3GPP TSG SA WG3 Security — S3#34 **S3-040689**
July 6 - 9, 2004
Acapulco, Mexico

Title:	Reply LS on multiple connections to VPLMNs simultaneously
Response to:	S3-040457 (S1-040389) Reply LS on multiple connections to VPLMNs simultaneously
Work Item:	WLAN
Source:	SA3
To:	SA1
Cc:	SA2

Contact Person:
Name: Yingxin Huang
Tel. Number: +86 82882753
E-mail Address: huangyx@huawei.com

Attachments: S3 040352, S3 040440, S3 040668

1. Question by SA2:

"SA1 ask SA3 group to provide comment whether simultaneous UE connections to multiple VPLMNs can be provided without reducing the security provided by 3GPP."

2. Reply by SA3:

At current stage, SA3 identified in the contribution S3-040352 to SA3#33 a potential compromise to 3GPP security by supporting simultaneous UE connections to multiple VPLMNs, or more generally, by supporting multiple WLAN Access sessions with different MAC address and/or VPLMN id, and/or WLANAN information. The corresponding CR S3-040440 to TS 33.234 was approved at SA3#33.

With the approved CR S3-040440 and S3-040668, SA3 have developed a mechanism to enable the restriction to multiple WLAN Access sessions of a subscriber. Thereby the multiple WLAN Access sessions (including simultaneous UE connections to multiple VPLMNs) can be properly restricted under the operator's need or subscriber's request. The need for restricting the number of simultaneous connections may depend, among other things, on the charging model, cf. S3-040352. Nevertheless, if SA1 decide that simultaneous connections to multiple VPLMNs have to be allowed, SA3 need to study the implications more in detail, as it would mean to remove the restriction provided by the mechanism cited above.

In summary, SA3 identified a potential impact to the 3GPP security with simultaneous UE connections to multiple VPLMNs or more general multiple WLAN Access sessions of a subscriber. Consequently, SA3 has put appropriate measures into place.

3. Actions

SA3 would like to ask SA1 take the above information into consideration in the decision about supporting multiple WLAN Access sessions.

4. Dates of Next SA3 Meetings:

TSG-SA3 Meeting #35	5-8 October 2004	Malta
TSG-SA3 Meeting #36	23-26 November 2004	Shenzhen, China

3GPP TSG-SA3 Meeting #33
Beijing, China, 10-14 May 2004

Tdoc ⌘S3-040352

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*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:	⌘	WLAN handover scenario
Source:	⌘	Nokia
Work item code:	⌘	WLAN-3G interworking security
Date:	⌘	02/05/2004
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:	⌘	If the WLAN-UE connects to multiple AAA server, there is no need to keep the previous connection for a geniue UE. The release mechanism can also mitigate any malicious mis-use of the crenditical to minimum.
Summary of change:	⌘	The change is added how to handle muliple registrations of the WLAN-UE based on local policy defined for AAA server and HSS.
Consequences if not approved:	⌘	The malicious usage of radio service will not be prevented.

Clauses affected:	⌘	6.1.1.1

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

Other comments:	⌘	

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.

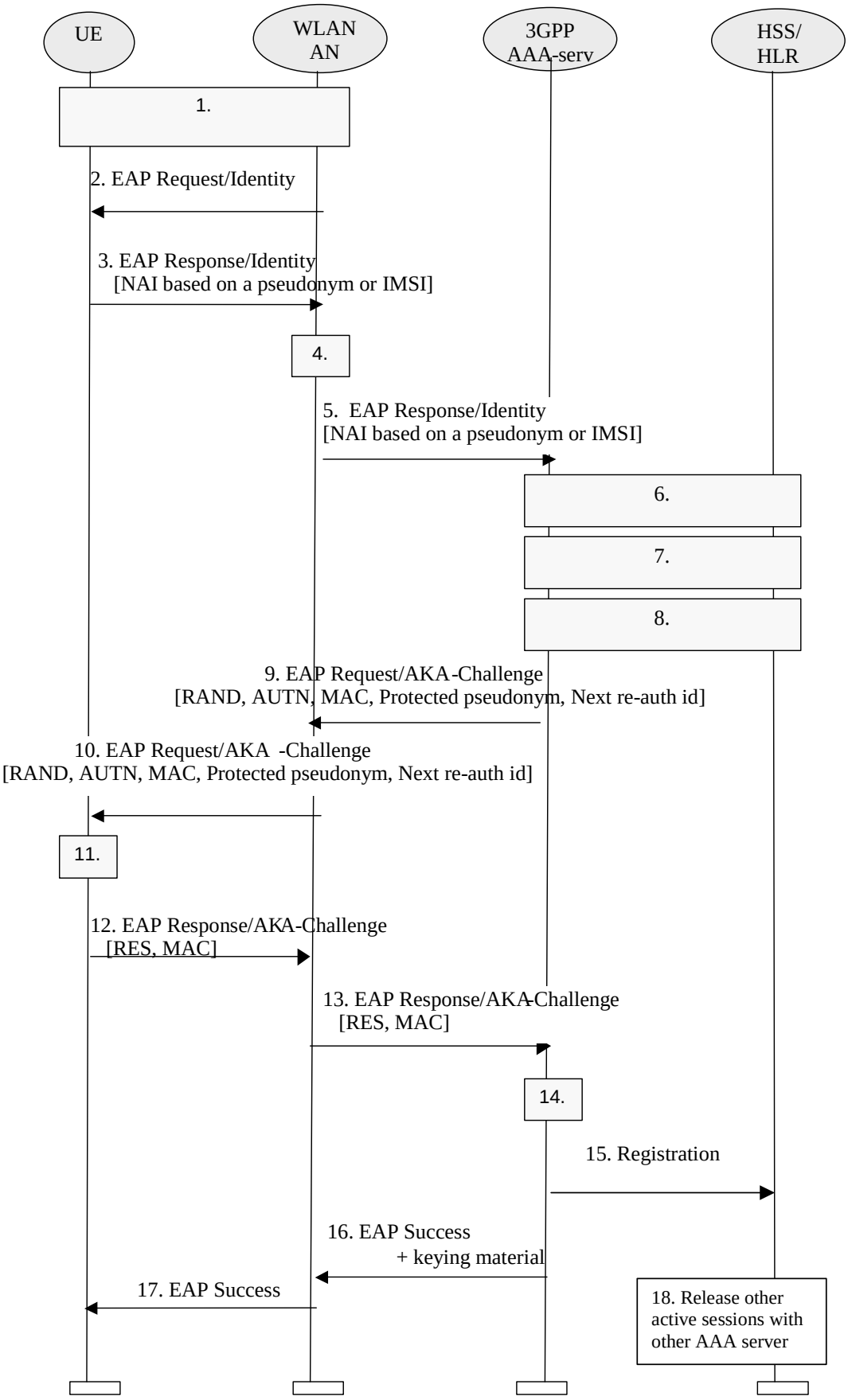


Figure 4: Authentication based on EAP AKA scheme

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 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. 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 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 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.

12. 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.

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

14. ~~14.~~ 3GPP AAA Server checks the received MAC and compares XRES to the received RES. If successful, the AAA server shall compare the MAC address 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 15).

