

Technical Specification Group Services and System Aspects TSGS#27(05)0108
Meeting #27, 14 - 17 March 2005, Tokyo, Japan

Source: TSG SA WG2
Title: CR(s) to 23.234
Agenda item: 7.2.3
Document for: APPROVAL

XXX

S2 Tdoc	Title	Spec	CR	Rev	Cat	C_Ver	Rel	WI
S2-050053	Removal of Obsolete Annexes	23.234	116	1	F	6.3.0	Rel-6	WLAN
S2-050052	Charging in WAG	23.234	117	1	F	6.3.0	Rel-6	WLAN
S2-050060	Correction of Requirements for 3GPP PS based services	23.234	118	1	F	6.3.0	Rel-6	WLAN
S2-050051	Parameter storage for I-WLAN	23.234	120		F	6.3.0	Rel-6	WLAN
S2-050432	Add the functionality of subscriber profile updating description	23.234	121	2	F	6.3.0	Rel 6	WLAN

CHANGE REQUEST

23.234 CR 116 rev 1 Current version: 6.3.0

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:	Removal of Obsolete Annexes		
Source:	3GPP TSG_SA WG2		
Work item code:	WLAN	Date:	27/01/2005
Category:	F	Release:	Rel-6
Use <u>one</u> 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 <u>one</u> of the following releases: Ph2 (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) Rel-7 (Release 7)	

Reason for change:	The current version of the TS contains Annexes with obsolete information: <ul style="list-style-type: none"> Annex A is an informative Annex with stage 3 level information. Since the stage 3 specifications are stable there is no need to have this information in the TS anymore. Moreover it contains invalid information, since it has not been updated. Annex E is an informative Annex about the discarded tunnel switching alternative. After stage 3 specifications are stable this Annex does not contain any relevant information to Rel-6 I-WLAN architecture.
Summary of change:	Annex A and E and the references to Annex A are removed.
Consequences if not approved:	The TS will contain irrelevant and invalid information.

Clauses affected:	5.1.2, 6.3.3, Annex A; Annex E										
Other specs affected:	<table border="1" style="border-collapse: collapse;"> <tr> <td style="padding: 2px;">Y</td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	
	Y	N									
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>									
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>										
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>										
<input checked="" type="checkbox"/>	Test specifications										
<input checked="" type="checkbox"/>	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.

****** Start of first set of changes ******

5.1.2 Existing 3GPP Element Impacts

The following requirements should be satisfied by the 3GPP-WLAN Interworking System function with regard to existing 3GPP network elements:

- Existing SIM and USIM shall be supported. Authentication shall rely on (U)SIM based authentication mechanisms. R6 USIM may include new functionality if necessary e.g. in order to improve privacy.
- Changes in the HSS/HLR/AuC shall be minimized.
- The Service Location Function (SLF) node shall be used in the same way as defined in 3GPP TS 23.228 [24] to find the address of a subscriber's HSS, if necessary.
- The WLAN connection established for a 3GPP subscriber shall have no impact to the capabilities of having simultaneous PS and CS connections for the same subscriber. (e.g. the HLRSS shall not deregister a PS subscriber when the UE registers on a WLAN)
- This TS proposes solutions for operators who want to interwork their WLAN with an existing pre-R6 HLR/HSS.
~~Please refer to Annex A.~~

****** End of first set of changes ******

****** Start of 2nd set of changes ******

6.3.3 D'/Gr' reference point

This optional reference point is located between 3GPP AAA Server and pre-R6 HLR/HSS. The prime purpose of the protocol(s) crossing this reference point is communication between WLAN AAA infrastructure and HLR. The protocol crossing this reference point is based upon the D/Gr reference points defined in 3GPP TS 29.002 [10]. Support of the D'/Gr' reference points requires no modifications to the MAP protocol at the HLR.

When the HLR makes it possible the functionality of the reference point is to enable:

- Retrieval of authentication vectors, e.g. for USIM authentication, from HLR.
- Registration of the 3GPP AAA Server of an authorised WLAN user in the HLR.
- Indication of change of subscriber profile within HLR (e.g. indication for the purpose of service termination).
- Purge procedure between the 3GPP AAA server and the HLR.
- Fault recovery procedure between the HLR and the 3GPP AAA server.
- Retrieval of service related information (e.g. APNs that may be selected by the WLAN UE) including indications of whether the service is to be supported by the HPLMN or by an identified VPLMN.
- Retrieval of online/offline charging function address from HLR.

