3GPP TSG-SA3 Meeting #28
Berlin, Germany, 5th-9th May, 2003

Tdoc ⌘S3-030259

CR-Form-v7

CHANGE REQUEST

⌘ **33.234 CR CRNum** ⌘**rev** **-** ⌘ Current version: **0.4.0** ⌘

*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:	⌘	Editorial changes to section 6.1 - AKA			
Source:	⌘	Ericsson			
Work item code:	⌘	WLAN	***Date:***	⌘	20/02/2003
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:	⌘	Clean up the text
Summary of change:	⌘	
Consequences if not approved:	⌘	

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

6.1 Authentication and key agreement

[Editor's note: This section shall describe in detail how the authentication is performed and how the keys are derived and delivered to the different nodes.]

[Editor's note: The content of this section is directly copied from TS 23.xxx v0.1.0 and shall be reviewed by SA3]

6.1.1 USIM-based 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.

~~However, requiring USIM based authentication does not automatically mean that the USIM needs to be included in the WLAN card, for example the WLAN device can be linked with a WLAN-UE supporting a USIM via, for example Bluetooth, Irda, USB or serial cable.~~

6.1.1.1 EAP/AKA Procedure

~~USIM based authentication may be based on existing AKA method. In the case of WLAN-3GPP system interworking, this method should be supported by a generic authentication mechanism (independently of the underlying WLAN standard), e.g. EAP. EAP/AKA authentication mechanism is described in Internet Draft draft-arkko-pppext-eap-aka (ref. [4]). The following procedure is based on EAP/AKA authentication mechanism:~~

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.

