3GPP TSG-SA3 Meeting #32 **Tdoc ⌘S3-040105**
Edingburgh, Scotland, 9-13 February, 2004

CR-Form-v7

Pseudo-CHANGE REQUEST

⌘ **33.234** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **0.8.0** ⌘

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:	⌘	Re-authentication clarifications and check of MAC in WLAN UE		
Source:	⌘	Ericsson		
Work item code:	⌘	WLAN Interworking	***Date:*** ⌘	27/01/2004
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: ⌘ An introduction in the re-authentication chapter has been added.

Added clarification regarding the temporary identities, that the support of this feature is mandatory for implementations in the network and WLAN UE, but optional for use in the network. The WLAN UE is mandated to support this feature. The process is initiated when the network sends to the WLAN UE the re-authentication identity, which will be replied to the network in the next re-authentication process. It is the network (i.e. AAA server) who decides whether to continue with fast re-authentication or with full re-authentication.

Also clarifications has been added to the full EAP-AKA and EAP-SIM procedures, to clarify that the WLAN UE derives required additional new keying material from the new computed IK and CK from USIM, and then checks the MAC received from the network with these newly derived keying material, i.e. the check of MAC takes place after the successful AKA has taken place on the USIM/SIM.

In addition some editorial errors or inconsistencies in TS 33.234 are corrected.

Summary of change: ⌘

Consequences if not approved: ⌘

Clauses affected: ⌘ 5, 6

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

Other comments: ⌘

5 Security features

[Editor's note: This section shall explain the provided security features in detail]

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

[Editor's note: This section shall deal with subscriber identity and authentication of the subscriber and Home Network/Serving Network. The authentication and key management mechanisms fulfilling the requirements in chapter 4 shall be listed here]

5.1.1 End to End WLAN Access Authentication (Scenario 2)

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

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

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

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

WLAN Authentication signalling shall be transported over ~~Wr~~ 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 ~~Wr~~ Wa reference point shall be based on standard Diameter[23,24] or RADIUS [15,26]protocols.

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

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

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

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

5.1.6 User Identity Privacy in WLAN Access

User identity privacy (Anonymity) is used to avoid sending the cleartext permanent subscriber identity (NAI) and make the subscriber's connections unlinkable to eavesdroppers.

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

The AAA server generates and delivers the pseudonym and/or the re-authentication identity to the WLAN-UE as part of the authentication process. The WLAN-UE shall not interpret the pseudonym or re-authentication identity, it will 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 pseudonym and re-authentication identity.

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 will 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.]

5.1.7 Re-authentication in WLAN Access

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

NOTE:

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

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

NOTE:

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

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

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

NOTE:

If several elements (UE, WLAN AN, 3GPP AAA server) maintain timers for periodic 802.1x/AAA re-authentications, then the element that has the shortest timer will determine the frequency of periodic

802.1x/AAA re-authentications, because each element is able to initiate an 802.1x/AAA re-authentication.

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

The 802.1x/AAA re-authentication process will be performed either with an EAP SIM/AKA full authentication process or with an EAP SIM/AKA fast re-authentication process~~ (from now on it will be simply called EAP SIM/AKA re-authentication)~~. ~~When the process is triggered, it is the WLAN UE's. decision to perform either a EAP SIM/AKA full authentication or a EAP SIM/AKA fast re-authentication This is indicated to the WLAN AN by sending either a pseudonym (EAP SIM/AKA full authentication) or a re-authentication id in EAP SIM/AKA fast re-authentication. ~~Both processes are described in this TS.

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

NOTE:

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

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

6 Security mechanisms

[Editor's note: This section shall describe the security mechanisms that are provided inter domain, intra domain and to the WLAN-UE.]