The functions provided on the D'/Gr' reference points are a subset of the functions provided on the D/Gr reference points described in 3GPP TS 29.002 [10].

If a 3GPP AAA Server supports the D' reference point, it will appear to the HLR/HSS as a VLR and shall behave according to the description of the behaviour of a VLR supporting the D reference point as described in 3GPP TS 29.002 [10].

If a 3GPP AAA Server supports the Gr' reference point, it will appear to the HLR/HSS as an SGSN and shall behave according to the description of the behaviour of an SGSN supporting the Gr reference point as described in 3GPP TS 29.002 [10].

~~Please refer to Annex A for further details of how this may work for different network scenarios.~~

****** End of 2nd set of changes ******

****** Start of 3rd set of changes ******

Annex A (informative):

Void~~Reference Points Signalling Flows~~

Editor's Note: In this annex, references to Diameter should be considered as informative examples.

~~A.1 Signalling Sequences examples for Wa Reference Point~~

~~A.1.1 Authentication, Authorisation and Session Key delivery~~

~~The purpose of this signalling sequence is to carry WLAN UE 3GPP AAA Server authentication and authorisation signalling over the Wa reference point. As a result of a successful authentication, authorisation information and session keying material for the authenticated session is delivered from the 3GPP AAA Server to the WLAN.~~

~~This Wa signalling sequence is initiated by the WLAN when authentication and authorisation of a WLAN UE is needed. This can take place when a new WLAN UE accesses WLAN, when a WLAN UE switches between WLAN APs or when a periodic re-authentication is performed.~~

~~The signalling sequence shown is based on Diameter. For signalling to WLANs using RADIUS the conversion defined in Diameter specification shall be used.~~

~~-~~

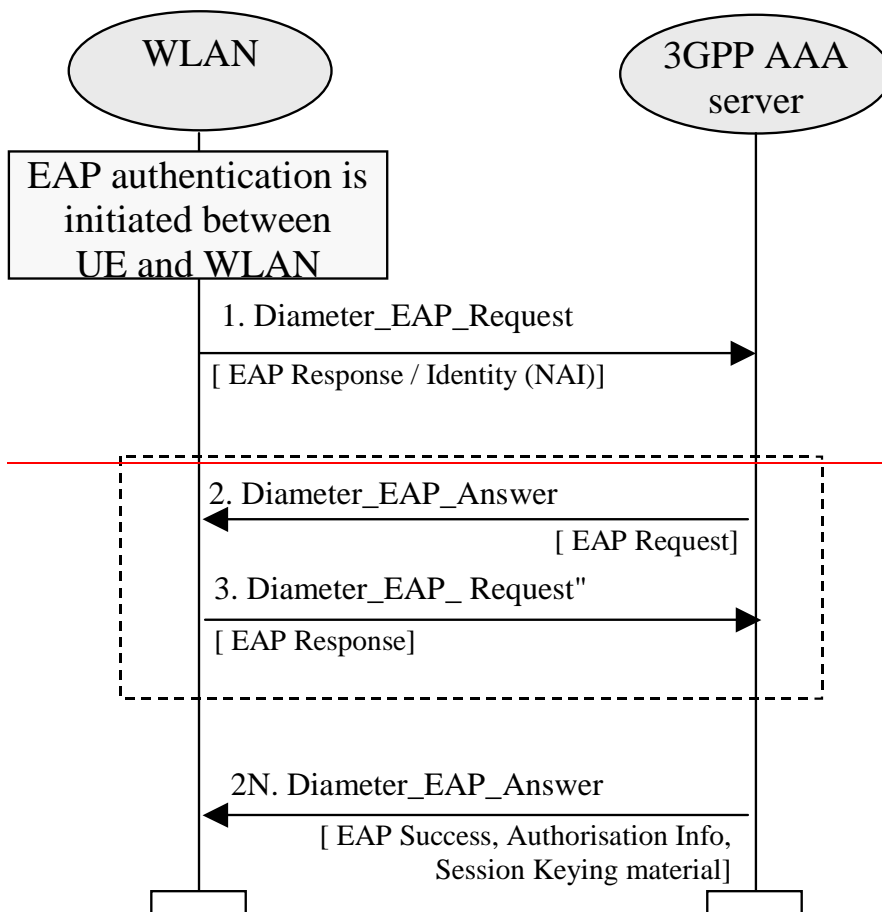


Figure A.1.1: Signalling example on Wa Reference Point for Authentication and Authorisation

