3GPP TSG SA WG3 Security — S3#30 **Tdoc ⌘S3-030547**
Povoa de Varzim, Portugal 6 - 10 October 2003

CR-Form-v7

Pseudo-CHANGE REQUEST

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

*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 procedures		
Source:	⌘	Ericsson		
Work item code:	⌘	WLAN	***Date:*** ⌘	15/09/2003
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:	⌘	This CR proposes the introduction of the re-authentication process, which is useful for example to keep control on user's session (specially when Diameter is not supported in the WLAN-AN). This re-authentication can be performed either with repetitive full authentication procedures (already described in TS 33.234) or with fast re-authentication procedures (not yet defined in TS 33.234). Re-authentication chapter 5.1.7 in TS 33.234 does not actually describe a fast re-authentication procedure but a recommendation about it. This CR proposes a description of the fast re-authentication process. This process optimizes, in terms of traffic load, a re-authentication based on frequent full authentication processes.
Summary of change:	⌘	New text in chapter 5.1.7 and 6.1.4 will shown re-authentication flows and explanations will be given. Changes in 6.1.1.1 and 6.1.2.1 in order to allow sending of re-authentication identity. Chapter 2 References is updated
Consequences if not approved:	⌘	There will be cases in which the 3GPP operator does not have an accurate knowledge of the user's session and can not set limits to its duration. If fast re-authentication process is not be defined, the UE will not be able to perform fast re-authentications which can help to relieve network traffic load.

Clauses affected:	⌘	5.1.7 Re-authentication 6.1.4 Re-authentication mechanisms 2 References

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

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

*** 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: " Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking;".

[2] 3GPP TR 23.934: "3GPP system to Wireless Local Area Network (WLAN) Interworking; Functional and architectural definition".

[3] RFC 2284, March 1998, "PPP Extensible Authentication Protocol (EAP)".

[4] draft-arkko-pppext-eap-aka-06, November 2002, "EAP AKA Authentication".

[5] draft-haverinen-pppext-eap-sim-07, November 2002, "EAP SIM Authentication".

[6] IEEE Std 802.11i/D2.0, March 2002, "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 101 761-4v1.3.1B "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 "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: "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: "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] draft-ietf-aaa-eap-02.txt, June 2003, " Diameter Extensible Authentication Protocol (EAP) Application".

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

5.1.7 Re-authentication

~~[Editor's note: The text below requires further study - SA3 have identified areas that will need to be enhanced with further contributions from SA3 delegates. For example, the rules on the ratio between full SIM/USIM authentication and the re-authentication method and the exact details of the replay protection scheme require further study.]~~

~~*"On some networks, EAP authentication may be performed frequently. For such cases, EAP SIM and EAP AKA include an optional re-authentication procedure. Re-authentication causes less load on the network and is faster to execute than the full SIM/USIM authentication procedure. Re-authentication is optional to implement for both the WLAN UE and 3GPP AAA server. On each EAP authentication, either one of the entities may also fall back on full authentication if they do not want to use re-authentication. Re-authentication is based on the keys derived on the preceding full authentication.*~~

~~*On re-authentication, the UE protects against replays with an unsigned 16-bit counter. The server includes an encrypted server nonce (NONCE_S) in the re-authentication request. The Message Authentication Code attribute in the client's response is calculated over NONCE_S to provide a challenge/response authentication scheme. The NONCE_S also contributes to the new session keys.*~~

~~*Because one of the objectives of the re-authentication procedure is to reduce load on the network, the re-authentication procedure does not require the 3GPP AAA server to contact a reliable database. Therefore, the re-authentication procedure makes use of separate re-authentication user identities. Pseudonyms and the permanent IMSI-based identity are reserved for full authentication only. The network does not need to store re-authentication identities as carefully as pseudonyms. If a re-authentication identity is lost and the network does not recognize it, the 3GPP AAA server can fall back on full authentication.*~~

~~*If the 3GPP server supports re-authentication, it may communicate an encrypted re-authentication identity for next re-authentication to the WLAN UE during full authentication. If the client wants to use re-authentication, it uses this re-authentication identity on next authentication."*~~

WLAN re-authentication is performed between WLAN-UE and 3GPP AAA server, through Ws and Wr interfaces.