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 WLAN Access Authentication

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

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

6.1.1.1 EAP/AKA Procedure

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

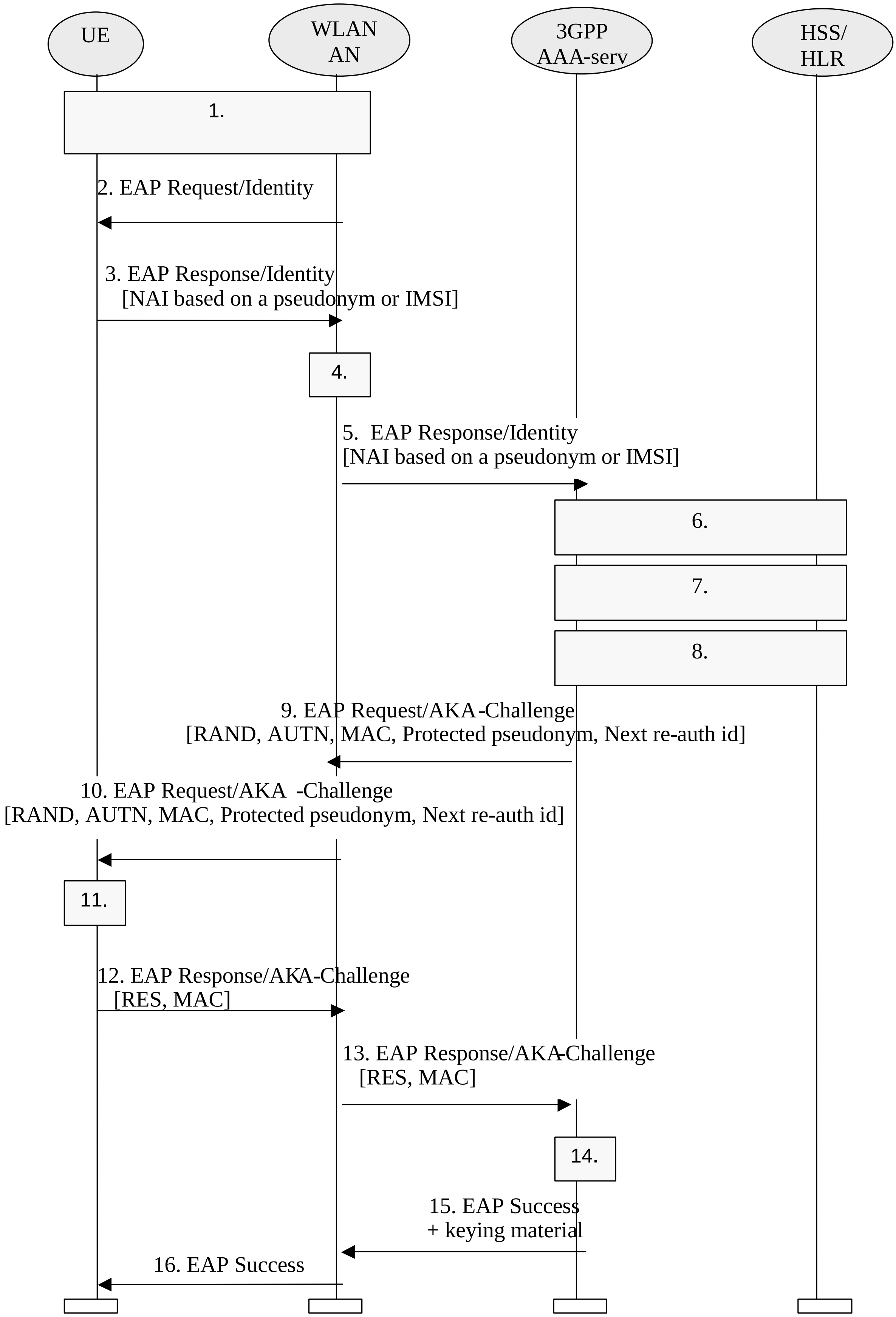

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity [NAI based on a pseudonym or IMSI]
4.
5. EAP Response/Identity [NAI based on a pseudonym or IMSI]
6.
7.
8.
9. EAP Request/AKA-Challenge [RAND, AUTN, MAC, Protected pseudonym, Next re-auth id]
10. EAP Request/AKA -Challenge [RAND, AUTN, MAC, Protected pseudonym, Next re-auth id]
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. 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: 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: 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. 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 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~~t~~ be chosen and 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 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.

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

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

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

12. 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~~a~~ new calculated MAC value to the WLAN-AN.

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

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

15. If all checks in step 14 are 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 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.

16. 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.

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.