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

    In case a pre-Rel 6 HSS is used, the AAA server shall instead, to handle the decision locally. The AAA shall creates a new session and records in local database the terminal's MAC address and the WLAN radio network identification, received over the Wa or Wd reference point, with the session information. If the AAA server identifies that 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 about the old sessions. Otherwise, f the comparison in step 2 indicates that the MAC address or the radio network information is different than in any ongoing session, then the authentication exchange is related to a scenario-2 session that was previously unknown to the 3GPP AAA server. Since a pre-release 6 HLR/HSS is being used, the 3GPP AAA needs to make the decision about closing an old session itself. If simultaneous sessions are not allowed, or if the number of allowed sessions has been exceeded, then the 3GPP AAA server closes an old scenario-2 session.

16. ~~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.~~17. 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.

18. If the same subscriber but different MAC address 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 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.

3GPP TSG SA WG3 Security — S3#33 **S3-040xxx**

10 - 14 May 2004

Beijing, China

Title: Limiting simultaneous WLAN scenario-2 connections

Source: Nokia

Document for: Discussion and approval

Agenda Item: WLAN

1 Introduction

This submission proposes a mechanism to limit the number of simultaneous scenario-2 sessions per subscriber in order to prevent certain fraud scenarios. The proposed mechanism works with IEEE 802.11i pre-authentication and it can also be adapted to allow some limited number of simultaneous scenario-2 sessions.

2 Discussion

2.1 Motivation

If a single subscriber is allowed to establish an unlimited number of WLAN scenario-2 sessions, then certain fraud scenarios can occur. For example, a malicious user might buy a subscription, share the subscription with a large number of users and later refuse to pay the incurred bills. Another example is that a malicious use buys a flat-rate subscription, and then charges for connectivity provided for other users.

It would be advantageous to limit the number of scenario-2 sessions a subscriber can have in order to eliminate these fraud scenarios.

2.2 How many simultaneous sessions are needed?

In general, a single WLAN radio can only have one scenario-2 session at a time, because there is a one-to-one correspondence between a scenario-2 session and a WLAN association. If we assume that only one WLAN radio is available, then the number of simultaneous sessions could be limited to at most one per subscriber at a moment.

It is conceivable that UEs might have several different WLAN radios, so there might be some use for a very small number of simultaneous scenario-2 sessions. Also in the split UE case, it might be desirable to allow two simultaneous connections, one from a phone and another from a laptop.

Hence, the required number of simultaneous scenario-2 sessions per subscriber is either one, or in some cases, some very small number such as two or three.

2.3 New sessions should prevail over old sessions

When simultaneous sessions are to be prevented, it would be better to disconnect the old sessions when a new session is established, rather than to block new session attempts when there is an ongoing session. Blocking new session attempts would be problematic because it may be difficult

to close all WLAN sessions in a timely manner. The valid user might have left the radio coverage of some previous WLAN network without explicitly closing the session, so an old WLAN session might still be dangling. Even though dangling sessions should be automatically closed as soon as possible, there can still be delays of at least a minute. Such dangling sessions should not prevent the valid user from creating new sessions.

Hence the preferred way of limiting the number of simultaneous scenario-2 sessions is to close the old session when a new session is established. Draft TS 23.234 already includes a procedure in the Wa and Wd reference points by which the 3GPP AAA server can disconnect a scenario-2 session, and a procedure in the Wx reference point by which the HSS can tell the 3GPP AAA server to disconnect a scenario-2 session.

2.4 IEEE 802.11i Pre-Authentication and Pairwise Master Key Caching

IEEE 802.11i specifies the concepts of Pairwise Master Key (PMK) caching and pre-authentication. In pre-authentication, the terminal can authenticate with several APs (AP2, AP3, …) while associated with a single AP (AP1). The AP1 with which the terminal is associated relays authentication information to the other APs (AP2, AP3, …), in other words, the terminal is not in radio communications with AP2, AP3, ….

The purpose of pre-authentication is to enable the terminal and other APs to establish Pairwise Master Keys in advance, so that handovers can later be performed quickly. PMK caching refers to the procedure where the terminal maintains copies of PMKs shared with several APs, and is able to quickly handover back to the previously visited APs.

Due to pre-authentication and PMK caching, WLAN authentication exchanges do not have a one-to-one correspondence to WLAN scenario-2 sessions or WLAN associations. When the terminal pre-authenticates with an AP, the AAA server should not close the connection with the original AP. Also when the terminal performs a handover between access points within the same WLAN radio network, the AAA server should not close the old connection, because PMK caching can later be used to return to the same AP quickly.

2.5 Proposed Mechanisms

2.5.1 General

WLAN radio network implementations already prevent having simultaneous sessions with the same MAC address in a single WLAN network. The access points usually use an Inter Access Point Protocol (IAPP) to notify each other when an association with a certain terminal MAC address is established. If some other access point also has an association, it will disassociate because it interprets it as the terminal having moved to a new access point.

Hence, it is only necessary to limit the simultaneous sessions in different WLAN radio networks, and with different MAC addresses. The terminal's MAC address is included in the AAA packets even according to current AAA protocols, and there will most likely be need to include some identifier of the WLAN radio network as well, for example to produce detailed and itemized bills about WLAN usage with WLAN network identification information to the end users.

Therfore it is proposed that the Wa and Wd reference points enable communicating the terminal's MAC address and an identifier of the WLAN radio network from the WLAN AN to the 3GPP AAA server. It is also proposed that the Wx reference point should enable communicating the terminal's MAC address and an identifier of the WLAN radio network from the 3GPP AAA server to the HSS (see section below the justification).

2.5.2 Operation with a release-6 HSS

If a release-6 compliant HSS is used, then the decision about whether to close an old session upon the establishment of a new session can be done by the HSS. The HSS is the only element that is aware of all the sessions a subscriber has, since there can be several 3GPP AAA servers. The 3GPP AAA server cannot be aware of the sessions the subscriber might have with other 3GPP AAA servers.

It is proposed that the AAA server operates as follows upon a scenario-2 authentication exchange:

1. After successful authentication, the AAA server checks whether there is an ongoing scenario-2 session for the subscriber. If there is no ongoing session, the AAA server registers this session with the HSS over the Wx reference point (as described in draft TS 23.234). The AAA server includes the terminal's MAC address and the WLAN radio network identification, received over the Wa or Wd reference point, in the registration.
2. If the AAA server detects that there is an ongoing session, the AAA server compares the MAC address 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.
3. If the comparison in step 2 indicates that the MAC address or the radio network information is different than in any ongoing sessions, then the authentication exchange is related to a new scenario-2 session or to a scenario-2 session that has been so far managed by a different 3GPP AAA server. Since a release 6 compliant HSS is being used, the 3GPP AAA server registers the new session with the HSS to let the HSS decide whether something needs to be done with the old sessions.

When an AAA server registers a scenario-2 session with the HSS, the HSS should operate as follows:

1. The HSS server compares the MAC address 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 close any sessions. (It should be noted that the 3GPP AAA server might change during a session, so not all new registrations necessarily relate to a new scenario-2 session).
2. If the comparison in step 1 indicates that the MAC address or the radio network information is different than in any ongoing session, then the registration is related to a new scenario-2 session. If simultaneous sessions are not allowed, or if the number of allowed sessions has been exceeded, then the HSS can close an old scenario-2 session by indicating the 3GPP AAA server of the old session to terminate the session.

