CR-Form-v7.1

CHANGE REQUEST

| ⌘ | **33.234 CR 023** | ⌘**rev** | **-** | ⌘ | Current version: | **6.2.0** | ⌘ |

*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 **X** Radio Access Network ☐ Core Network **X**

Title: ⌘	Clarification on the use of MAC addresses	
Source: ⌘	Ericsson	
Work item code: ⌘	WLAN	***Date:*** ⌘ 28/09/2004

Category: ⌘ **F**		***Release:*** ⌘ Rel-6	
	Use one of the following categories:	*Use one of the following releases:*	
	F (correction)	*Ph2 (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 be found in 3GPP TR 21.900.	*Rel-4 (Release 4)*	
		Rel-5 (Release 5)	
		Rel-6 (Release 6)	
		Rel-7 (Release 7)	

Reason for change: ⌘	Ericsson has submitted a discussion paper in which the use of the MAC address of a device to control simultaneous sessions is questioned. This CR introduces the necessary changes in TS 33.234 according to the conclusions of the discussion paper. Basically, the conclusions is that the AAA server can trust in the MAC address only in one situation in scenario 2: when the MAC addresses if in the authentication requests are being received from the same WLAN access network. In scenario 3, the MAC address cannot be trusted and hence it doesn't help to detect simultaneous accesses.
Summary of change: ⌘	Removal of MAC address and clarification of its use in different chapters. A new chapter is created in order to clarify the use of the MAC address.
Consequences if not approved: ⌘	Trusting in the MAC addresses may make the AAA server believe that there are no simultaneous sessions while in reality there are.

Clauses affected: ⌘	6.1.1, 6.1.2

	Y	N		
Other specs affected: ⌘	X		Other core specifications ⌘	24.234, 29.234
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘	

*** BEGIN SET OF CHANGES ***

5.7 Simultaneous access control

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

This control is cannot be performed in some situations. For example, if the two devices are accessing two different WLAN access points, the MAC address of one of them can be spoofed to be made equal to the other one. The situation, which can be controlled by means of the use of MAC addresses, is when two devices are accessing the same WLAN point. In that case, as the MAC addresses cannot be spoofed to be equal, the AAA server can detect if subsequent authentication requests, on behalf of the same user, are being performed with different MAC addresses. Then the AAA server can decide to reject the authentication requests.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

6.1.1 USIM-based WLAN Access Authentication

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

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

6.1.1.1 EAP-AKA Procedure

The EAP-AKA authentication mechanism is specified in ref. [4]. The present section describes how this mechanism is used in the WLAN-3GPP interworking scenario.
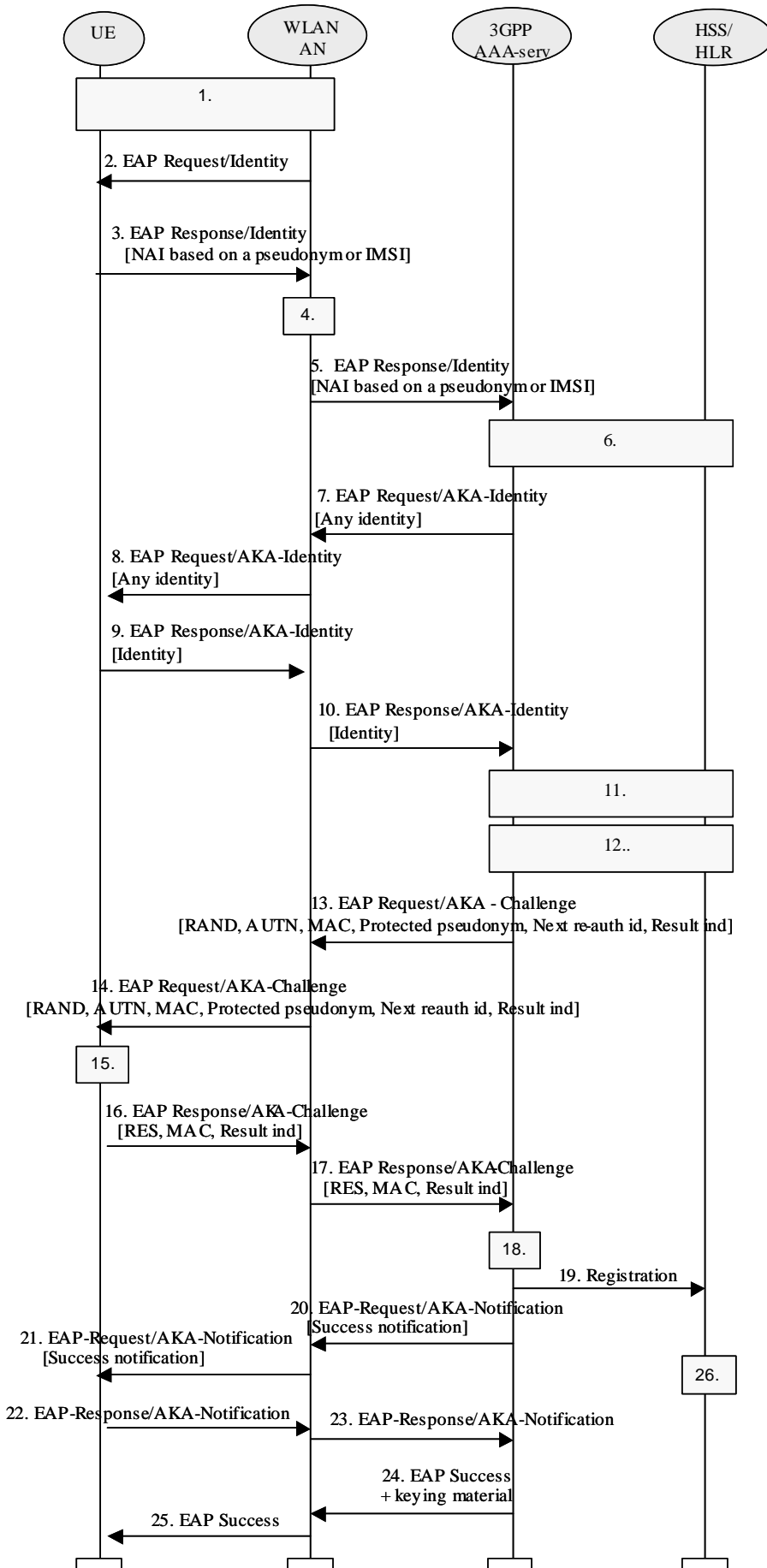
```
     ┌────────┐      ┌────────┐      ┌────────┐      ┌────────┐
     │   UE   │      │  WLAN  │      │  3GPP  │      │  HSS/  │
     │        │      │   AN   │      │AAA-serv│      │  HLR   │
     └────────┘      └────────┘      └────────┘      └────────┘
```