The WLAN-AN can initiate the re-authentication process periodically, triggered by the timeout of a counter which normally is set by O&M procedures in the WLAN-AN but it can be sent to the WLAN-AN by the AAA server in a RADIUS or Diameter message (in the attribute Session Timeout). At reception of this attribute, the WLAN-AN will substitute the previously set counter by the received one.

The re-authentication process initiated by the WLAN-AN will be performed either with a full authentication process or with a fast re-authentication process (from now on it will be simply called re-authentication). Both processes are described in this TS.

The re-authentication process must be implemented together with the full authentication procedure, although its use is optional and depends on operators' polices. These policies depend on the level of trust of the 3GPP operator and the WLAN AN, and the possible threats detected by operator which may require a periodic refresh of keys. The full process description can be found in ref. [4] and [5].

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

5.5 Immediate Service Termination

~~[Editor's note: This section shall deal with the network capability to terminate ongoing subscriber activities in the WLAN access when this is required due to e.g. end of subscription, expiration of charging account, detection of fraudulent activities, etc.]~~

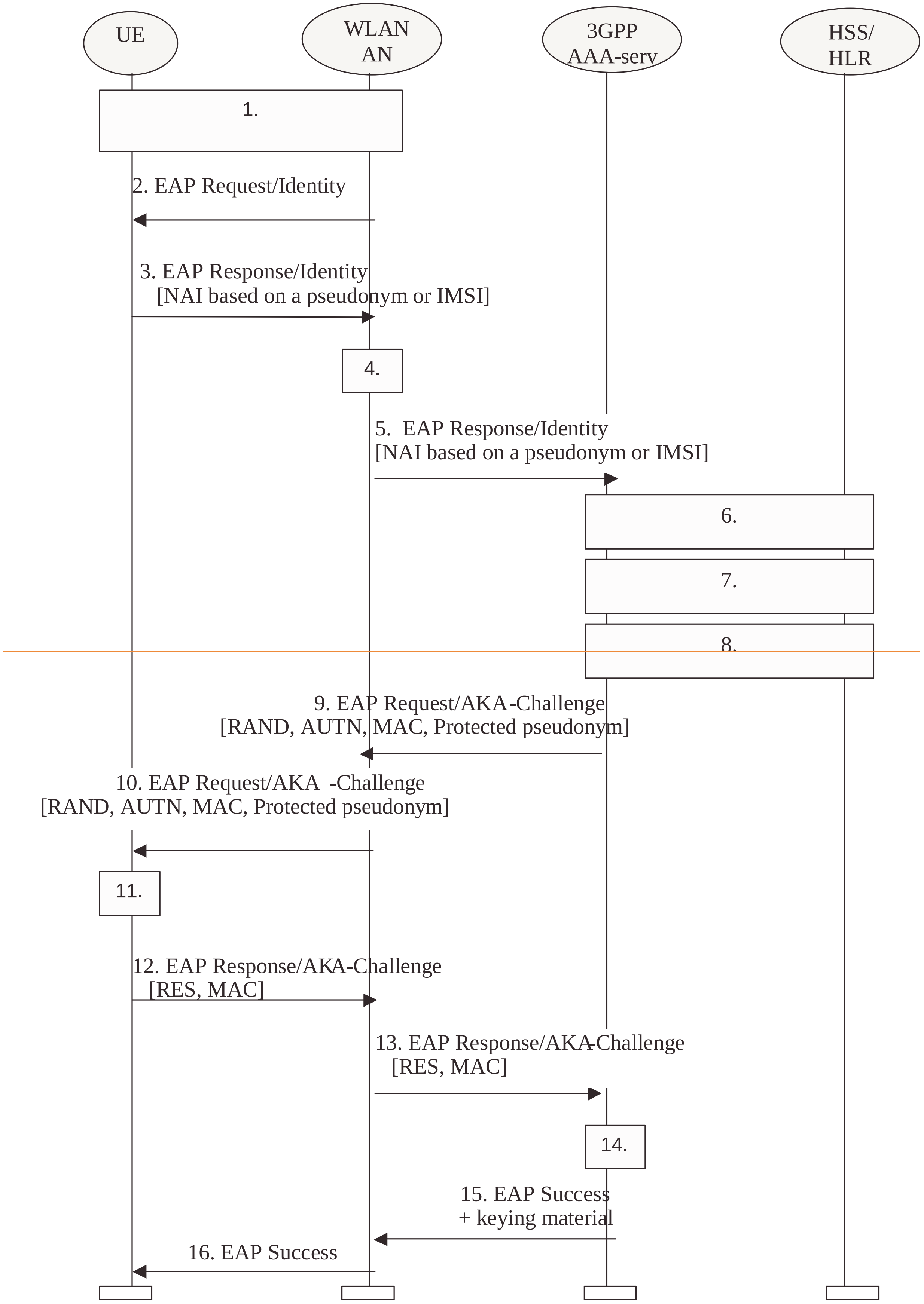
Currently there exist mechanisms in Diameter used to terminate a session for a certain user when the Home network decides it, for example when he/she runs out of credit. The problem shows up when Diameter has to coexist with RADIUS, which is the case of 3GPP-WLAN interworking. In it, the path between the Home AAA server and the UE is not guaranteed to be always in Diameter, but some path may be RADIUS due to legacy WLAN ANs which support only RADIUS. In order to solve this, the AAA server can order the WLAN AN to perform frequent re-authentications so that the home network can keep control on user's activity and for example when he/she runs out of credit, stop it in the next re-authentication. This case is specially interesting when there is low trust between the WLAN-AN and the 3GPP network.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