2.5.3 Operation with a pre-release 6 HLR/HSS

If a pre-release 6 HLR/HSS is used, then there is no centralized element that would be aware of all the sessions. In this case, the 3GPP AAA server needs to make the decisions about closing the old sessions itself. As the AAA server cannot be aware of the sessions the subscriber might have with other AAA servers, this mechanism cannot guarantee that simultaneous sessions would always be prevented.

It is proposed that when a pre-release 6 HLR/HSS is used, the 3GPP AAA server operates as follows upon a scenario-2 authentication exchange:

1. After successful authentication, the AAA server checks whether there is an ongoing scenario-2 session for the subscriber. If the subscriber has no ongoing sessions, the AAA server creates a new session and records the terminal's MAC address and the WLAN radio

network identification, received over the Wa or Wd reference point, with the session information.

2. If the 3GPP AAA server detects that the subscriber has an ongoing session after successful scenario-2 authentication, the AAA server compares the MAC address and the WLAN radio network information of the authentication exchange with the same information of the ongoing session(s). 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 about the old sessions.
3. If the comparison in step 2 indicates that the MAC address or the radio network information is different than in any ongoing session, then the authentication exchange is related to a scenario-2 session that was previously unknown to the 3GPP AAA server. Since a pre-release 6 HLR/HSS is being used, the 3GPP AAA needs to make the decision about closing an old session itself. If simultaneous sessions are not allowed, or if the number of allowed sessions has been exceeded, then the 3GPP AAA server closes an old scenario-2 session.

3 Proposal

We propose that SA3 adopt the mechanisms presented in Section 2.5.

3GPP TSG-SA3 Meeting #33
Beijing, China, 10-14 May 2004

Tdoc ⌘S3-040440

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **6.0.0** ⌘

*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:	⌘	WLAN mechanism to allow restrictions on simultaneous sessions
Source:	⌘	Nokia
Work item code:	⌘	WLAN-3G interworking security
Date:	⌘	14/05/2004
Category:	⌘	**C**
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:	⌘	If the WLAN-UE connects to multiple AAA servers, there is no need to keep the previous connection for a genuine UE. The release mechanism can also mitigate any malicious mis-use of the credential to minimum.
Summary of change:	⌘	The change is added how to handle muliple registrations of the WLAN-UE based on local policy defined for AAA server and HSS/HLR.
Consequences if not approved:	⌘	The malicious usage of radio service will not be prevented.

Clauses affected:	⌘	6.1.1.1, 6.1.2.1

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

Other comments:	⌘	

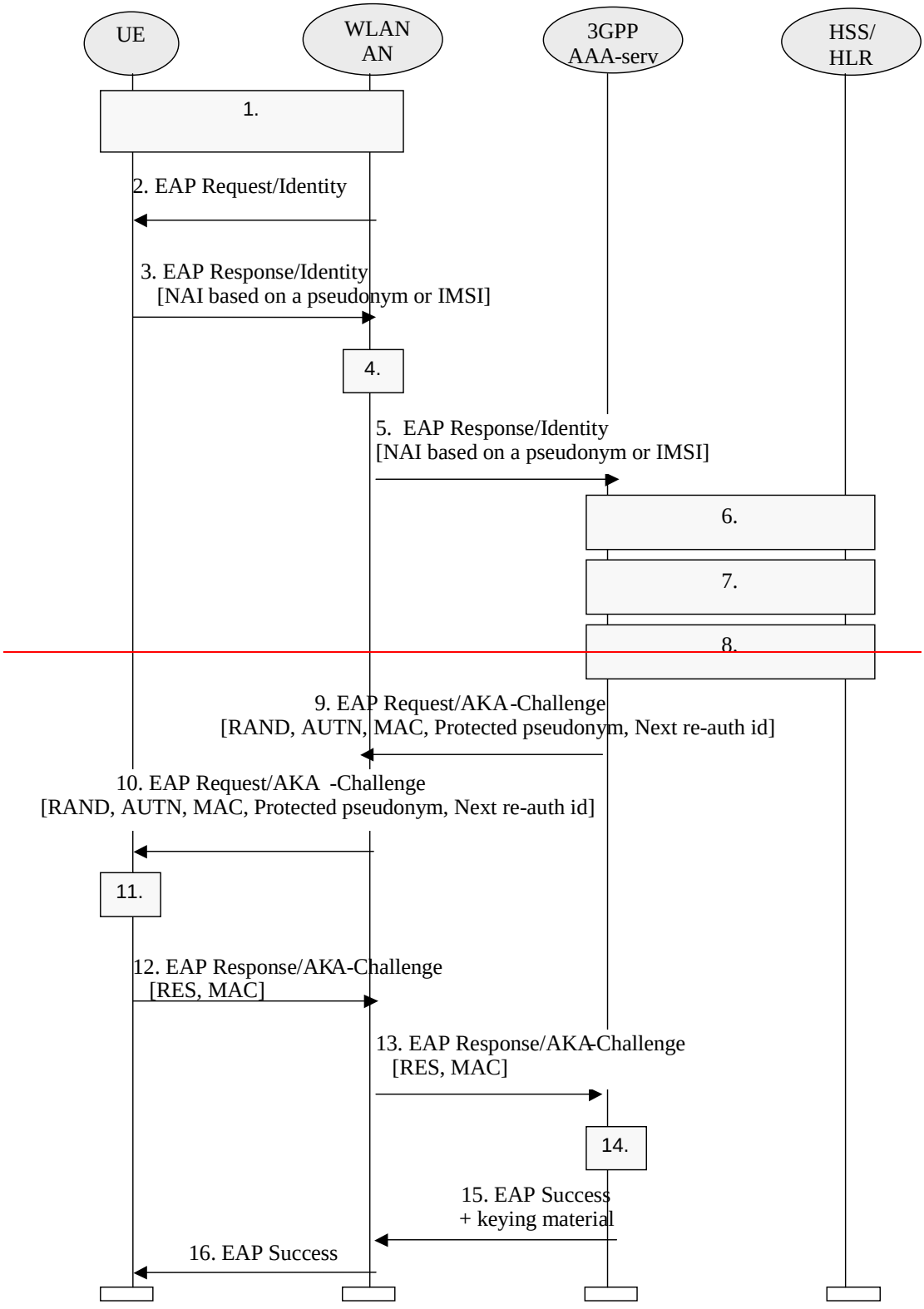
6.1.1 USIM-based WLAN Access Authentication

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.



