [EAP Response/Identity [Re-authentication id]
4. EAP Response/Identity [Re-authentication id]
5. EAP Request/SIM/Reauthentication [Counter, NONCE, MAC, Re-authentication id]
6. Transfer EAP [EAP Request/SIM/Reauthentication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

Figure 14: Fast re-authentication with EAP SIM

1. The network sends a EAP request identity message.

2. 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.

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

6. The TE transfers the message to the MT with the parameters.

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 with the Counter received from the network.

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. TE forwards the EAP success to the MT as a success indication

~~10~~11. After receiving the success indication, ~~T~~the MT sends the new calculated MSK and EMSK and sends them to the TE.

3GPP TSG SA WG3 Security — S3#34 **S3-040668**
July 6 - 9, 2004, Acapulco, Mexico **Revised S3-040494**

CR-Form-v7

CHANGE REQUEST

⌘ **33.234 CR 015** ⌘**rev** **-** ⌘ Current version: **6.1.0** ⌘

*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:	⌘	Modification of mechanism to restrict simultaneous WLAN sessions
Source:	⌘	SA WG3
Work item code:	⌘	WLAN ***Date:*** ⌘ 07/07/2004
Category:	⌘	**C** ***Release:*** ⌘ Rel-6

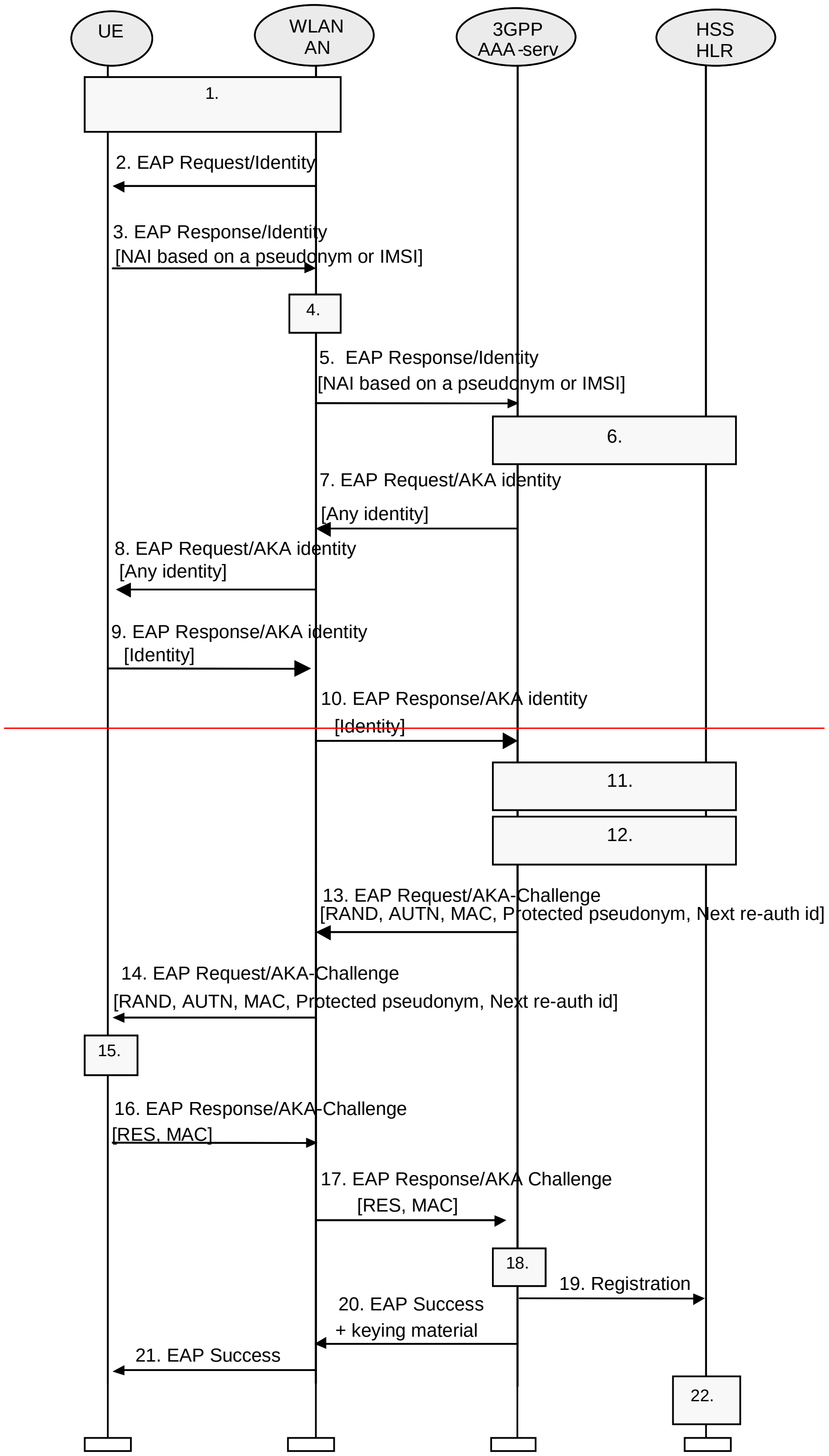
Use one of the following categories:	*Use one of the following releases:*
F *(correction)*	*2 (GSM Phase 2)*
A *(corresponds to a correction in an earlier release)*	*R96 (Release 1996)*
B *(addition of feature),*	*R97 (Release 1997)*
C *(functional modification of feature)*	*R98 (Release 1998)*
D *(editorial modification)*	*R99 (Release 1999)*
Detailed explanations of the above categories can	*Rel-4 (Release 4)*
be found in 3GPP TR 21.900.	*Rel-5 (Release 5)*
	Rel-6 (Release 6)

Reason for change:	⌘	The current TS included a restriction mechanismthat requests that the 3GPP AAA server should report to the HSS whenever multiple WLAN Access sessions are detected. To avoid load on the HSS/HLR, it is preferable for the 3GPP AAA server itself to terminate the old session.
Summary of change:	⌘	The below changes are added: 1. a mechanism to avoid the WLAN-UE connecting to multiple AAA servers in step 6 (6.1.1.1) and step 10 (6.1.2.1) 2. remove the step15 (6.1.1.1), step18 (6.1.2.1) and change the last steps, so that the AAA need not inform the HSS/HLR after it has detected multiple WLAN Access sessions, but instead the AAA teminates the unallowed multiple sessions by itself. 3. according to an SA2 decision, the term "scenario2" is replaced with the proper wording.
Consequences if not approved:	⌘	Unnecessary heavy burden to the HSS/HLR for 3GPP-WLAN interworking for WLAN Access Authentication. Obsoleted term used in the TS.

Clauses affected:	⌘	6.1.1.1, 6.1.2.1				
		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	23.234, 29.234
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

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]
14. EAP Request/AKA-Challenge
[RAND, AUTN, MAC, Protected pseudonym, Next re-auth id]
15.
16. EAP Response/AKA-Challenge
[RES, MAC]
17. EAP Response/AKA Challenge
[RES, MAC]
18.
19. Registration
20. EAP Success
+ keying material
21. EAP Success
22.