6.1.1.1 EAP/AKA Procedure

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


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

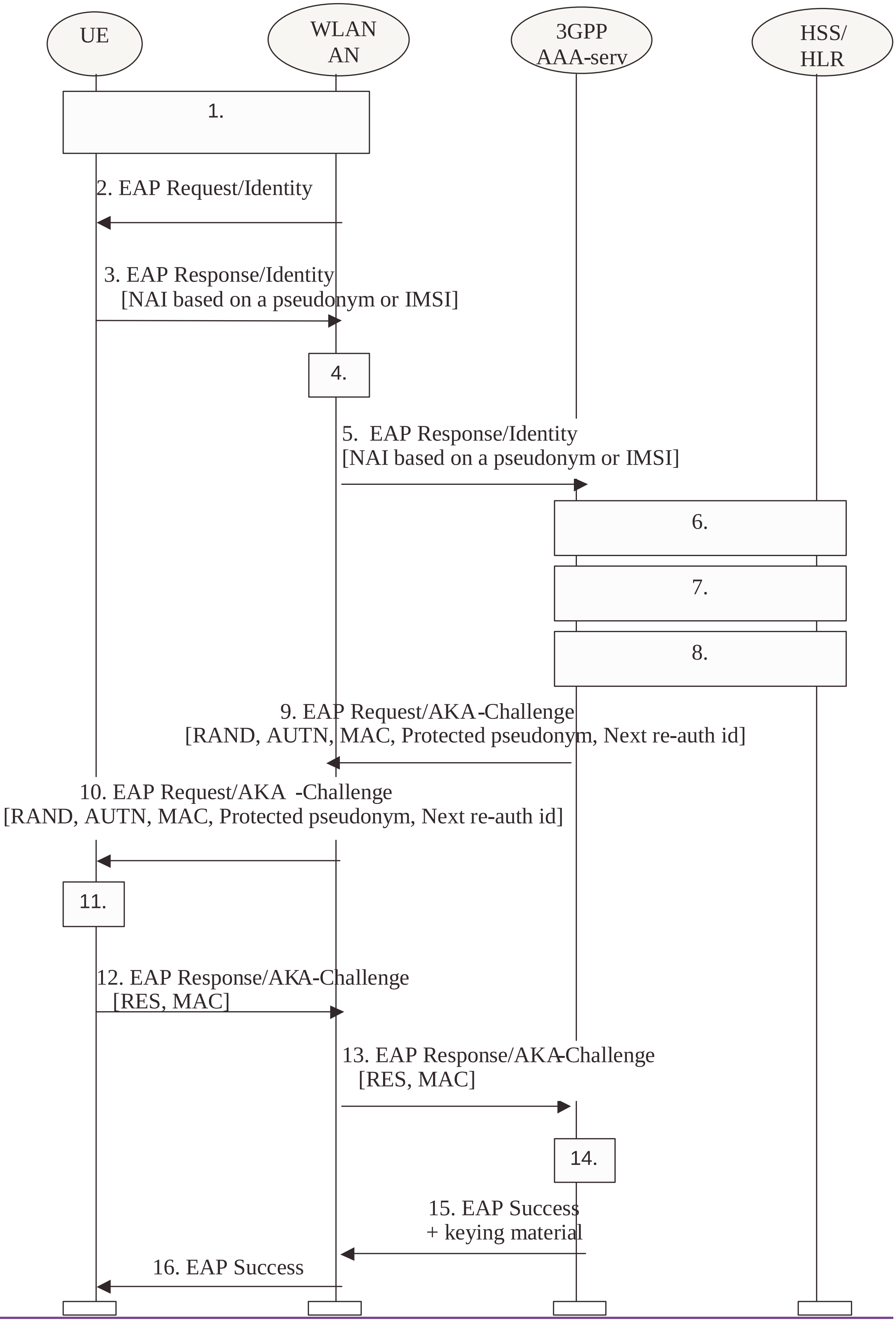

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity
[NAI based on a pseudonym or IMSI]
4.
5. EAP Response/Identity
[NAI based on a pseudonym or IMSI]
6.
7.
8.
9. EAP Request/AKA-Challenge
[RAND, AUTN, MAC, Protected pseudonym, Next re-auth id]
10. EAP Request/AKA -Challenge
[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 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 mat 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 ~~(in case it was generated)~~ 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 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 re-authentication process.
10. The 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, c.f. [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

    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-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.