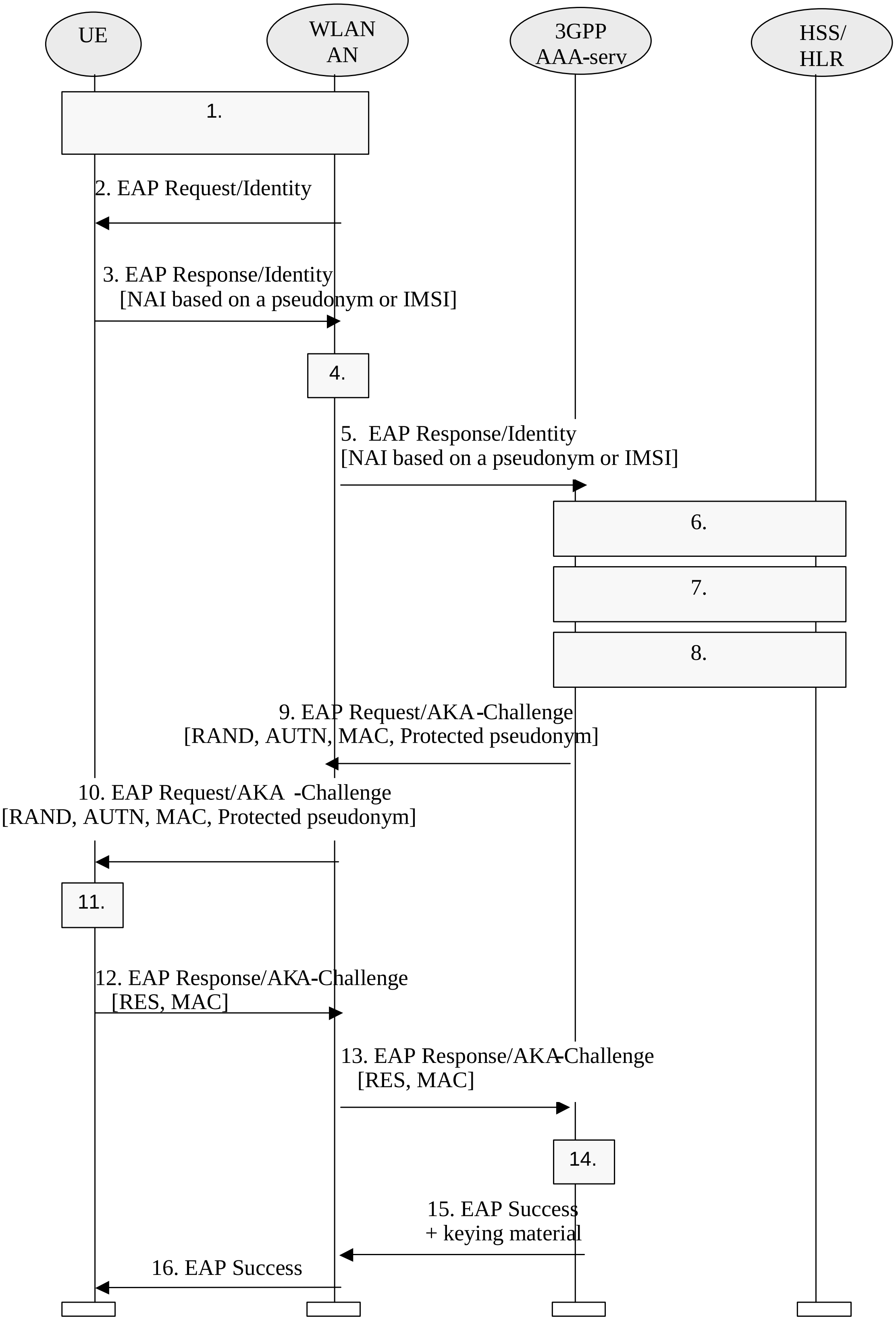

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity
[NAI based on a pseudonym or IMSI]
4.
5. EAP Response/Identity
[NAI based on a pseudonym or IMSI]
6.
7.
8.
9. EAP Request/AKA-Challenge
[RAND, AUTN, MAC, Protected pseudonym]
10. EAP Request/AKA -Challenge
[RAND, AUTN,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

Figure 7.1 Authentication based on EAP AKA scheme

1. ~~After WLAN connection establishment, Extensible Authentication Protocol is started with~~A connection is established between the WLAN-UE and the WLAN-AN, using a Wireless LAN technology specific procedure (out of scope for ~~3GPP~~this specification).

2. The ~~WLAN~~ 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 ~~starts EAP AKA authentication procedure by sending~~sends an EAP Response/Identity message. The WLAN-UE sends its identity complying ~~to~~ with 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 : generating an identity conforming to NAI format from IMSI is defined in EAP/AKA [4]

4. ~~The 3GPP AAA Server is chosen based on the NAI~~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 : ~~diameter/radius proxy chaining and/or~~ Ddiameter 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.

6. ~~6.~~ The 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: 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. 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.)

8. New keying material is derived from IK and CK., cf. [4]. This~~e~~ ~~extra~~ keying material is required by EAP-AKA, and some extra keying material ~~in order to pass the encrypted and integrity protected temporary identifier to the WLAN-UE. The keying material~~ may also be ~~used~~ generated for WLAN technology specific confidentiality and/or integrity protection.

A new pseudonym ~~is~~ may be chosen and ~~encrypted~~protected (i.e. encrypted and integrity protected) using EAP-AKA generated keying material.

9. 3GPP AAA Server sends RAND, AUTN, a message authentication code (MAC) and ~~encrypted temporary identifier~~ protected pseudonym (in case it was generated) to ~~WLAN~~ WLAN-AN in EAP Request/AKA-Challenge message.

10. The ~~WLAN~~ WLAN-AN sends the EAP Request/AKA-Challenge message to the WLAN-UE.

11. 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,cf [4]. If AUTN is correct, the USIM computes RES, IK and CK.

Using IK and CK, the WLAN-UE checks the received MAC and derives required additional keying material~~ from IK and CK~~.

If a protected pseudonym was received, then the WLAN-UE ~~-~~stores the pseudonym for future authentications.

12. WLAN-UE sends EAP Response/AKA-Challenge containing calculated RES and a new MAC value to ~~WLAN~~WLAN-AN.

13. ~~WLAN~~ WLAN-AN sends the EAP Response/AKA-Challenge packet to 3GPP AAA Server

14. 3GPP AAA Server checks the received MAC and compares XRES ~~and~~ to the received RES.

15. If ~~the comparison~~all checks in step 14 ~~is~~ are successful, then 3GPP AAA Server sends the EAP Success message to ~~WLAN~~WLAN-AN. If some extra keying material was generated for WLAN technology specific confidentiality and/or integrity protection, ~~The~~ then the 3GPP AAA Server includes ~~the~~ this ~~derived~~ keying material in the underlying AAA protocol message (i.e. not at EAP level). The ~~WLAN~~ WLAN-AN stores the keying material to be used in communication with the authenticated WLAN-UE.

16. ~~WLAN~~ 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~~ WLAN-AN may share ~~session~~ keying material derived during that exchange.