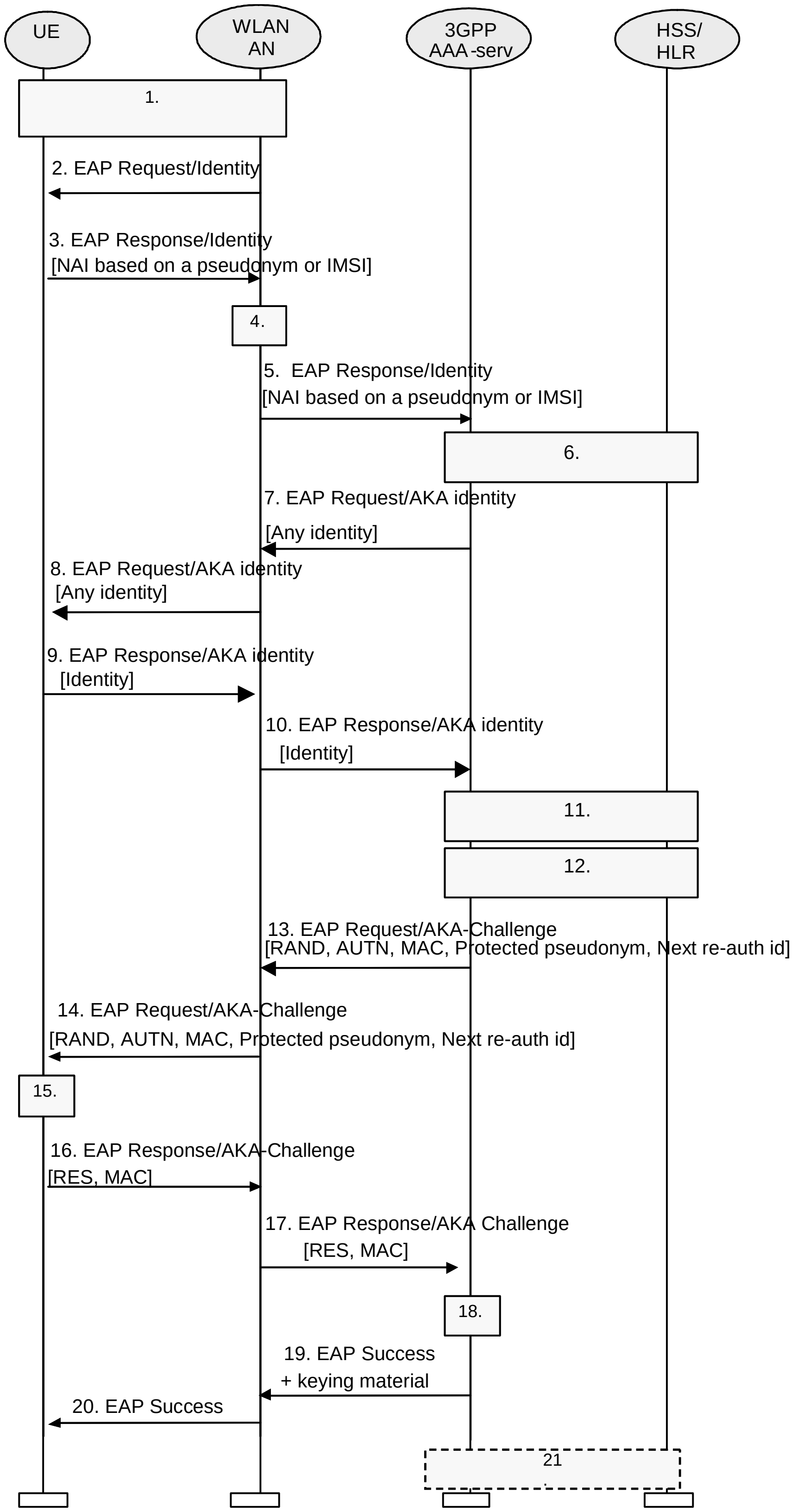

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity
[NAI based on a pseudonym or IMSI]
4.
5. EAP Response/Identity
[NAI based on a pseudonym or IMSI]
6.
7. EAP Request/AKA identity
[Any identity]
8. EAP Request/AKA identity
[Any identity]
9. EAP Response/AKA identity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

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 6shall 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.

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.

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.~~ 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~~19. If all checks in step 18 are successful, then the 3GPP AAA Server sends the EAP Success message to the WLAN-AN. 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.

~~21~~20. 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.

~~22~~21. 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 ~~the~~ with different radio network information that 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,~~ 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.

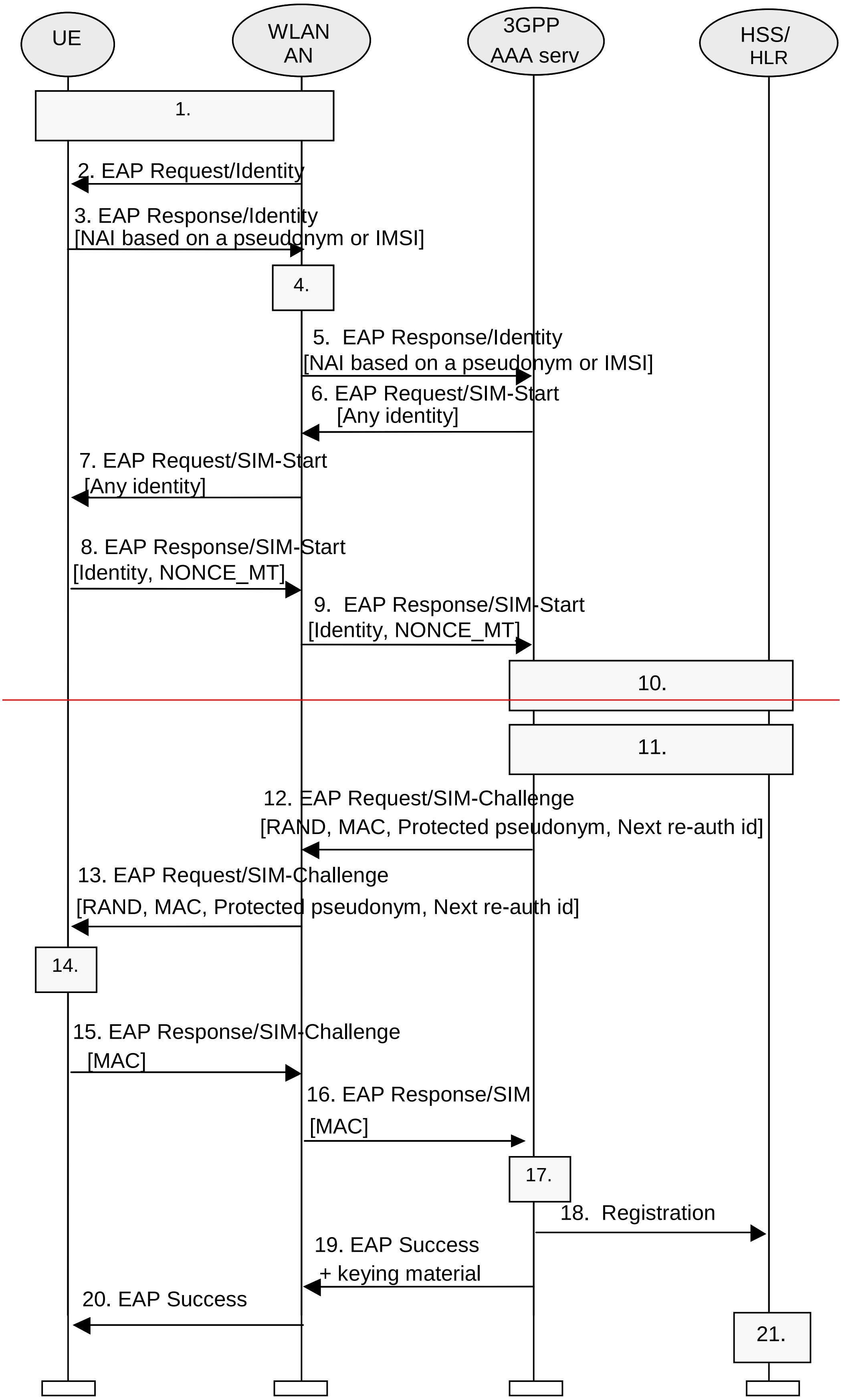
6.1.2 GSM SIM based WLAN Access authentication

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]
13. EAP Request/SIM-Challenge [RAND, MAC, Protected pseudonym, Next re-auth id]
14.
15. EAP Response/SIM-Challenge [MAC]
16. EAP Response/SIM [MAC]
17.
18. Registration
19. EAP Success + keying material
20. EAP Success
21.