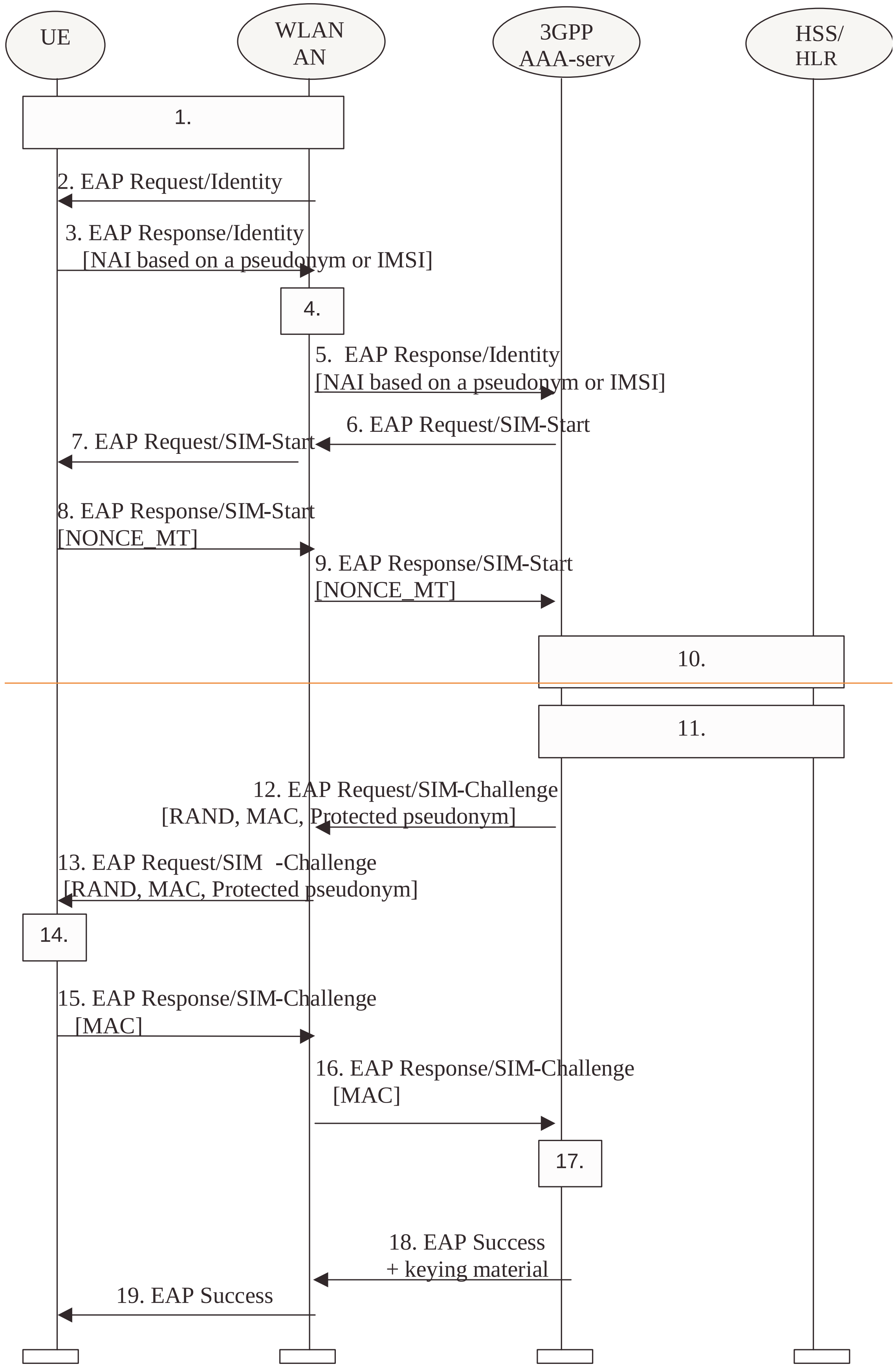
16. WLAN-AN informs the WLAN-UE about the successful authentication with the EAP Success message. Now the EAP AKA exchange has been successfully completed, and the WLAN-UE and the WLAN-AN share keying material derived during that exchange.