1. The WLAN initiates authentication procedure towards 3GPP network by sending Diameter_EAP_Request message to 3GPP AAA Server. This Diameter message carries encapsulated EAP Response/Identity message to 3GPP AAA Server. This message also carries a Session ID used to identify the session within the WLAN and optionally a well defined identification of the WLAN AN (e.g. transported in the NAS Identifier parameter).
2. 3GPP AAA Server performs the authentication procedure based on information retrieved from HSS/HLR. 3GPP AAA Server sends message Diameter_EAP_Answer to WLAN. This message carries encapsulated EAP Request message. The content of the EAP Request message is dependent on the EAP type being used. WLAN conveys the EAP Request message to the WLAN UE.
3. WLAN UE responds to WLAN by a EAP Response message. WLAN encapsulates it into Diameter_EAP_Request message and sends it to 3GPP AAA Server. The contents of the EAP Response message is dependent on the EAP type being used.

The number of roundtrip Diameter signalling exchanges similar to the signal pair 2 and 3 is dependent e.g. on the EAP type being used.

- 2N When 3GPP AAA server has successfully authenticated and authorised the 3GPP subscriber, the 3GPP AAA Server sends final Diameter_EAP_Answer message carrying encapsulated EAP Success message to WLAN. WLAN forwards the EAP Success message to the WLAN UE.

— This Diameter_EAP_Answer message also carries the authorisation information (e.g. NAS Filter Rule or Tunneling attributes) for the authenticated session. Message also carries the keying material from 3GPP AAA Server to WLAN to be used for the authenticated session by WLAN.

A.1.2 Immediate purging of a user from the WLAN access

The purpose of this signalling sequence is to indicate to the WLAN that a specific WLAN UE shall be disconnected from accessing the WLAN interworking service.

This signalling sequence is initiated by the 3GPP AAA Server when a WLAN UE needs to be disconnected from accessing WLAN interworking service. For example, a WLAN UE used by a 3GPP subscriber may need to be disconnected when the 3GPP subscriber's subscription is cancelled or when the 3GPP subscriber's online charging account expires.

The signalling sequence shown is based on Diameter. For signalling to WLANs using RADIUS the conversion defined in Diameter specification shall be used.

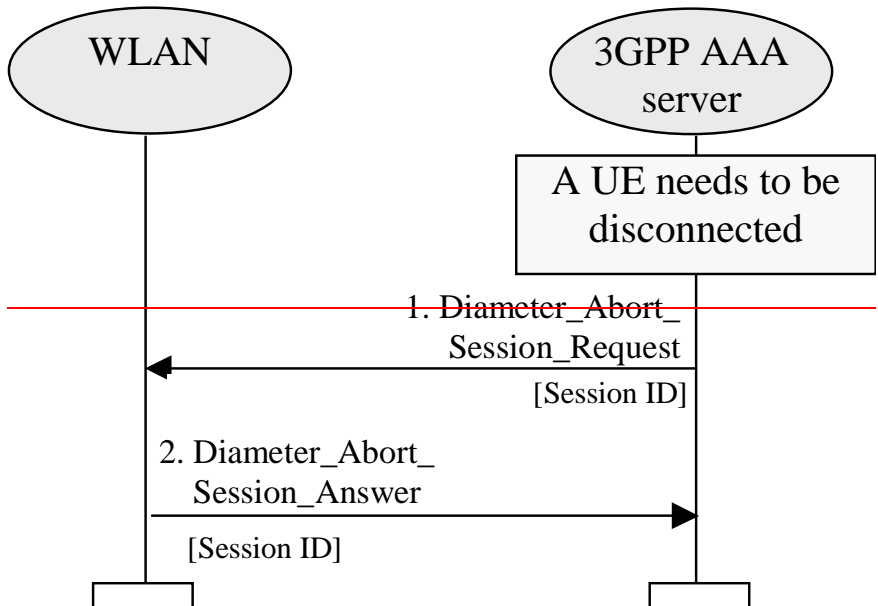


Figure A.1.2: Signalling example on Wa Reference Point for User Purging

1. When 3GPP AAA Server needs to disconnect (e.g. after receiving an external trigger) a 3GPP subscriber from the WLAN access service, the 3GPP AAA Server sends a Diameter_Abort_Session_Request to WLAN. This message contains the Session ID by which the session is identified within WLAN.
2. WLAN responds by Diameter_Abort_Session_Answer as defined in Diameter.