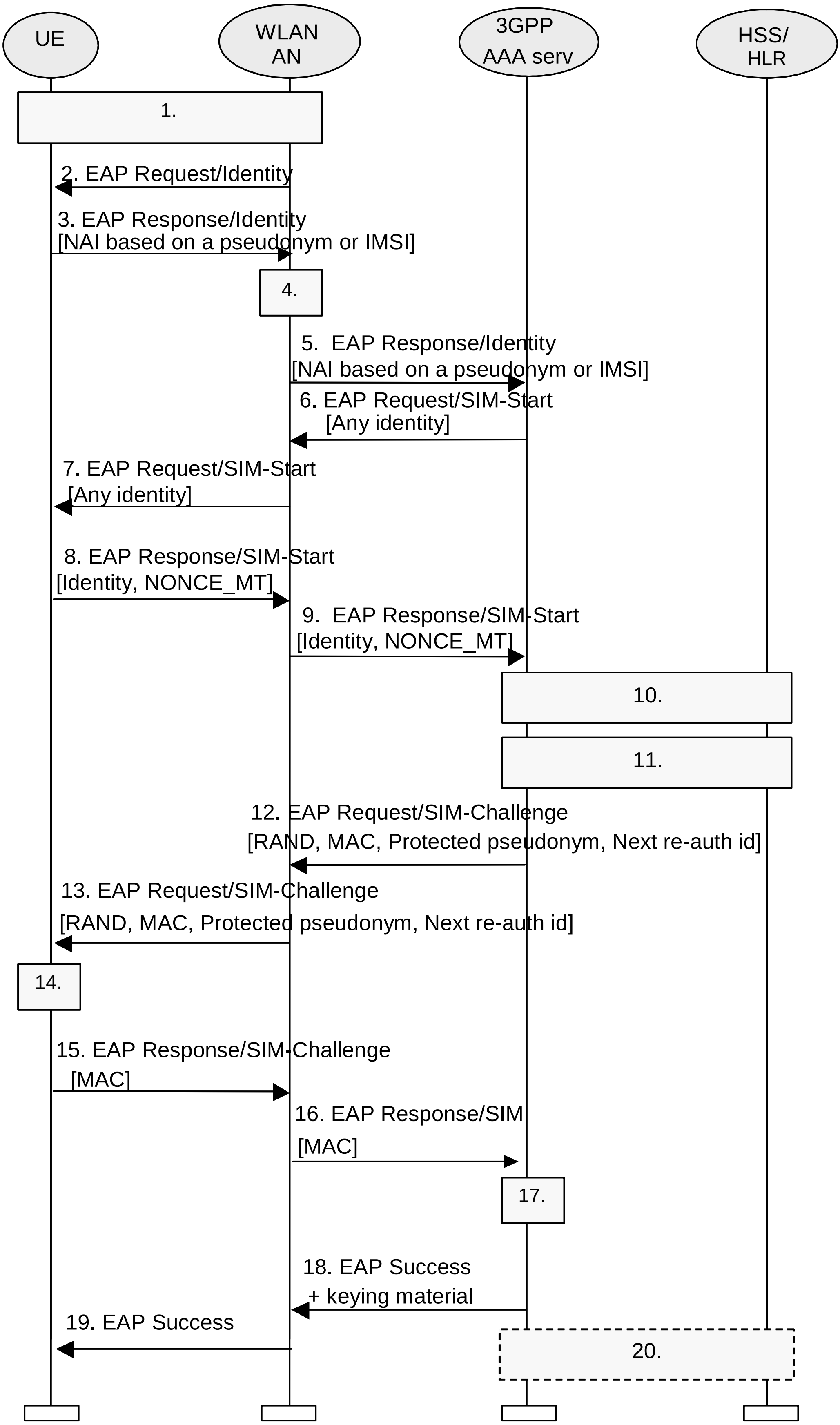

UE
WLAN AN
3GPP AAA serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity [NAI based on a pseudonym or IMSI]
4.
5. EAP Response/Identity [NAI based on a pseudonym or IMSI]
6. EAP Request/SIM-Start [Any identity]
7. EAP Request/SIM-Start [Any identity]
8. EAP Response/SIM-Start [Identity,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

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.

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.

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-UE's MAC address, the VPLMN Identity, as well as the identifier of the WLAN radio network used.~~

~~19~~18. If the comparison in step 17 is successful, then 3GPP AAA Server sends the EAP Success message to WLAN-AN. 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.

~~20~~19. 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.

~~21~~20. 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~~the~~ radio network information that 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,~~ , 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.

3GPP TSG SA WG3 Security — S3#34 **_Tdoc ⌘S3-040669_**
Acapulco, Mexico 6 - 9 July 2004

CR-Form-v7

CHANGE REQUEST

⌘	**33.234**	**CR**	**016**	⌘ **rev**	**-**	⌘	Current version:	**6.1.0** ⌘

*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:	⌘	Wa interface security		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	07/07/2004
Category:	⌘	**C**	***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:* *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:	⌘	Security of the Wa interface is not currently addressed in the specification.
Summary of change:	⌘	Removal of editor's note *"Threats on the Wa interface are not clear yet, so protection on this interface is for further study."* Specification of security mechanisms for the Wa interface.
Consequences if not approved:	⌘	The editor's note may indicate uncertainties in the security of the Wa interface. Lack of security specifications for the Wa interface may lead to insecure or incompatible implementations.

Clauses affected:	⌘	2, 4.2.2, 5.1.3				
		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] draft-ietf-eap-rfc2284bis-06.txt, October 2003: "PPP Extensible Authentication Protocol (EAP)".

[4] draft-arkko-pppext-eap-aka-11, October 2003: "EAP AKA Authentication".

[5] draft-haverinen-pppext-eap-sim-12, October 2003: "EAP SIM Authentication".

[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-03.txt, October 2003: "Diameter Extensible Authentication Protocol (EAP) Application".

[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-01.txt, November 2003: "EAP Key Management Framework".

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

[29] draft-ietf-ipsec-ikev2-13.txt, March 2004: "Internet Key Exchange (IKEv2) Protocol".

[30] RFC 2406, November 1998: "IP Encapsulating Security Payload (ESP)".

[31] draft-ietf-ipsec-ui-suites-05.txt, April 2004: "Cryptographic Suites for IPsec".

[32] draft-ietf-ipsec-udp-encaps-08.txt, February 2004: "UDP Encapsulation of IPsec Packets".

[33] draft-ietf-ipsec-ikev2-algorithms-04.txt, September 2003: "Cryptographic Algorithms for use in the Internet Key Exchange Version 2".

[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”

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

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.

Editors note: It is for further study if this is possible.

- 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.

~~Editor's note: Threats on the Wa interface are not clear yet, so protection on this interface is for further study.~~

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

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

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

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

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

*** END SET OF CHANGES ***

3GPP TSG SA WG3 Security — S3#34
Acapulco, Mexico 6 - 9 July 2004

Tdoc ⌘S3-040670

CHANGE REQUEST

⌘	**33.234**	**CR**	**017**	⌘	**rev**	**-**	⌘	Current version:	**6.1.0**	⌘

*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:	⌘	Introduction of protected result indications		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	07/07/2004
Category:	⌘	**F** *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.	***Release:*** ⌘	Rel-6 *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 latest versions of the internet drafts of EAP SIM and EAP AKA introduce the optional feature of protected success result indications. It allows the AAA server and the WLAN UE to negotiate the use of this feature, which consists of sending a protected EAP-Notification message previous to the EAP-Success message. The purpose of this CR is to introduce this feature in TS 33.234
Summary of change:	⌘	EAP SIM and EAP AKA flows for authentication and fast re-authentication are updated, introducing the optionality of the EAP-Notification message to protect EAP-Success message. An editor's note that questioned this feature is removed
Consequences if not approved:	⌘	TS 33.234 not consistent with EAP SIM and EAP AKA procedures

Clauses affected:	⌘	4.2.2, 6.1.1, 6.1.2 and 6.1.4				
		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	24.234
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

*** BEGIN SET OF CHANGES ***

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.

~~Editors note: It is for further study if this is possible.~~

- 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.

Editor's note: Threats on the Wa interface are not clear yet, so protection on this interface is for further study.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

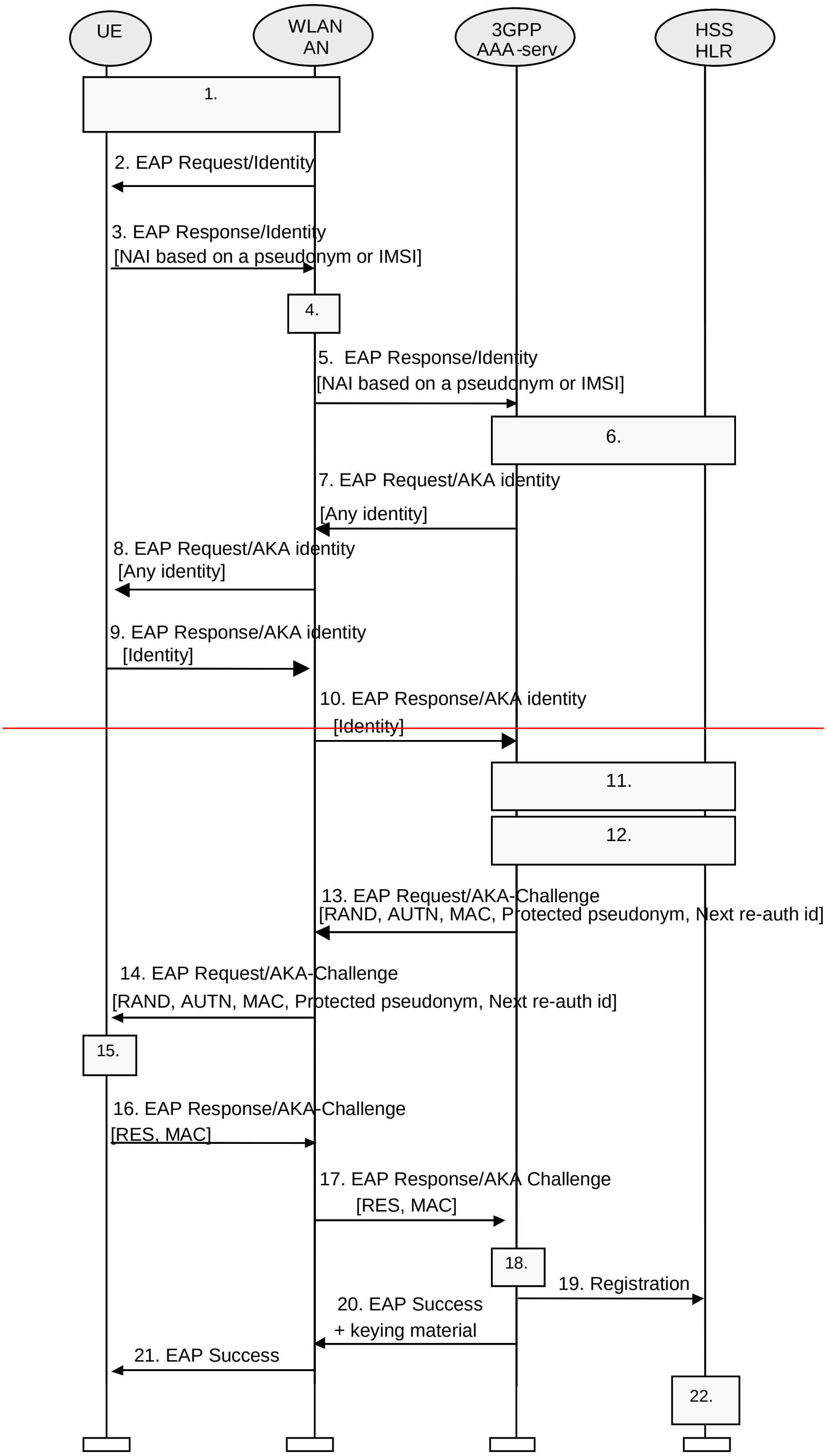
6.1.1 USIM-based WLAN Access Authentication

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

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]
14. EAP Request/AKA-Challenge
[RAND, AUTN, MAC, Protected pseudonym, Next re-auth id]
15.
16. EAP Response/AKA-Challenge
[RES, MAC]
17. EAP Response/AKA Challenge
[RES, MAC]
18.
19. Registration
20. EAP Success
+ keying material
21. EAP Success
22.