~~Note 1: The 3GPP AAA Server performs the authentication. AAA Proxies may be used between the WLAN Access Network and the AAA Server, but they are shown in the diagram.~~

6.1.2 GSM SIM based 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.

~~The SIM does not necessarily have to be included in the WLAN card, for example the WLAN device can be linked with a UE supporting a SIM via, for example Bluetooth, Irda, USB or serial cable.~~

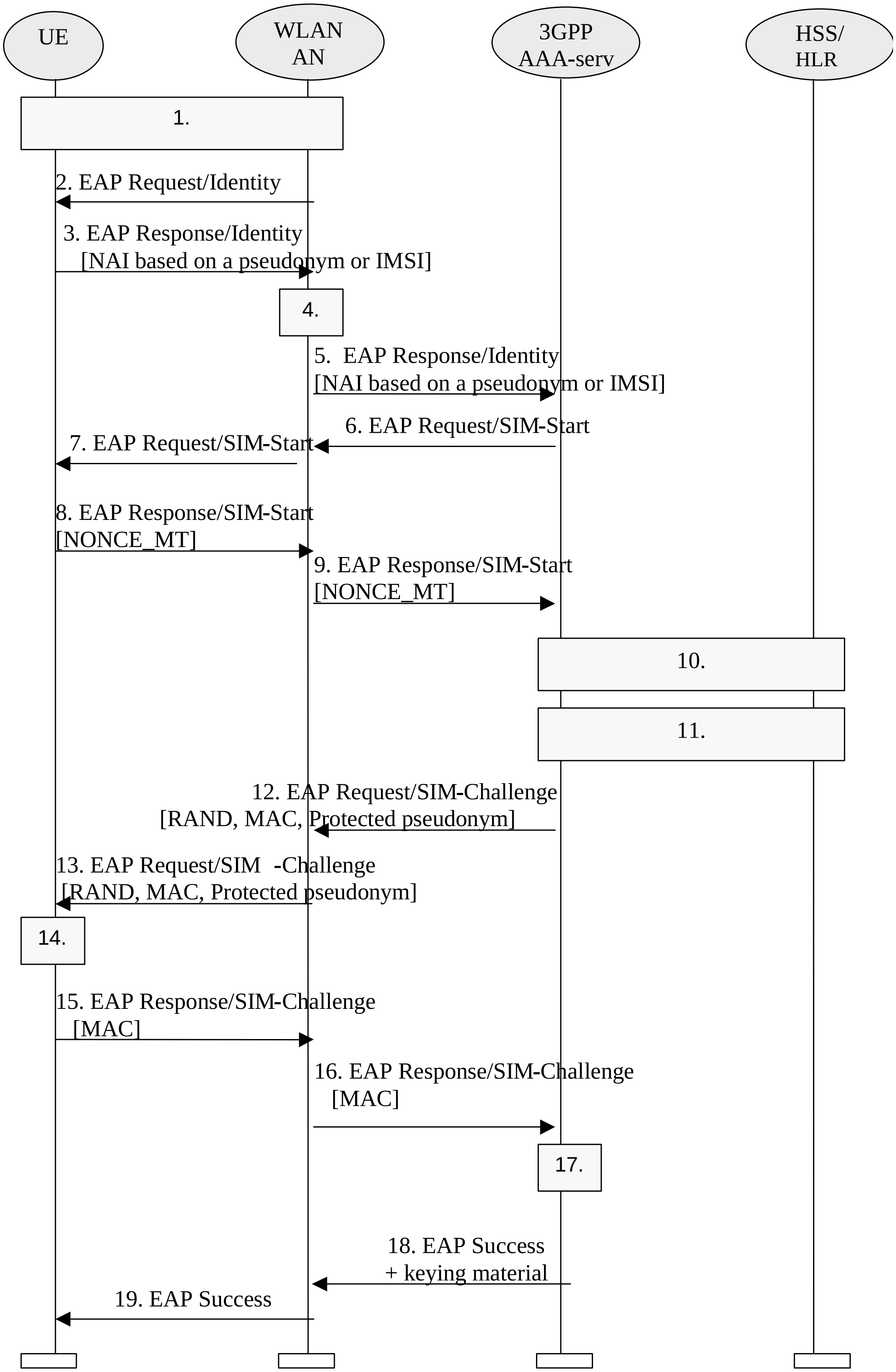
~~*[Editor's note: also see section 4.2.3 on WLAN UE split]*~~