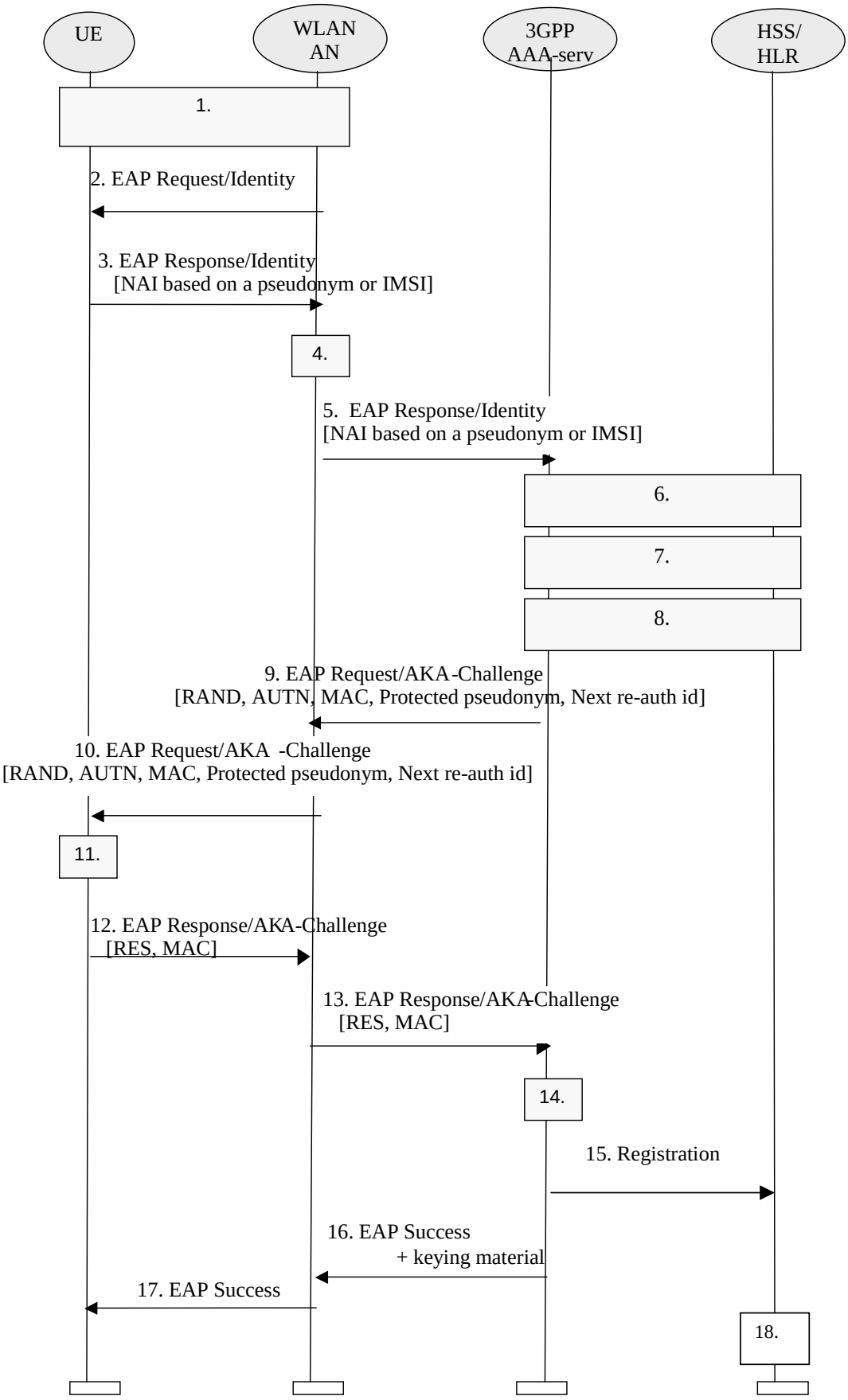


Figure 4: Authentication based on EAP AKA scheme

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. 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 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 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.

12. 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.

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. 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 15).

15. 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~~register to~~ the HSS for a decision. The AAA server shall ~~also~~ 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.

16. 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.~~17. 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.

18. 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.

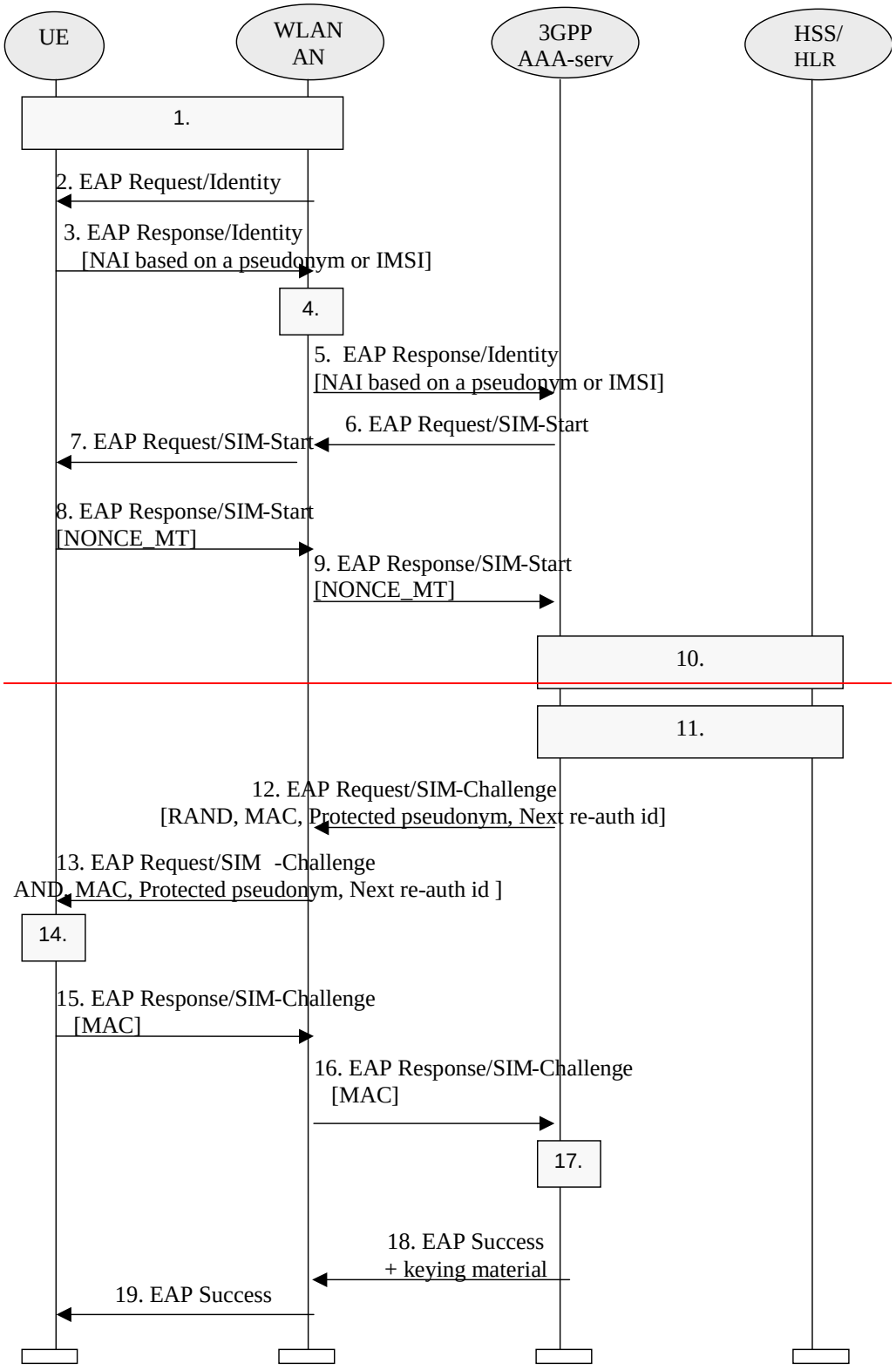
6.1.2 GSM SIM based WLAN Access authentication

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.