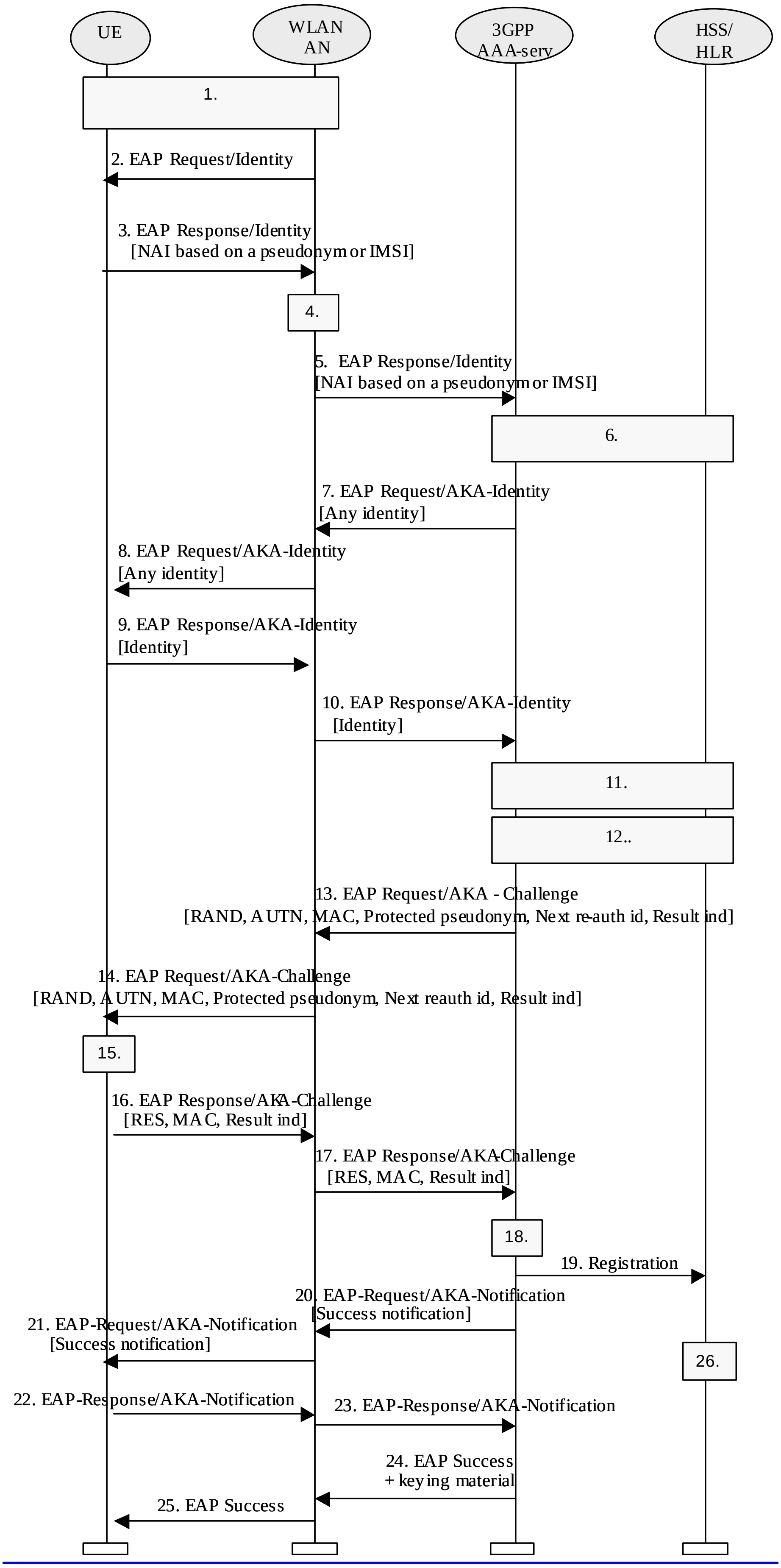

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity [NAI based on a pseudonym or IMSI]
4.
5. EAP Response/Identity [NAI based on a pseudonym or IMSI]
6.
7. EAP Request/AKA-Identity [Any identity]
8. EAP Request/AKA-Identity [Any identity]
9. EAP Response/AKA-Identity [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 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. 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

~~20~~24. ~~If all checks in step 18 are successful, then~~ 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.

~~21~~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.

~~22~~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.

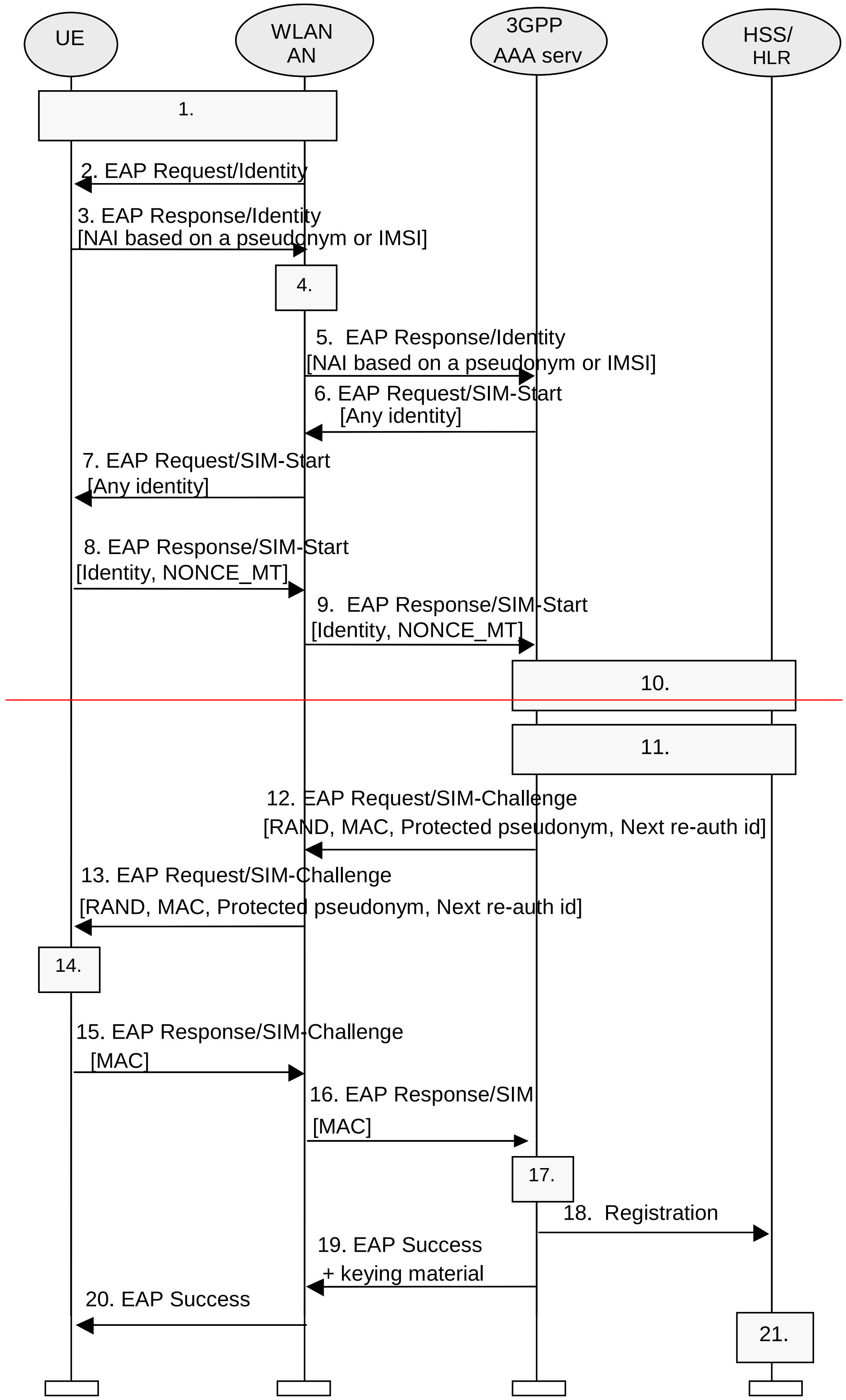
6.1.2 GSM SIM based WLAN Access authentication

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]
13. EAP Request/SIM-Challenge [RAND, MAC, Protected pseudonym, Next re-auth id]
14.
15. EAP Response/SIM-Challenge [MAC]
16. EAP Response/SIM [MAC]
17.
18. Registration
19. EAP Success + keying material
20. EAP Success
21.