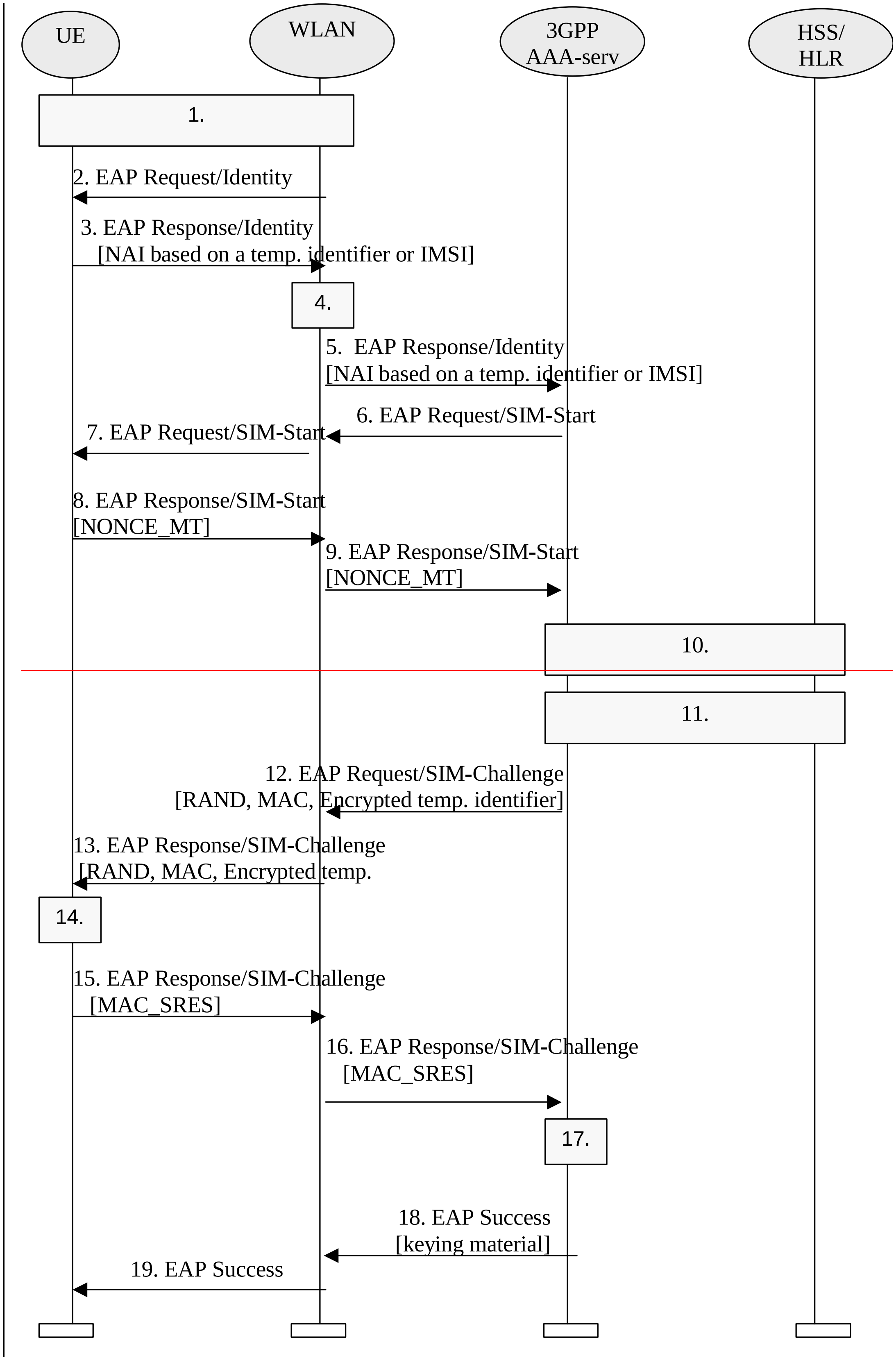
6.1.2.1 EAP SIM procedure

~~SIM based authentication (i.e. when no USIM is available) shall be based on [5]. The enhancements for network authentication shall be used..~~

~~The following procedure is based on EAP SIM authentication mechanism:~~

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
7. EAP Request/SIM-Start
8. EAP Response/SIM-Start [NONCE_MT]
9. EAP Response/SIM-Start [NONCE_MT]
10.
11.
12. EAP Request/SIM-Challenge [RAND, MAC, Protected pseudonym]
13. EAP Request/SIM -Challenge [RAND, MAC, Protected pseudonym]
14.
15. EAP Response/SIM-Challenge [MAC]
16. EAP Response/SIM-Challenge [MAC]
17.
18. EAP Success + keying material
19. EAP Success