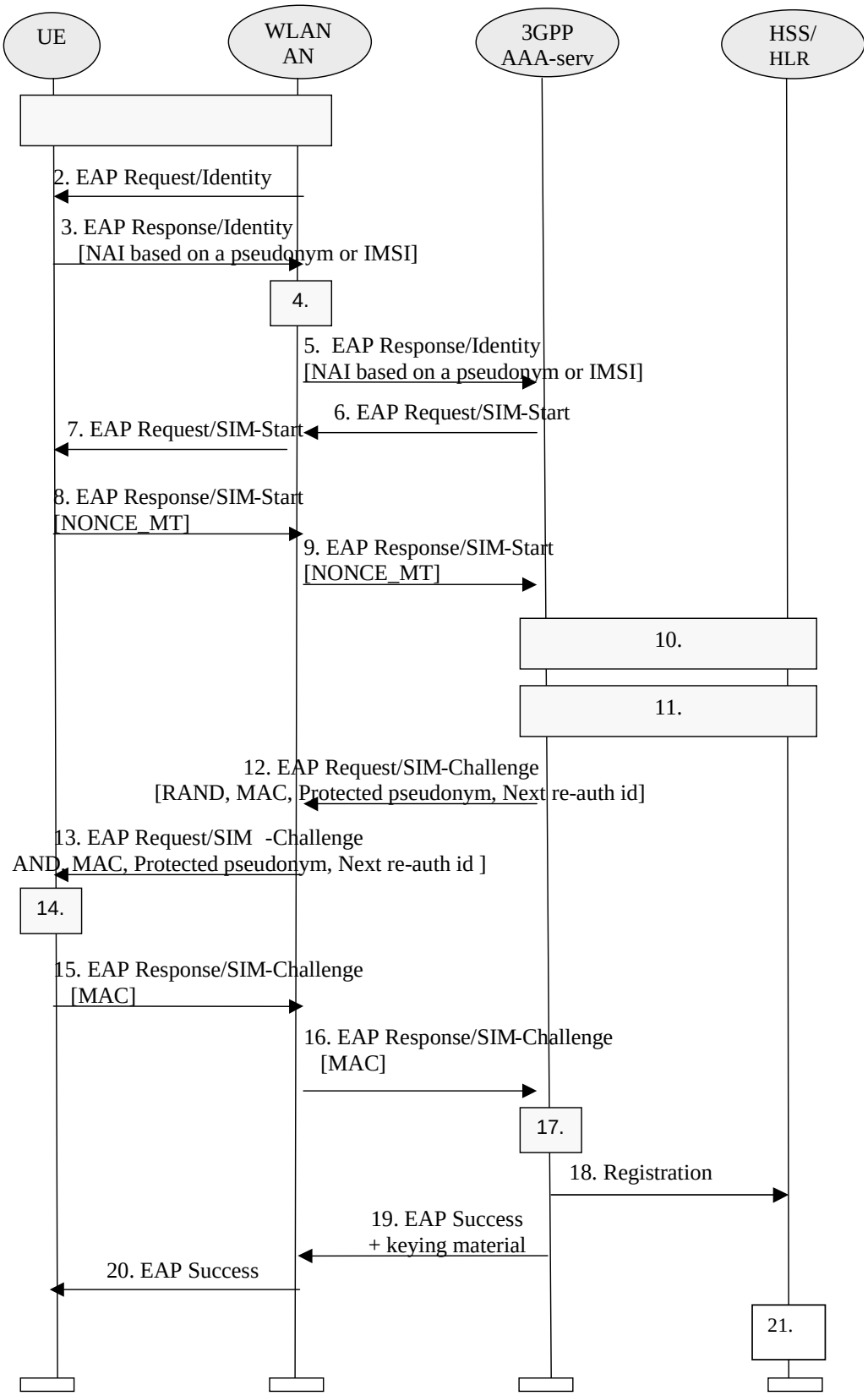


Figure 5: Authentication based on EAP SIM scheme

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.

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

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

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

21. 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.

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

CR-Form-v7

CHANGE REQUEST

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

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: | UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Modification of mechanism to restrict simultaneous WLAN sessions
Source:	⌘	Huawei
Work item code:	⌘	WLAN-3G interworking security
Date:	⌘	07/07/2004
Category:	⌘	**C**
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:	⌘	The current TS included a restriction mechanismthat requests that the 3GPP AAA server should report to the HSS whenever multiple WLAN Access sessions are detected. To avoid load on the HSS/HLR, it is preferable for the 3GPP AAA server itself to terminate the old session.
Summary of change:	⌘	The below changes are added: 1. a mechanism to avoid the WLAN-UE connecting to multiple AAA servers in step 6 (6.1.1.1) and step 10 (6.1.2.1) 2. remove the step15 (6.1.1.1), step18 (6.1.2.1) and change the last steps, so that the AAA need not inform the HSS/HLR after it has detected multiple WLAN Access sessions, but instead the AAA teminates the unallowed multiple sessions by itself. 3. according to an SA2 decision, the term “scenario2” is replaced with the proper wording.
Consequences if not approved:	⌘	Unnecessary heavy burden to the HSS/HLR for 3GPP-WLAN interworking for WLAN Access Authentication. Obsoleted term used in the TS.