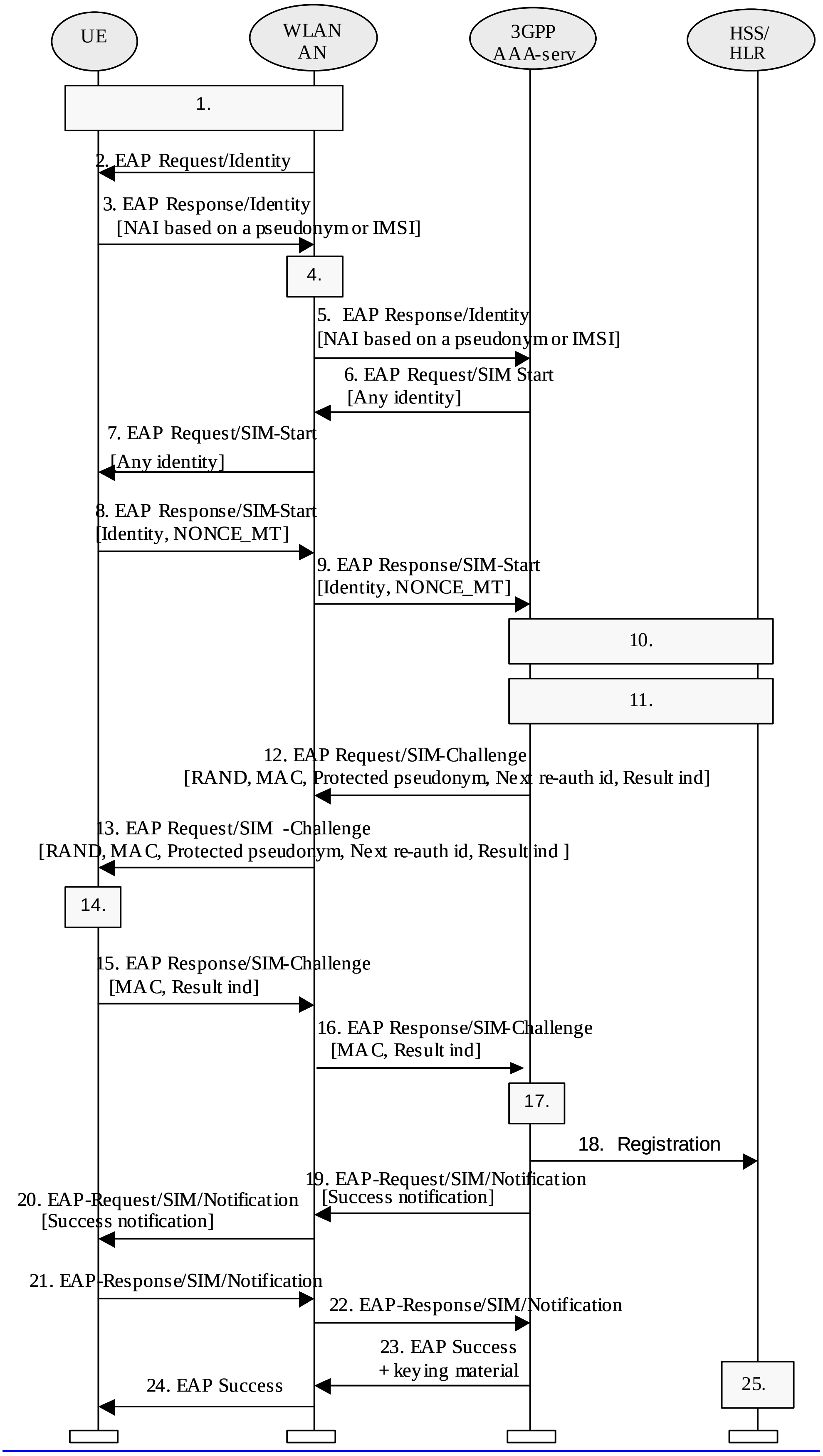

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity [NAI based on a pseudonym or IMSI]
4.
5. EAP Response/Identity [NAI based on a pseudonym or IMSI]
6. EAP Request/SIM Start [Any identity]
7. EAP Request/SIM-Start [Any identity]
8. EAP Response/SIM-Start [Identity, 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 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. 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-UE's 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

~~19~~23. ~~If the comparison in step 17 is successful, then~~ 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.

~~20~~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.

~~21~~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.

*** END SET OF CHANGES ***

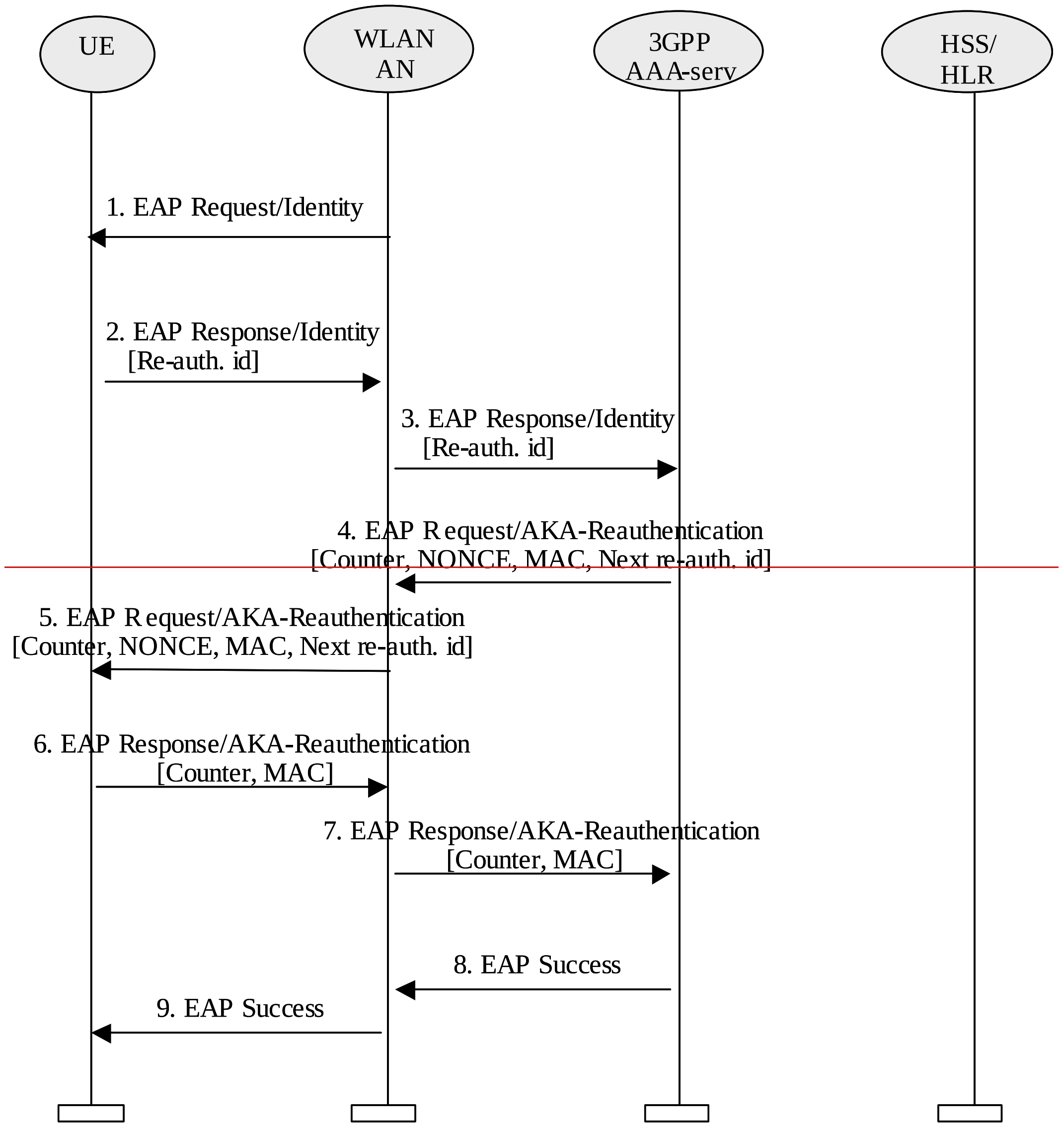
*** BEGIN SET OF CHANGES ***

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.