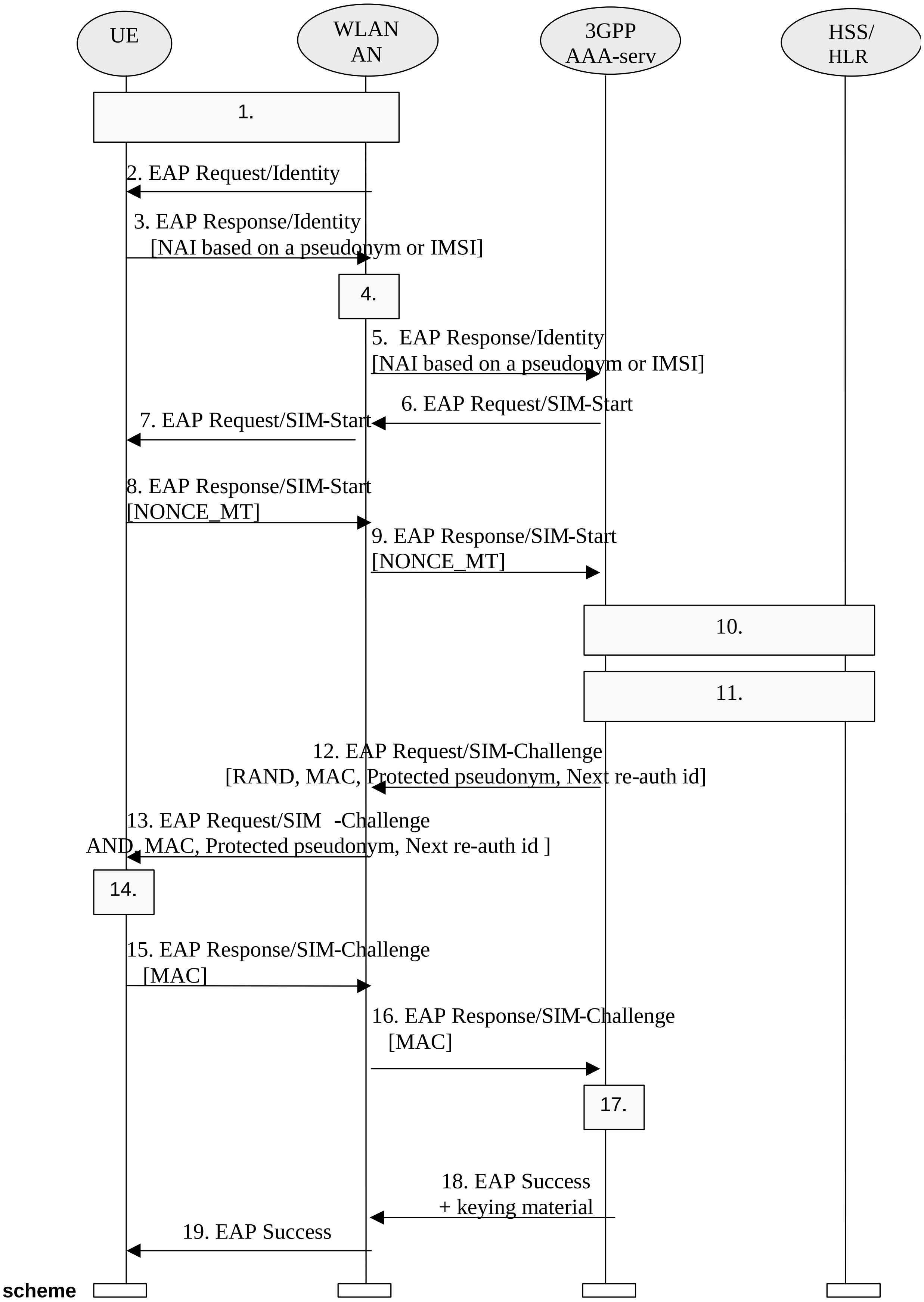

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity
[NAI based on a pseudonym or IMSI]
4.
5. EAP Response/Identity
[NAI based on a pseudonym or IMSI]
6. EAP Request/SIM-Start
7. EAP Request/SIM-Start
8. EAP Response/SIM-Start
[NONCE_MT]
9. EAP Response/SIM-Start
[NONCE_MT]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

Figure 7.2: 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 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 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: 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: 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. 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.

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-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-AN.

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

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 ~~t~~ 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.

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.

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.

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.

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

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

6.1.4 Fast r~~R~~e-authentication mechanisms in WLAN Access

When authentication processes have to be performed frequently, it can lead to a high network load specially when the number of connected users is high. Then it is more efficient to perform fast re-authentications. Thus the fast 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 ~~in the AAA server~~ is optional and depends on operator’s policies, which will be enforced by the AAA server by means of sending the re-authentication identity in any authentication process. The complete procedure is defined in ref [4]. In this section it is described how the process works for WLAN-3GPP interworking.