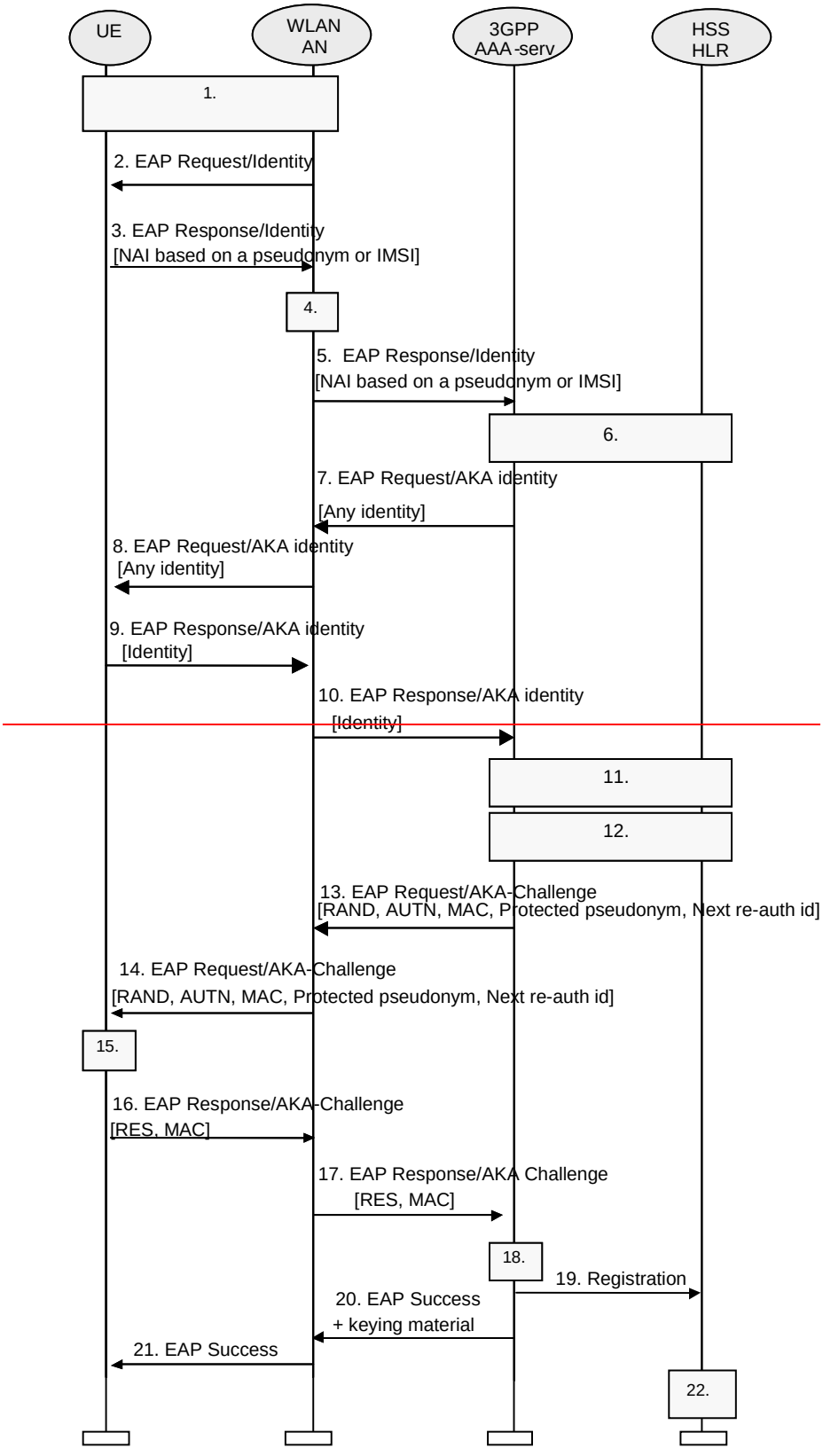
Clauses affected:	⌘	6.1.1.1, 6.1.2.1

Other specs affected:	⌘	Y	N			
		X		Other core specifications	⌘	23.234, 29.234
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

6.1.1.1 EAP/AKA Procedure

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



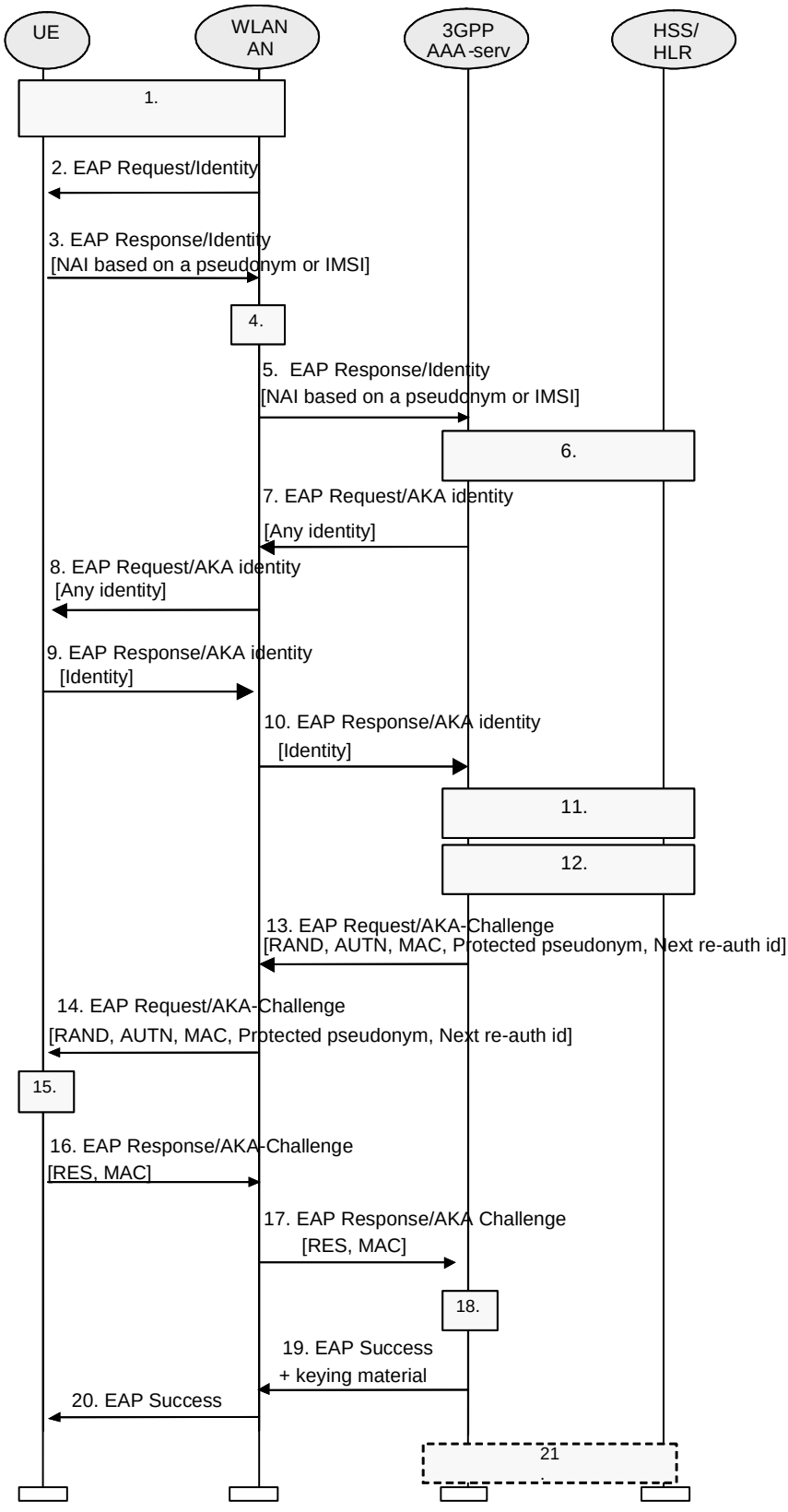


Figure 4: Authentication based on EAP AKA scheme

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

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

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

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

NOTE 1: Generating an identity conforming to NAI format from IMSI is defined in EAP/AKA [4].

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

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

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

6. 3GPP AAA Server identifies the subscriber as a candidate for authentication with EAP-AKA, based on the received identity. The 3GPP AAA Server then checks that it has an unused authentication vector available for that subscriber . If not, a set of new authentication vectors is retrieved from HSS/HLR. A mapping from the temporary identifier to the IMSI may be required.

   The HSS/HLR shall check if there is a 3GPP AAA server already registered to serve for this subscriber In case the HSS/HLR detects that another 3GPP AAA server has already registered for this subscriber, it shall provide the current 3GPP AAA server with the previously registered AAA server address. The authentication signalling is then routed to the previously registered 3GPP AAA server with Diameter-specific mechanisms, e.g., the current 3GPP AAA server transfers the previously registered AAA server address to the AAA proxy or the WLAN AN, or the current 3GPP AAA server acts as a AAA proxy and forwards the authentication message to the previously registered 3GPP AAA server.

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

7. The 3GPP AAA server requests again the user identity, using the EAP Request/AKA Identity message. This identity request is performed as the intermediate nodes may have changed or replaced the user identity received in the EAP Response Identity message, as specified in ref. [4]. However, this new request of the user identity can be omitted by the home operator if there exist the certainty that the user identity could not be changed or modifies by any means in the EAP Response Identity message.