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, Next re-auth. id]
5. EAP R equest/AKA-Reauthentication [Counter, NONCE, MAC, Next re-auth. id]
6. EAP Response/AKA-Reauthentication [Counter, MAC]
7. EAP Response/AKA-Reauthentication [Counter, MAC]
8. EAP Success
9. EAP Success

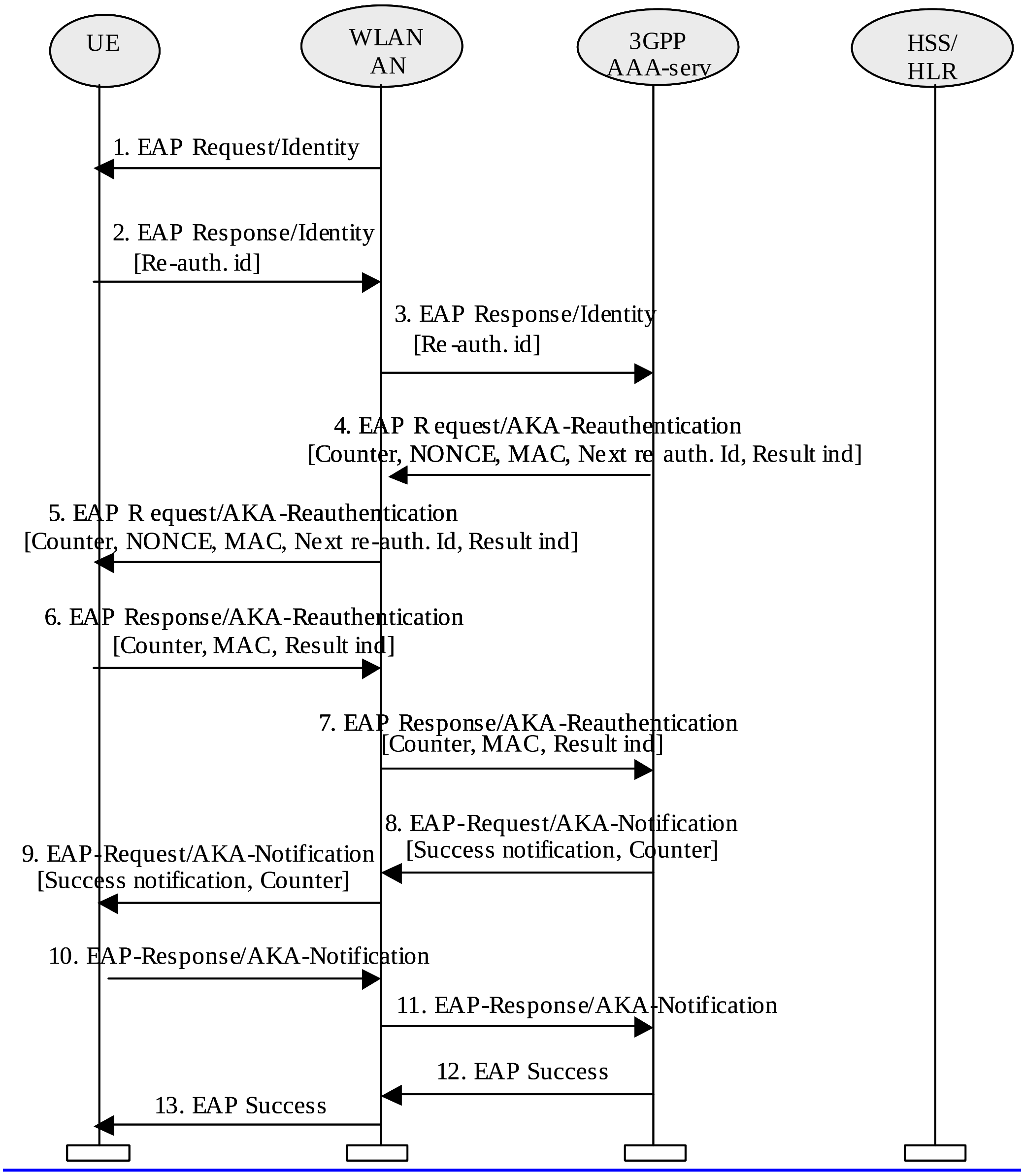

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1. EAP Request/Identity
2. EAP Response/Identity [Re-auth. id]
3. EAP Response/Identity [Re-auth. id]
4. EAP Request/AKA-Reauthentication [Counter, NONCE, MAC, Next re auth. Id, Result ind]
5. EAP Request/AKA-Reauthentication [Counter, NONCE, MAC, Next re-auth. Id, Result 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
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

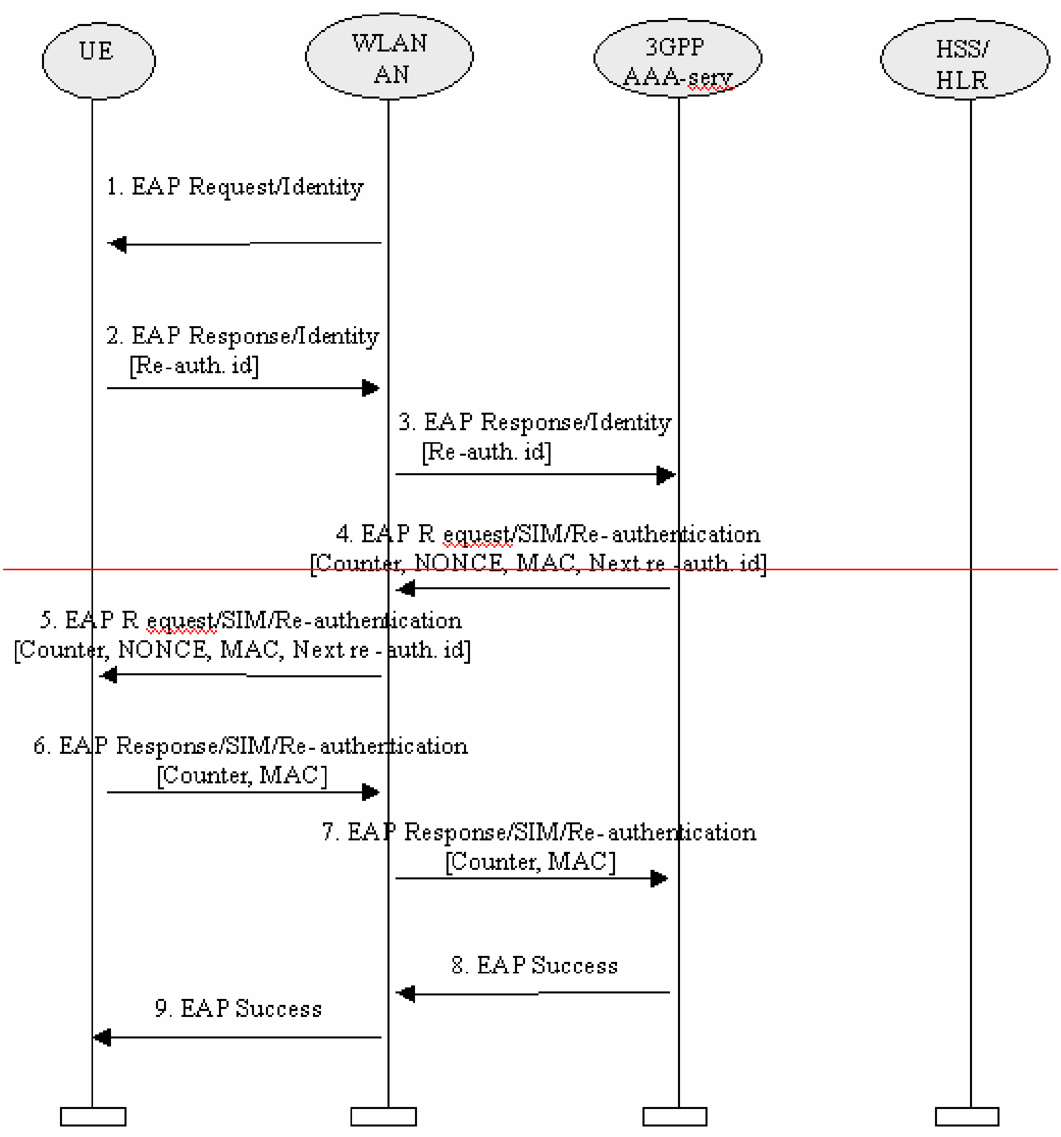
~~8~~12. The AAA server ~~verifies that the Counter value is the same as it sent, and the MAC is correct, and~~ sends an EAP Success message.