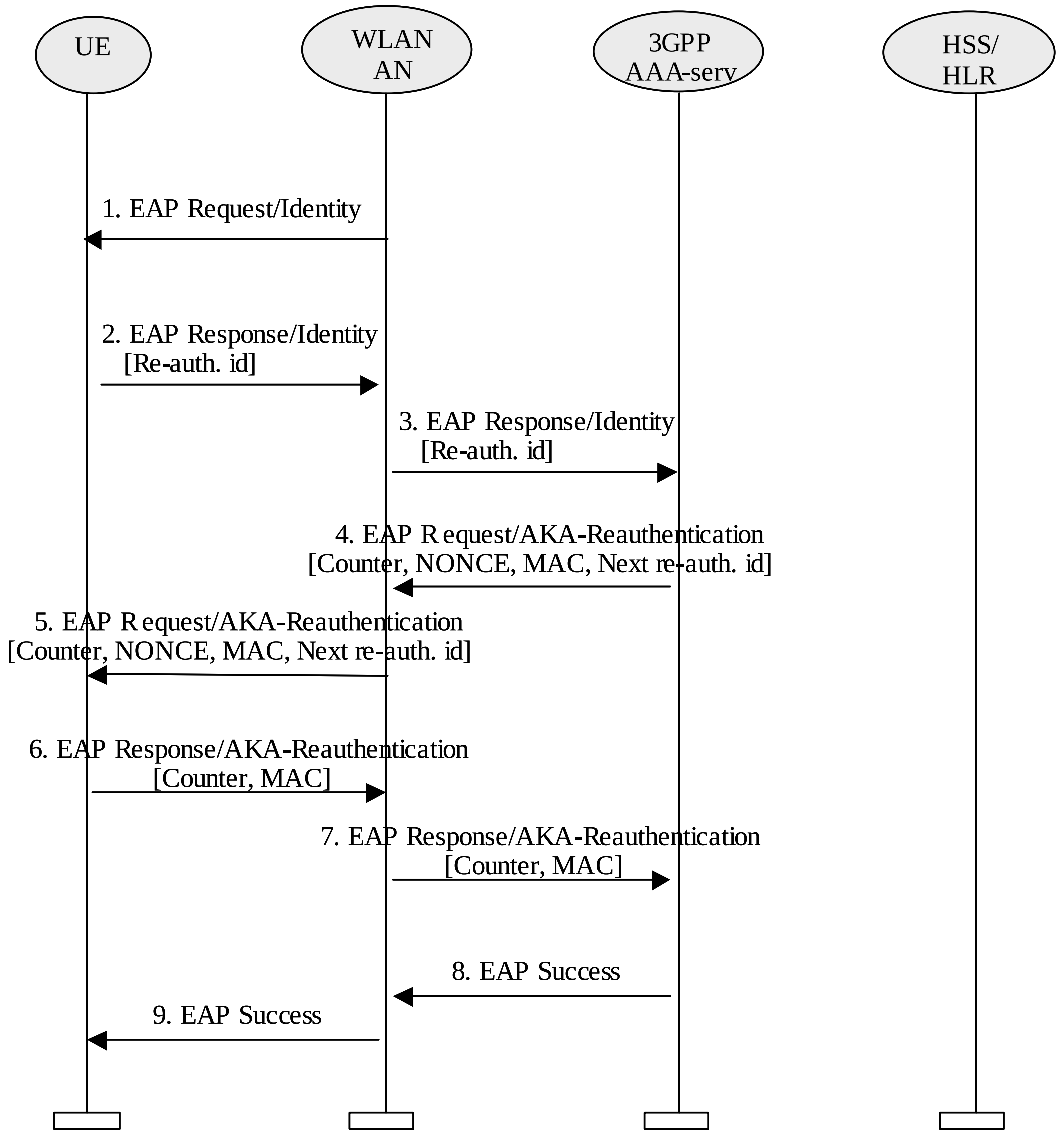

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1. EAP Request/Identity
2. EAP Response/Identity [Re-auth. id]
3. EAP Response/Identity [Re-auth. id]
4. EAP Request/AKA-Reauthentication [Counter, NONCE, MAC, Next re-auth. id]
5. EAP Request/AKA-Reauthentication [Counter, NONCE, MAC, Next re-auth. id]
6. EAP Response/AKA-Reauthentication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

Figure 6: EAP AKA fast r~~R~~e-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). ~~The WLAN-UE can take the decision of not performing a re-authentication but a full authentication. In that case, it will include a pseudonym in the message to the WLAN-AN and a normal authentication process will take place.~~
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 will force a full-authentication (to avoid the use of the re-authentication identity more than once).
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.
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 an EAP Success message.