*** END SET OF CHANGES ***

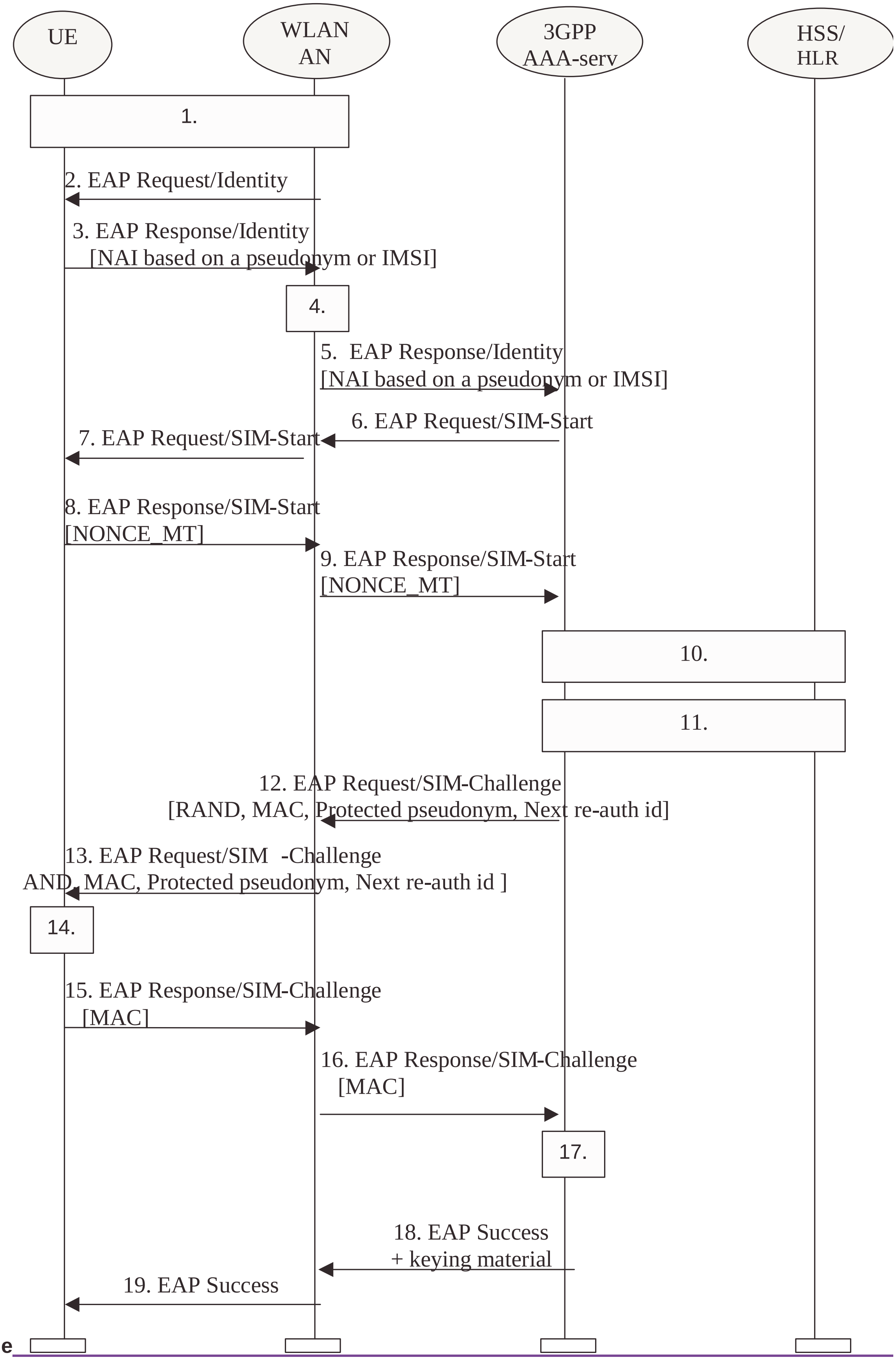
*** BEGIN SET OF CHANGES ***

6.1.2.1 EAP SIM procedure

The EAP-SIM authentication mechanism is specified in ref. [5]. The present section describes how this mechanism is used in the WLAN-3GPP interworking scenario.


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

~~7.2: Authentication based on EAP SIM~~


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

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 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: 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, ~~and~~ protected pseudonym and re-authentication identity (the two latter in case ~~it was~~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 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 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 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 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.

*** END SET OF CHANGES ***

*** BEGIN SET OF CHANGES ***

## 6.1.4	Re-authentication mechanisms

~~[Editor's note: This section shall describe the mechanisms to support the re-authentication feature described in 5.1.7]~~

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 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 re-authentication mechanism described in this chapter, although its use is optional and depends on operator's policies. The complete procedure is defined in ref [4]. In this section it is described how the process works for WLAN-3GPP interworking.