~~9~~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
HSS/ HLR
1. EAP Request/Identity
2. EAP Response/Identity [Re-auth. id]
3. EAP Response/Identity [Re -auth. id]
4. EAP R equest/SIM/Re-authentication [Counter, NONCE, MAC, Next re -auth. id]
5. EAP R equest/SIM/Re-authentication [Counter, NONCE, MAC, Next re - auth. id]
6. EAP Response/SIM/Re-authentication [Counter, MAC]
7. EAP Response/SIM/Re-authentication [Counter, MAC]
8. EAP Success
9. EAP Success

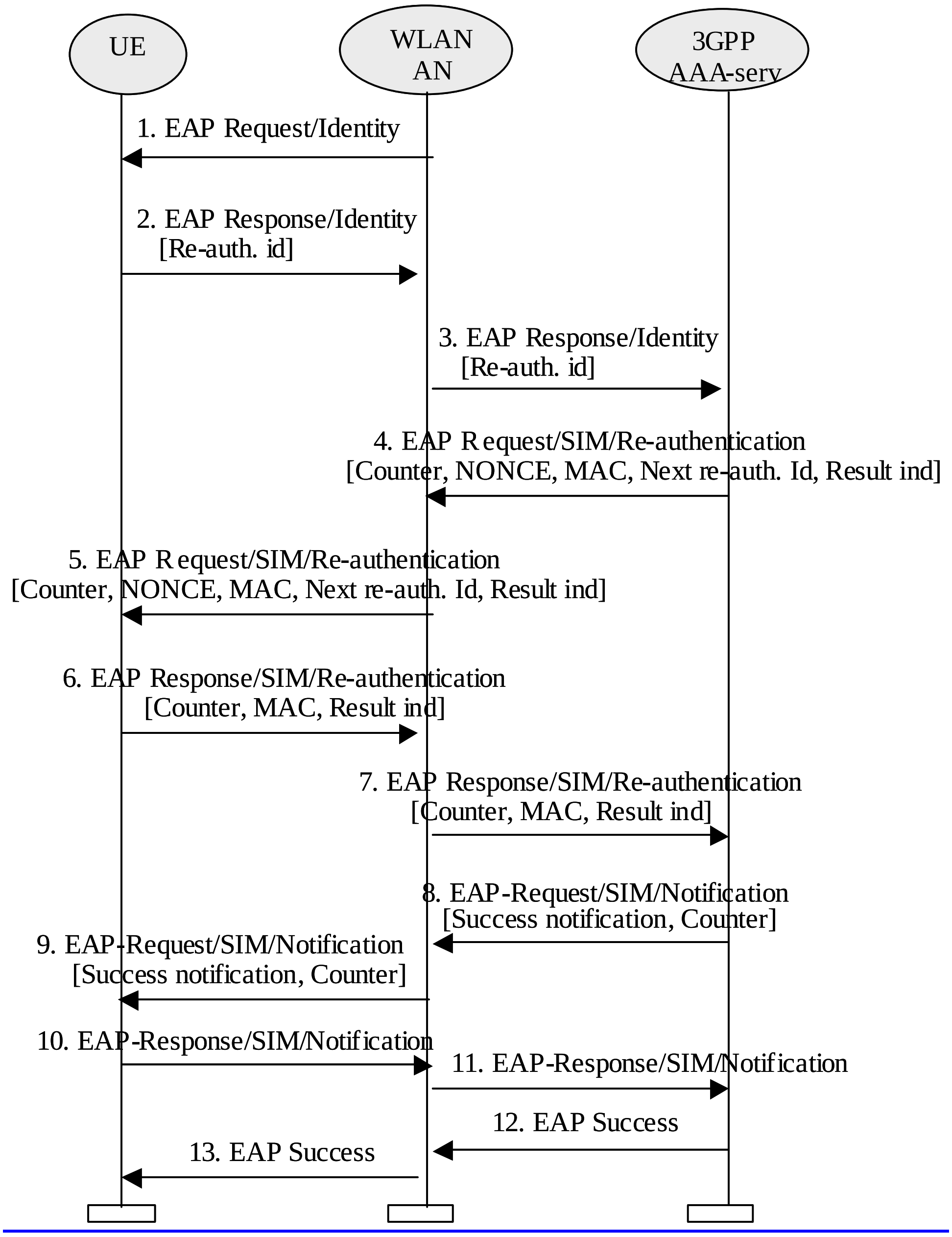

UE
WLAN AN
3GPP AAA-serv
1. EAP Request/Identity
2. EAP Response/Identity [Re-auth. id]
3. EAP Response/Identity [Re-auth. id]
4. EAP Request/SIM/Re-authentication [Counter, NONCE, MAC, Next re-auth. Id, Result ind]
5. EAP Request/SIM/Re-authentication [Counter, NONCE, MAC, Next re-auth. Id, Result ind]
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
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

~~8~~12. The AAA server ~~verifies that the Counter value is the same as it sent, and the MAC is correct, and~~ sends an EAP Success message.

~~9~~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 — S3#34 **Tdoc ⌘S3-040671**
Acapulco, Mexico 6 - 9 July 2004

CR-Form-v7

CHANGE REQUEST

⌘ **33.234 CR 018** ⌘ **rev -** ⌘ Current version: **6.1.0** ⌘

*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 authentication procedure in Wm interface		
Source:	⌘	SA WG3		
Work item code:	⌘	WLAN	***Date:*** ⌘	22/06/2004
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: ⌘ Wm interface (PDG-AAA server) authentication procedure is not yet defined. The purpose of this CR is to start with the definition of the interface for tunnel establishment purposes in WLAN 3GPP IP access.

Summary of change: ⌘ A new subchapter will be included specifying the procedures between the PDG and the AAA server, and how key derivation and delivery is performed in order to authenticate the tunnel in WLAN 3GPP IP access.

Consequences if not approved: ⌘ WLAN 3GPP IP access not possible to implement, tunnel authentication procedure not defined.

Clauses affected: ⌘ 6.1.5 and 2

Other specs affected: ⌘

Y	N		
X		Other core specifications	⌘ 29.234, 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] draft-ietf-eap-rfc2284bis-06.txt, October 2003: "PPP Extensible Authentication Protocol (EAP)".

[4] draft-arkko-pppext-eap-aka-11, October 2003: "EAP AKA Authentication".

[5] draft-haverinen-pppext-eap-sim-~~12~~13, ~~October~~ April ~~2003~~2004: "EAP SIM Authentication".

[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-03.txt, October 2003: "Diameter Extensible Authentication Protocol (EAP) Application".

[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-01.txt, November 2003: "EAP Key Management Framework".

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

[29] draft-ietf-ipsec-ikev2-~~12~~14.txt, ~~January~~ May 2004, “Internet Key Exchange (IKEv2) Protocol”

[30] RFC 2406, November 1998, “IP Encapsulating Security Payload (ESP)”

[31] draft-ietf-ipsec-ui-suites-04.txt, August 2003, “Cryptographic Suites for IPsec”

[32] draft-mariblanca-aaa-eap-lla-01.txt, June 2004, "EAP lower layer attributes for AAA protocols".

[33] 3GPP TS23.234;” 3GPP system to Wireless Local Area Network (WLAN) interworking”