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

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 will be enforced by the AAA server by means of sending the re-authentication identity in any authentication process. The complete procedure is defined in ref [4]. In this section it is described how the process works for WLAN-3GPP interworking.

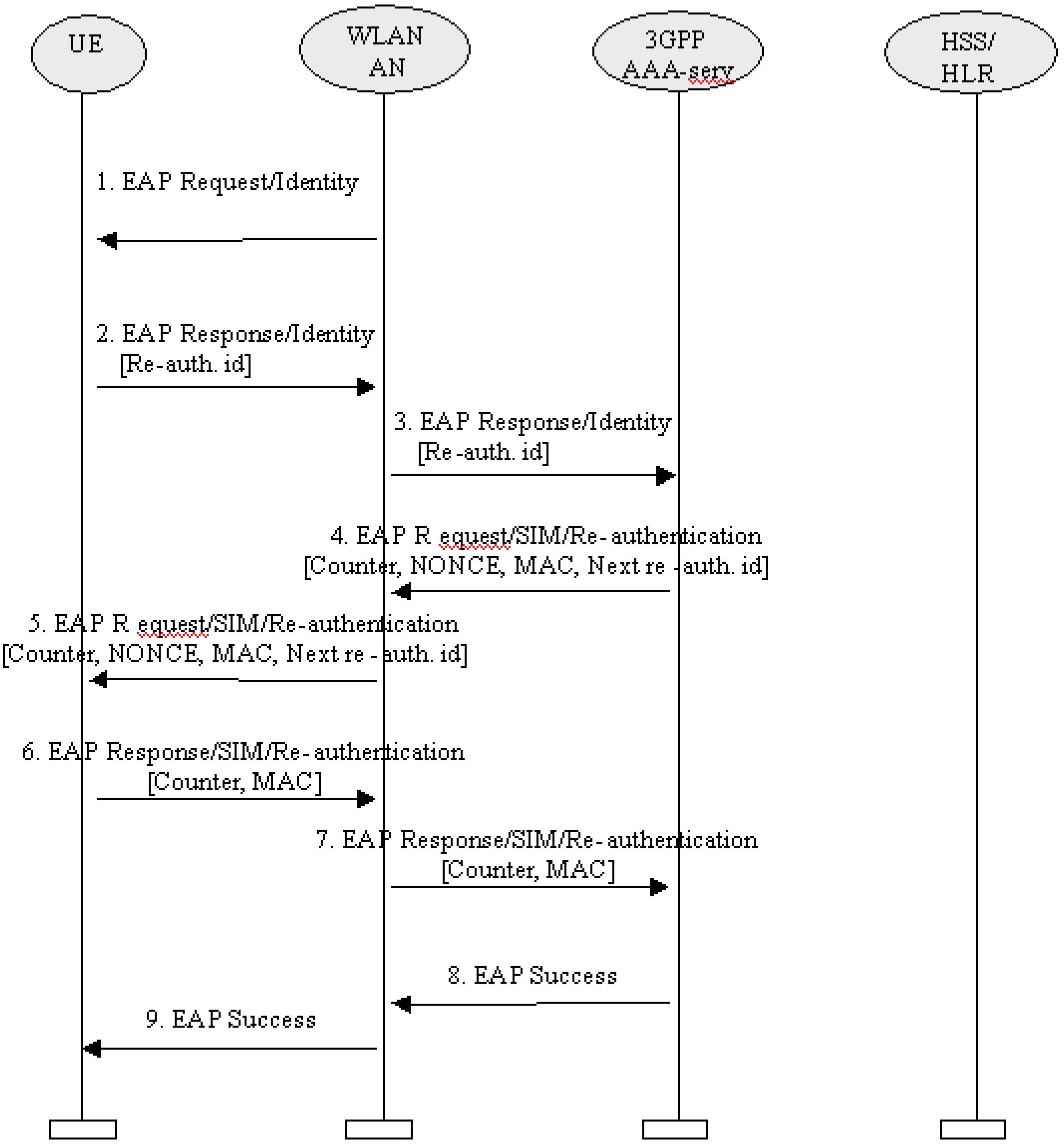

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1. EAP Request/Identity
2. EAP Response/Identity [Re-auth. id]
3. EAP Response/Identity [Re-auth. id]
4. EAP Request/SIM/Re-authentication [Counter, NONCE, MAC, Next re-auth. id]
5. EAP Request/SIM/Re-authentication [Counter, NONCE, MAC, Next re-auth. id]
6. EAP Response/SIM/Re-authentication [Counter, MAC]
7. EAP Response/SIM/Re-authentication [Counter, MAC]
8. EAP Success
9. EAP Success