8. The WLAN AN forwards the EAP Request/AKA Identity message to the WLAN UE.

9. The WLAN UE responds with the same identity it used in the EAP Response Identity message.

10. The WLAN AN forwards the EAP Response/AKA Identity to the 3GPP AAA server. The identity received in this message will be used by the 3GPP AAA server in the rest of the authentication process. If an inconsistency is found between the identities received in the two messages (EAP Response Identity and EAP Response/AKA Identity) so that the user profile and authentication vectors previously retrieved from HSS/HLR are not valid, these data shall be requested again to HSS/HLR (step 6shall be repeated before continuing with step 11).

NOTE 4: In order to optimise performance, the identity re-request process (the latter four steps) should be performed when the 3GPP AAA server has enough information to identify the user as an EAP-AKA user, and before user profile and authentication vectors retrieval, although protocol design in Wx interface may not allow to perform these four steps until the whole user profile has been downloaded to the 3GPP AAA server.

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

Although this step is presented after step 6 in this example, it could be performed at some other point, however before step 14. (This will be specified as part of the Wx interface.)

12. New keying material is derived from IK and CK., cf. [4]. This keying material is required by EAP-AKA, and some extra keying material may also be generated for WLAN technology specific confidentiality and/or integrity protection.

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

13. 3GPP AAA Server sends RAND, AUTN, a message authentication code (MAC) and two user identities (if they are generated): protected pseudonym and/or re-authentication id to WLAN-AN in EAP Request/AKA-Challenge message. The sending of the re-authentication id depends on 3GPP operator's policies on whether to allow fast re-authentication processes or not. It implies that, at any time, the AAA server decides (based on policies set by the operator) to include the re-authentication id or not, thus allowing or disallowing the triggering of the fast re-authentication process.

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

15. The WLAN-UE runs UMTS algorithm on the USIM. The USIM verifies that AUTN is correct and hereby authenticates the network. If AUTN is incorrect, the terminal rejects the authentication (not shown in this example). If the sequence number is out of synch, terminal initiates a synchronization procedure, c.f. [4]. If AUTN is correct, the USIM computes RES, IK and CK.

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

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

16. The WLAN UE calculates a new MAC value covering the EAP message with the new keying material. WLAN-UE sends EAP Response/AKA-Challenge containing calculated RES and the new calculated MAC value to WLAN-AN.

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

18. The 3GPP AAA Server checks the received MAC and compares XRES to the received RES. ~~If successful, the AAA server shall compare the MAC address, VPLMN Identity and the WLAN radio network information of the authentication exchange with the same information of the ongoing sessions. If the information is the same as with an ongoing session, then the authentication exchange is related to the ongoing session, so there is no need to do anything for the old sessions (skip step 19)~~.

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

~~20~~19. If all checks in step 18 are successful, then the 3GPP AAA Server sends the EAP Success message to the WLAN-AN. If some extra keying material was generated for WLAN technology specific confidentiality and/or integrity protection then the 3GPP AAA Server includes this keying material in the underlying AAA protocol message (i.e. not at the EAP level). The WLAN-AN stores the keying material to be used in communication with the authenticated WLAN-UE.

~~21~~20. The WLAN-AN informs the WLAN-UE about the successful authentication with the EAP Success message. Now the EAP ~~-~~AKA exchange has been successfully completed~~,~~ and the WLAN-UE and the WLAN-AN share keying material derived during that exchange.

~~22~~21. If there is no other ongoing WLAN Access session for the subscriber detected by the 3GPP AAA server, and the WLAN registration for this subscriber is not performed previously, then the 3GPP AAA server shall initiate the WLAN registration to the HSS/HLR. Otherwise, the AAA server shall compare the MAC address, VPLMN Identity and the WLAN access network information of the authentication exchange with the same information of the ongoing sessions. If the information is the same as with an ongoing session, then the authentication exchange is related to the ongoing session, so there is no need to do anything for old sessions. If it is the same subscriber but with a different MAC address, or with a different VPLMN identity or ~~the~~ with different radio network information that is received than in any ongoing session, ~~then the registration is related to~~

~~a new scenario 2 session. The HSS shall close an old scenario 2 session by indicating to the 3GPP AAA server of the old session to terminate the session,~~ the 3GPP AAA server then considers that the authentication exchange is related to a new WLAN Access session. It shall terminate an old WLAN Access session after the successful authentication of the new WLAN Access session, based on the policy whether simultaneous sessions are not allowed, or whether the number of allowed sessions has been exceeded.

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

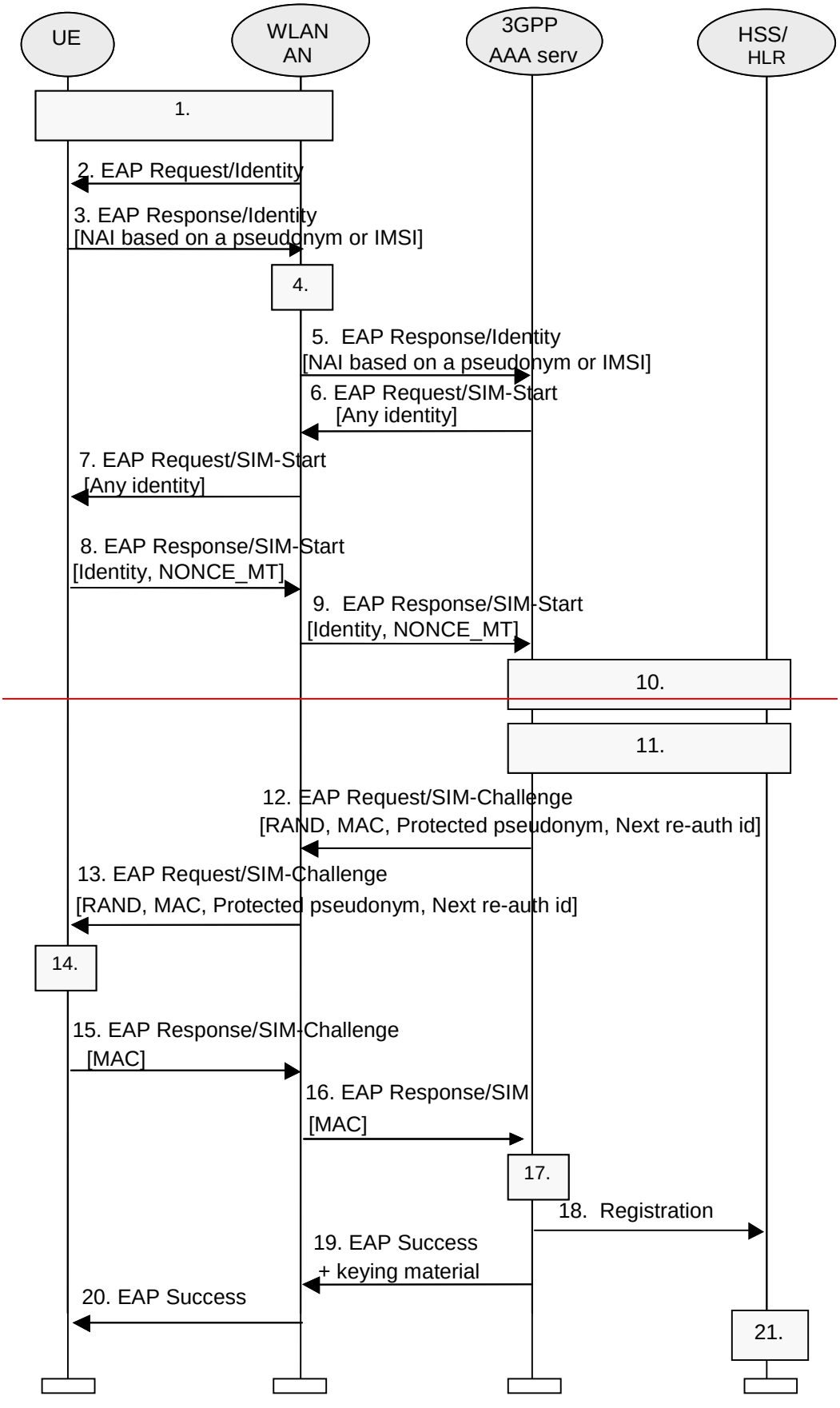
6.1.2 GSM SIM based WLAN Access authentication