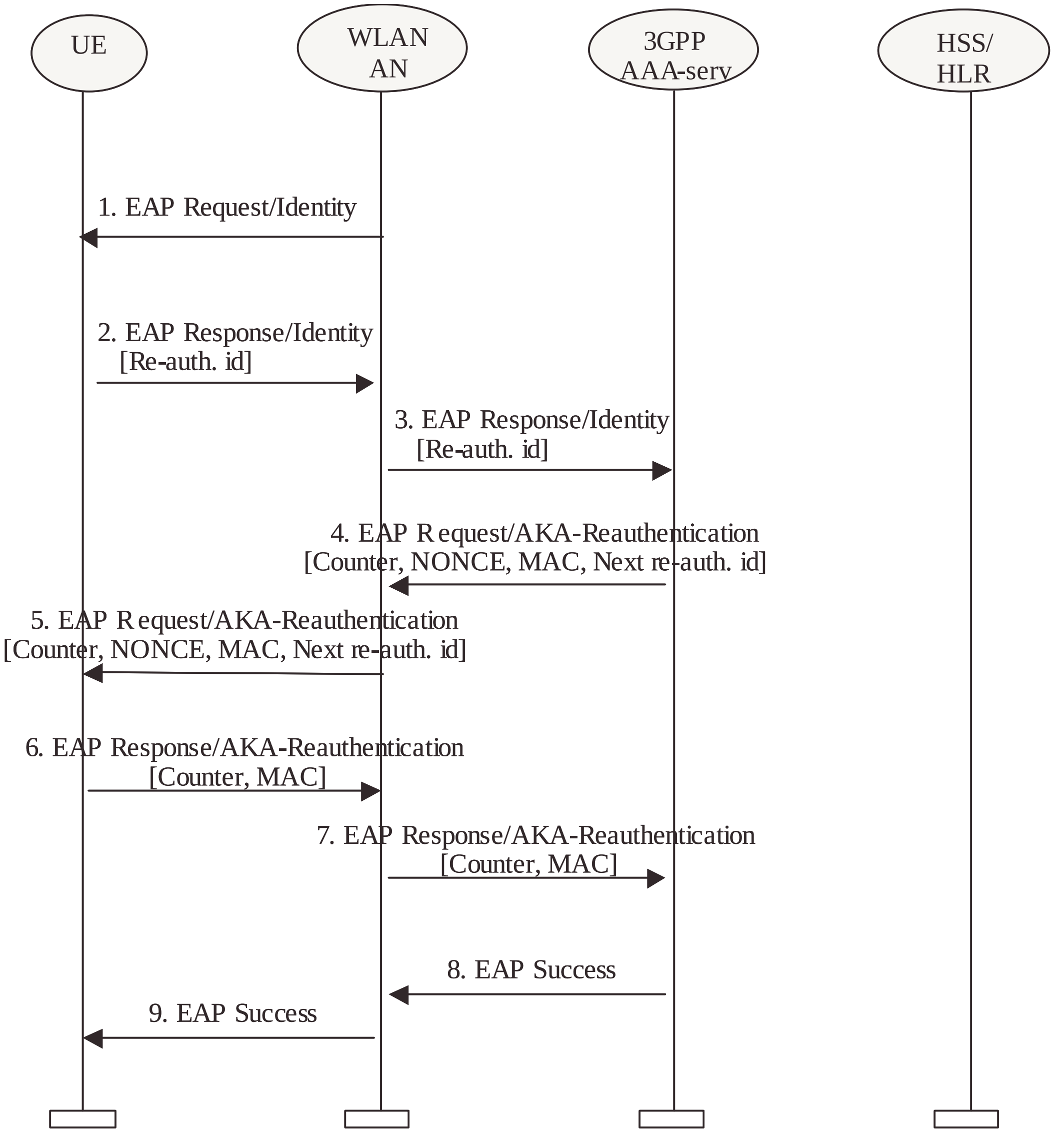

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1. EAP Request/Identity
2. EAP Response/Identity [Re-auth. id]
3. EAP Response/Identity [Re-auth. id]
4. EAP R equest/AKA-Reauthentication [Counter, NONCE, MAC, Next re-auth. id]
5. EAP R equest/AKA-Reauthentication [Counter, NONCE, MAC, Next re-auth. id]
6. EAP Response/AKA-Reauthentication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

Figure 7.3 : EAP AKA 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). 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 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 re-authentication mechanism described in this chapter, although its use is optional and depends on operator's policies. The complete procedure is defined in ref [4]. In this section it is described how the process works for WLAN-3GPP interworking.