UE
WLAN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity [NAI based on a temp. identifier or IMSI]
4.
5. EAP Response/Identity [NAI based on a temp. identifier or IMSI]
6. EAP Request/SIM-Start
7. EAP Request/SIM-Start
8. EAP Response/SIM-Start [NONCE_MT]
9. EAP Response/SIM-Start [NONCE_MT]
10.
11.
12. EAP Request/SIM-Challenge [RAND, MAC, Encrypted temp. identifier]
13. EAP Response/SIM-Challenge [RAND, MAC, Encrypted temp.
14.
15. EAP Response/SIM-Challenge [MAC_SRES]
16. EAP Response/SIM-Challenge [MAC_SRES]
17.
18. EAP Success [keying material]
19. EAP Success

7.2 Authentication based on EAP SIM scheme

1. A connection is established between the WLAN-UE and the WLAN-AN, using ~~After WLAN connection establishment, Extensible Authentication Protocol is started with~~ a Wireless LAN technology specific procedure (out of scope for this specification).

2. The ~~WLAN~~ 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 ~~starts EAP SIM authentication procedure by sending~~ an EAP Response/Identity message. The WLAN-UE sends its identity complying ~~to~~ with 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 : generating an identity conforming to NAI format from IMSI is defined in EAP/SIM ~~(draft-haverinen-pppext-eap-sim-04.txt)~~[5].

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).~~The 3GPP AAA Server is chosen based on the NAI.~~

Note : ~~diameter/radius proxy chaining and/or d~~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.

6. ~~6.~~ The 3GPP AAA Server identifies the subscriber as a candidate for authentication with EAP-SIM, based on the received identity, ~~based on the NAI,~~ and then it sends the EAP Request/SIM-Start packet to ~~WLAN~~WLAN-AN.

Note: 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~~ 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 sends the EAP Response/SIM-Start packet, containing NONCE_MT, to ~~WLAN~~WLAN-AN

9. ~~WLAN~~ WLAN-AN sends the EAP Response/SIM-Start packet to 3GPP AAA Server

10. The AAA server checks that it has ~~N~~ available N unused ~~triplets~~ authentication vectors for the subscriber. Several ~~triplets~~ GSM authentication vectors are required in order to generate ~~longer session keys~~keying material with effective length equivalent to EAP-AKA. If N authentication vectors ~~triplets~~ are not available, a set of authentication ~~triplets~~ 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~~e~~ ~~extra~~ keying material is required ~~in order to calculate a network authentication value and to pass the encrypted and integrity protected temporary identifier to the WLAN-UE. The~~by EAP-SIM, and some extra keying material may also be ~~used~~ 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-SIM generated keying material.

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

~~A new temporary identifier is chosen and encrypted.~~

3GPP AAA Server sends RAND, MAC, and protected pseudonym (in case it was generated)~~encrypted temporary identifier~~ to ~~WLAN~~ WLAN-AN in EAP Request/SIM-Challenge message.

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

14. WLAN-UE runs N times the GSM A3/A8 algorithms in the SIM~~N times~~, 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 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.

WLAN-UE calculates a new MAC covering the EAP message concatenated to ~~a combined response value MAC_SRES from~~ 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~~_SRES~~ to ~~WLAN~~WLAN-AN.

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

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

18. ~~18.~~ If the comparison in step 17 is successful, then 3GPP AAA Server sends the EAP Success message to ~~WLAN~~WLAN-AN. If some extra keying material was generated for WLAN technology specific confidentiality and/or integrity protection, then the ~~The~~ 3GPP AAA Server includes ~~the~~ this derived keying material in the underlying AAA protocol message (i.e. not at EAP level). The ~~WLAN~~ WLAN-AN stores the keying material to be used in communication with the authenticated WLAN-UE.

19. ~~WLAN~~ 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~~ WLAN-AN may share ~~session~~ keying material derived during that exchange.

~~Note 1: The 3GPP AAA Server that is referred to in this diagram is the one that actually realises the authentication. If AAA Proxies are used between the WLAN Access Network and the AAA Server, they are not referred to in this diagram.~~

Note~~ 2~~: the derivation of the value of N is for further study