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

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

6.1.2.1 EAP SIM procedure

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



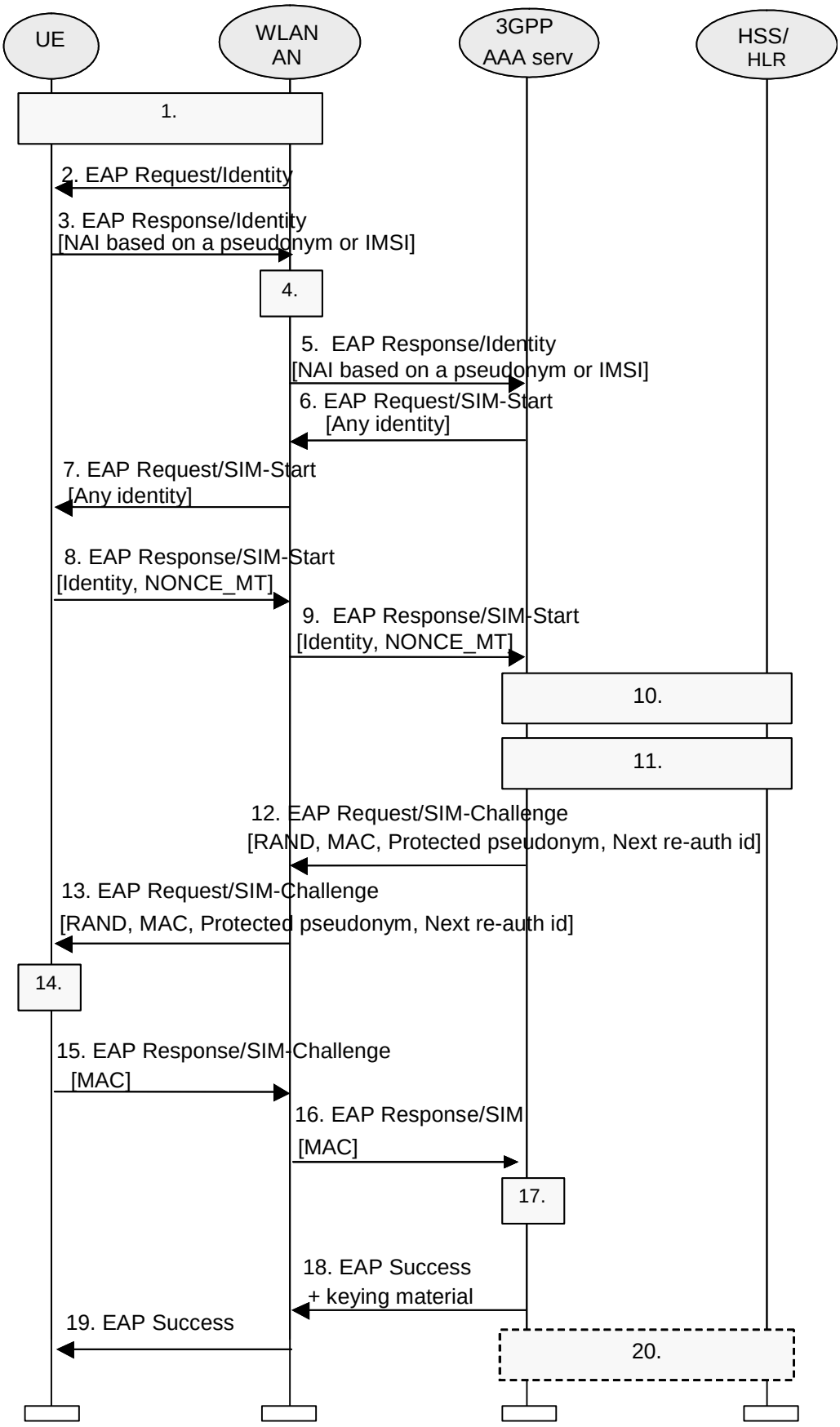


Figure 5: Authentication based on EAP SIM scheme

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    The HSS/HLR shall check if there is a 3GPP AAA server already registered to serve for this subscriber. In case the HSS/HLR detects that another 3GPP AAA server has already registered for this subscriber, it shall provide the current 3GPP AAA server with the previously registered AAA server address. The authentication signalling is then routed to the previously registered 3GPP AAA server with Diameter-specific mechanisms, e.g., the current 3GPP AAA server transfers the previously registered AAA server address to the AAA proxy or the WLAN AN, or the current 3GPP AAA server acts as a AAA proxy and forwards the authentication message to the previously registered 3GPP AAA server.

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

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

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

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

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

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

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

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

    This computing gives N SRES and Kc values.

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

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

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

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

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

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

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

~~18. Otherwise, the AAA server considers that the authentication exchange is related to a new scenario 2 session. In this case the AAA server shall contact the HSS/HLR for a decision. The AAA server shall inform the HSS/HLR of the WLAN-UE's MAC address, the VPLMN Identity, as well as the identifier of the WLAN radio network used.~~

~~19~~18. If the comparison in step 17 is successful, then 3GPP AAA Server sends the EAP Success message to WLAN-AN. If some extra keying material was generated for WLAN technology specific confidentiality and/or integrity protection, then the 3GPP AAA Server includes this derived keying material in the underlying AAA protocol message. (i.e., not at EAP level). The WLAN-AN stores the keying material to be used in communication with the authenticated WLAN-UE.

~~20~~19. WLAN-AN informs the WLAN-UE about the successful authentication with the EAP Success message. Now the EAP SIM exchange has been successfully completed, and the WLAN-UE and the WLAN_AN may share keying material derived during that exchange.

~~21~~20. If there is no other ongoing WLAN Access session for the subscriber detected by the 3GPP AAA server, and the WLAN registration for this subscriber is not performed previously, then the 3GPP AAA server shall initiate the WLAN registration to the HSS/HLR.

Otherwise, the AAA server shall compare the MAC address, VPLMN Identity and the WLAN access network information of the authentication exchange with the same information of the ongoing sessions. If the information is the same as with an ongoing session, then the authentication exchange is related to the ongoing session, so there is no need to do anything for old sessions. If it is the same subscriber but with a different MAC address, or with a different VPLMN identity, or with different~~the~~ radio network information that is received than in any ongoing session, ~~then the registration is related to a new scenario 2 session. The HSS/HLR shall close an old scenario 2 session by indicating to the 3GPP AAA server of the old session to terminate the session,~~ , the 3GPP AAA server then considers that the authentication exchange is related to a new WLAN Access session. It shall terminate an old WLAN Access session after the successful authentication of the new WLAN Access session, based on whether simultaneous sessions are not allowed, or whether the number of allowed sessions has been exceeded.

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

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