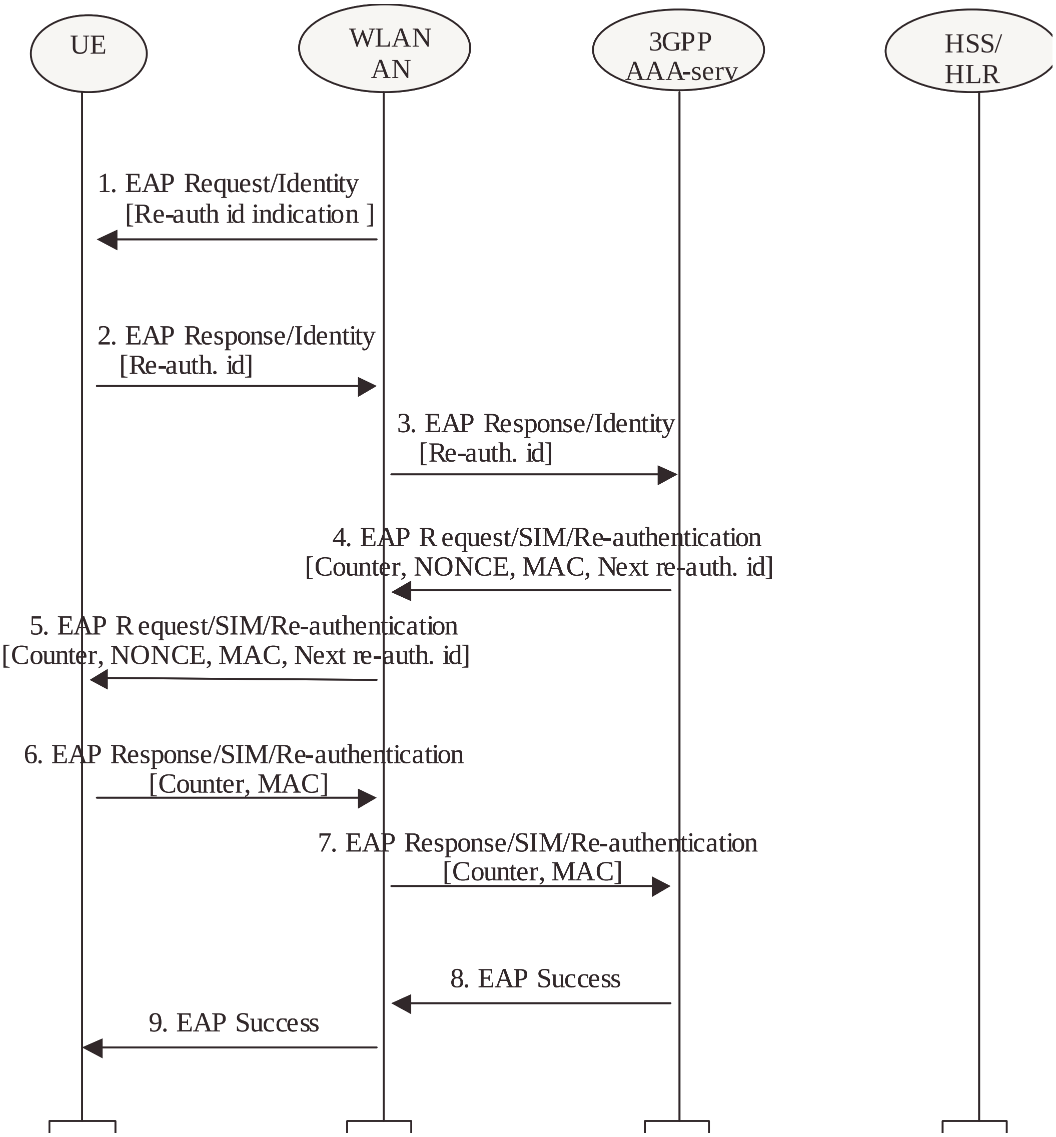

UE
WLAN AN
3GPP AAA-serv
HSS/ HLR
1. EAP Request/Identity [Re-auth id indication]
2. EAP Response/Identity [Re-auth. id]
3. EAP Response/Identity [Re-auth. id]
4. EAP R equest/SIM/Re-authentication [Counter, NONCE, MAC, Next re-auth. id]
5. EAP R equest/SIM/Re-authentication [Counter, NONCE, MAC, Next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

Figure 7.4 : EAP SIM 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). 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 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.

*** END SET OF CHANGES ***