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).

    The MAC address shall be checked only if the WLAN radio network information is the same as the ongoing sessions. If not, the MAC address cannot be considered trusted and no action is taken (skip step 19).

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

20. If all checks in step 18 are successful, the 3GPP AAA Server shall send the message EAP Request/AKA-Notification, previous to the EAP Success message, if the 3GPP AAA Server requested previously to use protected successful result indications. This message is MAC protected.

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

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

23. The WLAN AN forwards the EAP Response/AKA-Notification message to the 3GPP AAA server. The 3GPP AAA Server shall ignore the contents of this message

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

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

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

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

6.1.2   GSM SIM based WLAN Access authentication

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

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

6.1.2.1 EAP SIM procedure

The EAP-SIM authentication mechanism is specified in ref. [5]. The present section describes how this mechanism is used in the WLAN-3GPP interworking scenario.
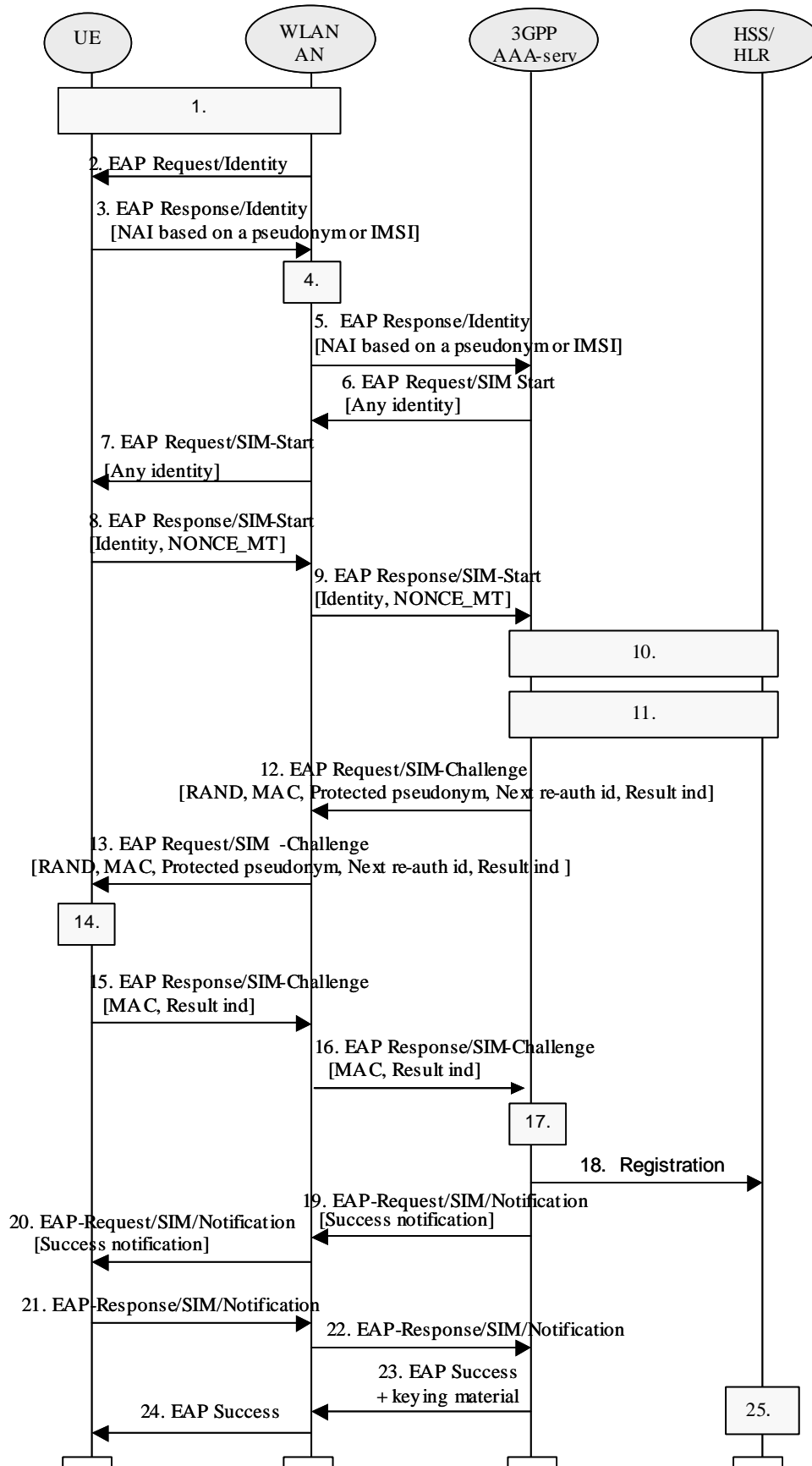
UE   WLAN AN   3GPP AAA-serv   HSS/HLR