*** END SET OF CHANGES ***

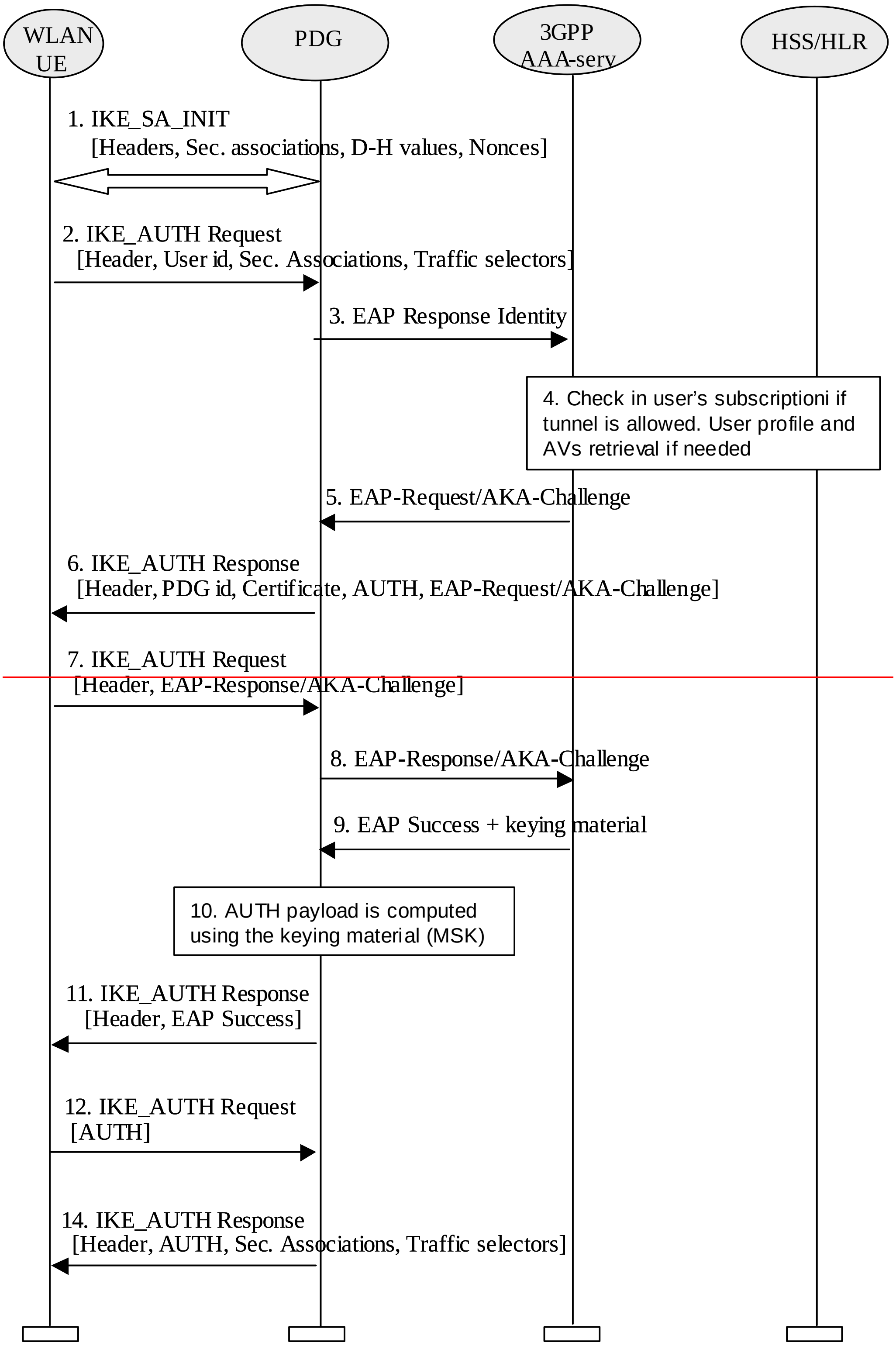
*** BEGIN SET OF CHANGES ***

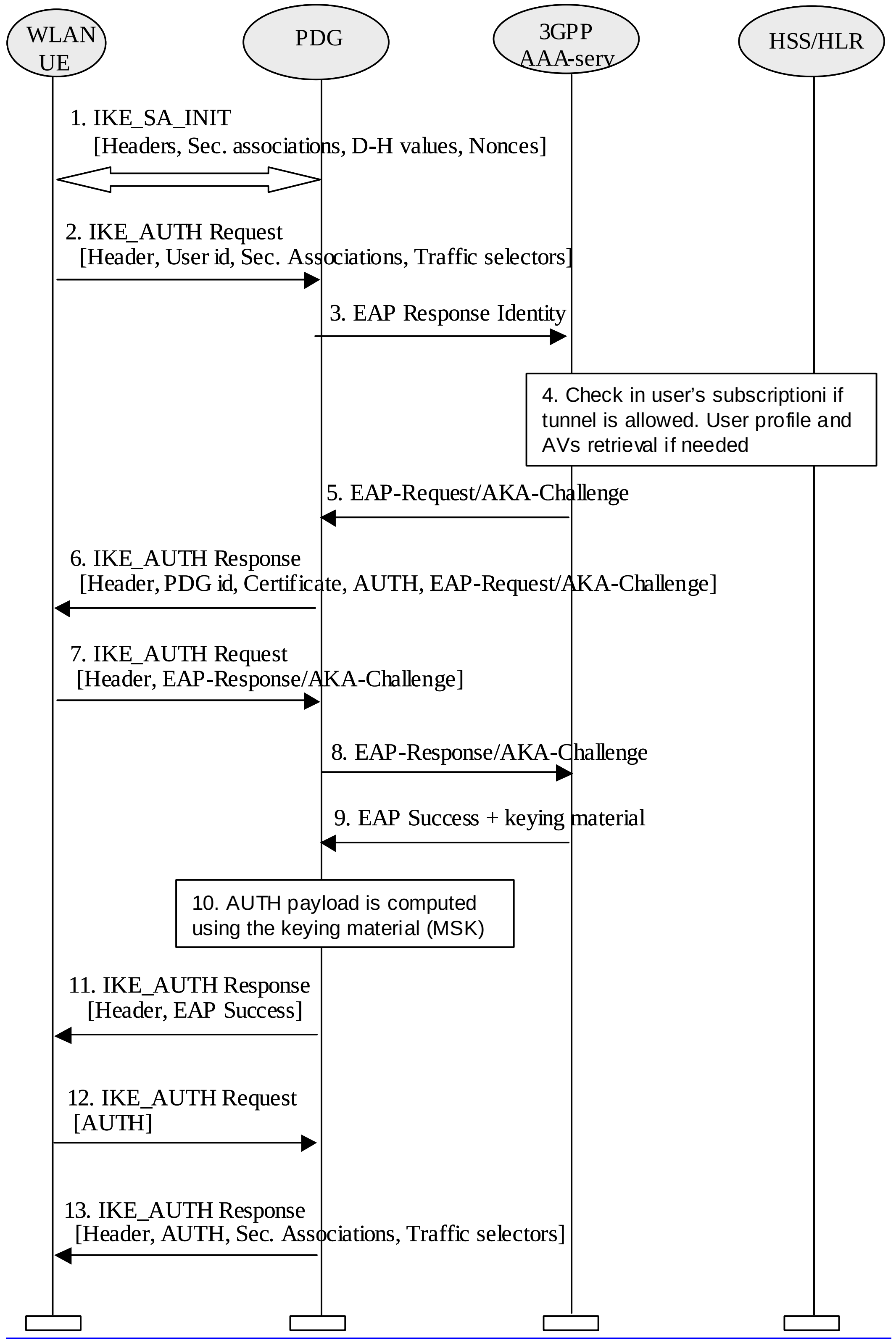
6.1.5.1 Tunnel full authentication and authorization

The tunnel end point in the network is the PDG. 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 user's 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]
14. 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. EAP Response Identity
4. Check in user's 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 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: (1)-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 ref. [33] section 5.3.4) (2) W-APN should be sent in this step, because in [33], 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 user's 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

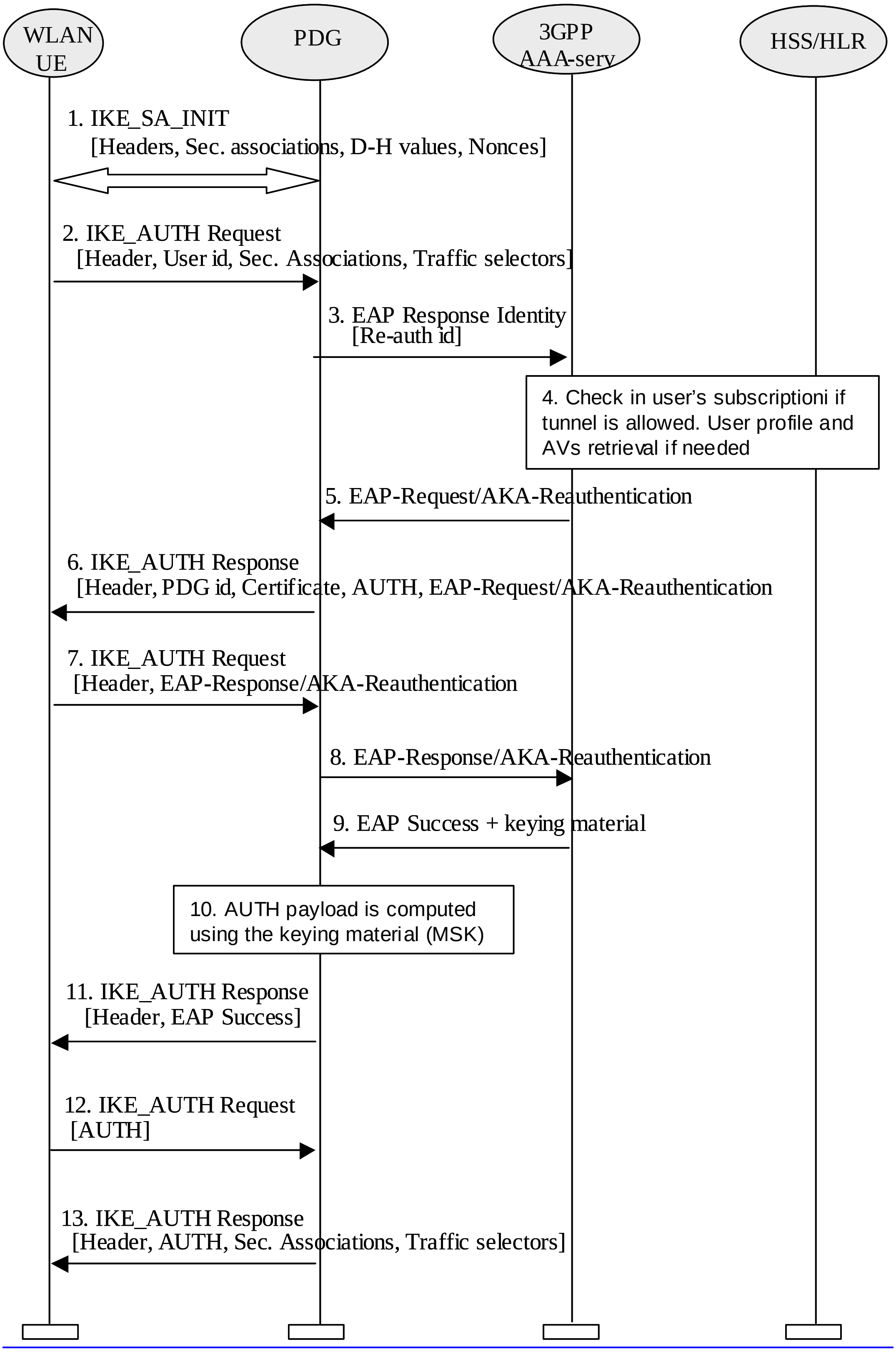
12.The WLAN UE shall take its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the PDG

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 user's 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 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 user's 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 ***