Figure 7: EAP SIM fast rRe-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). ~~The WLAN-UE can take the decision of not performing a re-authentication but a full authentication. In that case, it will include a pseudonym in the message to the WLAN-AN and a normal authentication process will take place.~~

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 will force a full-authentication (to avoid the use of the re-authentication identity more than once).
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.
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 an EAP Success message.
9. The EAP Success message is forwarded to the WLAN-UE.

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

6.4.1 Temporary Identity Generation

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

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

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

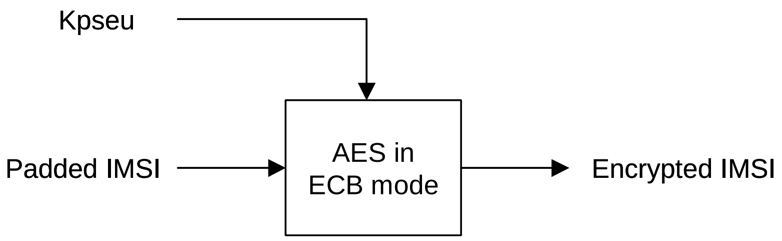
   E.g.: IMSI = 214070123456789 (MCC = 214 ; MNC = 07 ; MSIN = 0123456789)

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

   Observe that, at reception of a temporary identity, it is easy to remove the padding of the *Compressed IMSI* as none of the IMSI digits will be represented with 4 bits set to 1. Moreover, a sanity check should be done at reception of a pseudonym, by checking that the padding, the MCC and the MNC are correct, and that all characters are digits.
2. A *Padded IMSI* is created by concatenating an 8-octet random number to the *Compressed IMSI*.

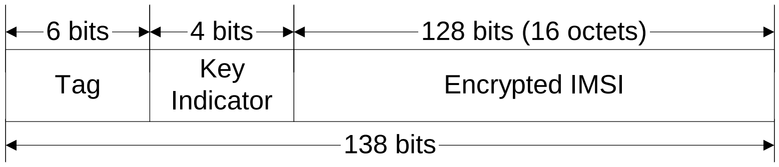
A 128-bit secret key, Kpseu, is used for the encryption. The same secret key must be configured at all the WLAN AAA servers in the operator network so that any WLAN AAA server can obtain the permanent identity from atemporary identity generated at any other WLAN AAA server (see section 6.4.2).

The figure below summarises how the *Encrypted IMSI* is obtained.



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

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



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

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

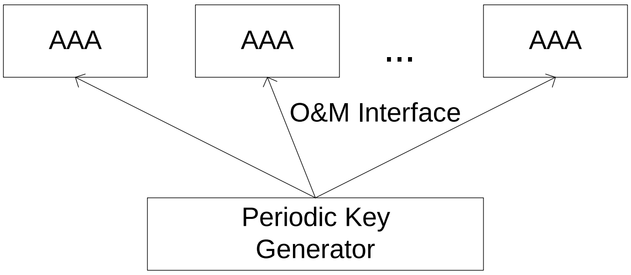
6.4.2 Key Management

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

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

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

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



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

6.4.3 Impact on Permanent User Identities

User identities (permanent or temporary) are sent with the form of a NAI, according to the EAP-SIM/AKA specifications, and the maximum length of a NAI that we can expect to be handled correctly by standard equipment is 72 octets (see ref. [14]). Moreover, this NAI will be transported inside the User-Name attribute of a RADIUS Access-Request, with standard length up to 63 octets (see ref. [15]). Therefore, it can be assumed that the maximum length of a WLAN user identity should be 63 octets (i.e. 63 characters).

Since the length of the ~~pseudonym~~ temporary identity proposed in section 6.4.1 is 23 characters, the length of the realm part of any WLAN permanent user identity must always be 40 characters or less. This applies regardless of whether the length of the username part of the permanent user identity is less than 23 characters. (Note that a WLAN temporary user identity is formed as a NAI with the pseudonym or re-authentication identity as the username part and the same realm part as the permanent user identity.)

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