1.

2. EAP Request/Identity

3. EAP Response/Identity
[NAI based on a pseudonym or IMSI]

4.

5. EAP Response/Identity
[NAI based on a pseudonym or IMSI]

6. EAP Request/SIM Start
[Any identity]

7. EAP Request/SIM-Start
[Any identity]

8. EAP Response/SIM-Start
[Identity, NONCE_MT]

9. EAP Response/SIM-Start
[Identity, NONCE_MT]

10.

11.

12. EAP Request/SIM-Challenge
[RAND, MAC, Protected pseudonym, Next re-auth id, Result ind]

13. EAP Request/SIM -Challenge
[RAND, MAC, Protected pseudonym, Next re-auth id, Result ind]

14.

15. EAP Response/SIM-Challenge
[MAC, Result ind]

16. EAP Response/SIM-Challenge
[MAC, Result ind]

17.

18. Registration

19. EAP-Request/SIM/Notification
[Success notification]

20. EAP-Request/SIM/Notification
[Success notification]

21. EAP-Response/SIM/Notification

22. EAP-Response/SIM/Notification

23. EAP Success
+ keying material

24. EAP Success

25.

Figure 5: Authentication based on EAP SIM scheme

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

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

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

3. The WLAN-UE sends an EAP Response/Identity message. The WLAN-UE sends its identity complying with the Network Access Identifier (NAI) format specified in RFC 2486. NAI contains either a temporary identifier (pseudonym) allocated to WLAN-UE in previous authentication or, in the case of first authentication, the IMSI.

NOTE 1: Generating an identity conforming to NAI format from IMSI is defined in EAP/SIM.

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

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

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

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

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

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

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

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

9. WLAN-AN sends the EAP Response/SIM-Start packet to 3GPP AAA Server. The identity received in this message will be used by the 3GPP AAA server in the rest of the authentication process. If an inconsistency is found between the identities received in the two messages (EAP Response Identity and EAP Response/SIM Start) so that any user data retrieved previously from HSS/HLR are not valid, these data shall be requested again to HSS/HLR.

10. The AAA server checks that it has available N unused authentication vectors for the subscriber. Several GSM authentication vectors are required in order to generate keying material with effective length equivalent to EAP-AKA. If N authentication vectors are not available, a set of authentication vectors is retrieved from HSS/HLR. A mapping from the temporary identifier to the IMSI may be required.

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

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

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

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

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

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

    3GPP AAA Server sends RAND, MAC, protected pseudonym and re-authentication identity (the two latter in case they were generated) to WLAN-AN in EAP Request/SIM-Challenge message. The sending of the re-authentication id depends on 3GPP operator's policies on whether to allow fast re-authentication processes or not. It implies that, at any time, the AAA server decides (based on policies set by the operator) to include the re-authentication id or not, thus allowing or disallowing the triggering of the fast re-authentication process.

    The 3GPP AAA Server may send as well a result indication to the WLAN-UE, in order to indicate that it wishes to protect the success result message at the end of the process (if the outcome is successful). The protection of result messages depends on home operator's policies.

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

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

    This computing gives N SRES and Kc values.

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

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

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

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

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

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

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

17. 3GPP AAA Server compares its copy of the response MAC with the received MAC. If successful, the AAA server shall compare the MAC address, VPLMN Identity and the WLAN radio network information of the authentication exchange with the same information of the ongoing sessions. If the information is the same as with an ongoing session, then the authentication exchange is related to the ongoing session, so there is no need to do anything for the old sessions (skip step 18).

    The MAC address shall be checked only if the WLAN radio network information is the same as the ongoing sessions. If not, the MAC address cannot be considered trusted and no action is taken (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.

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

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

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

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

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

*** END SET OF CHANGES ***