A.2 Signalling Sequences examples for Wx Reference Point

A.2.1 Authentication Information Retrieval

This signalling sequence is initiated by a 3GPP AAA Server when a new set of authentication information for a given subscriber is to be retrieved from an HSS/HLR.

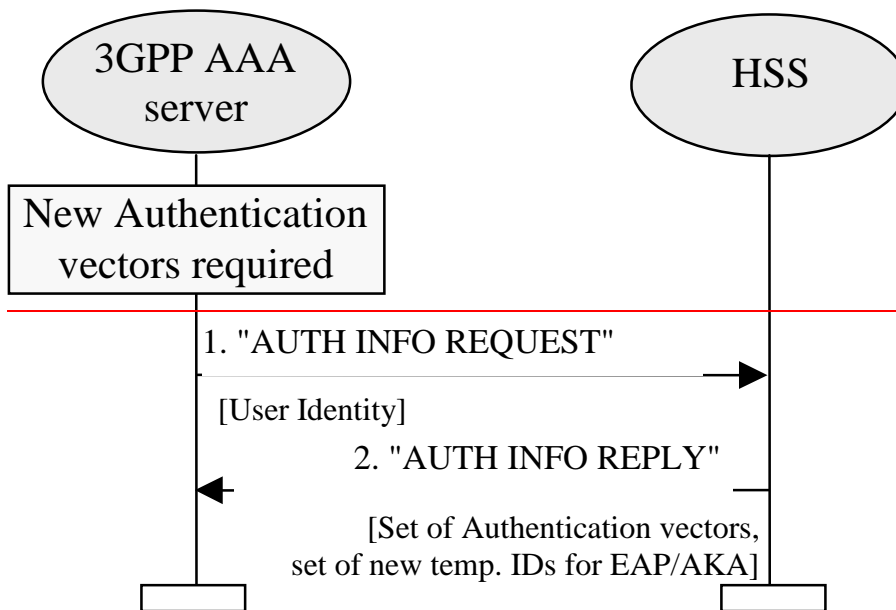


Figure A.2.1 Signalling example on Wx Reference Point for Authentication Information Retrieval

1. 3GPP AAA server detects that it requires new authentication vectors for a given 3GPP subscriber. This can happen for example, when a new 3GPP subscriber has accessed 3GPP AAA Server for authentication or when a new set of authentication information is required for one of the 3GPP subscribers already registered in the 3GPP AAA server.

— 3GPP AAA server sends "AUTH INFO REQUEST" message to the HSS/HLR requesting a set of authentication vectors. In the message the subscriber is identified by the IMSI, which is derived by the 3GPP AAA server from the username part of the NAI

Editor's Note: For USIM authentication (EAP/AKA) it is ffs whether the temporary identifiers should instead of HSS/HLR be allocated in the 3GPP AAA Server, i.e. whether IMSI or Temporary identifier Is used as user identity over Wx.

2. HSS/HLR replies by a "AUTH INFO REPLY" message containing the requested authentication vectors.

— For USIM authentication (EAP/AKA) HSS/HLR has also allocated a new set of pseudonyms for the subscriber to be given to the subscriber in each subsequent authentication.

Editor's Note: It is ffs whether the temporary identifiers should instead of HSS/HLR be allocated in the 3GPP AAA Server

— In case of UMTS AKA authentication, each authentication vector consists of RAND, XRES, AUTN, CK, and IK.

— 3GPP AAA Server stores the authentication vectors and pseudonyms to be used in future authentication procedures for the subscriber.

A.2.2 Subscriber Profile Retrieval

This signalling sequence is initiated by a 3GPP AAA Server when a new subscriber has accessed the 3GPP AAA server and the subscription profile information of that subscriber is not available in the 3GPP AAA server. This signalling sequence can also be used if for some reason the subscription profile of a subscriber is lost. Subscription profile contains e.g. authorisation information.

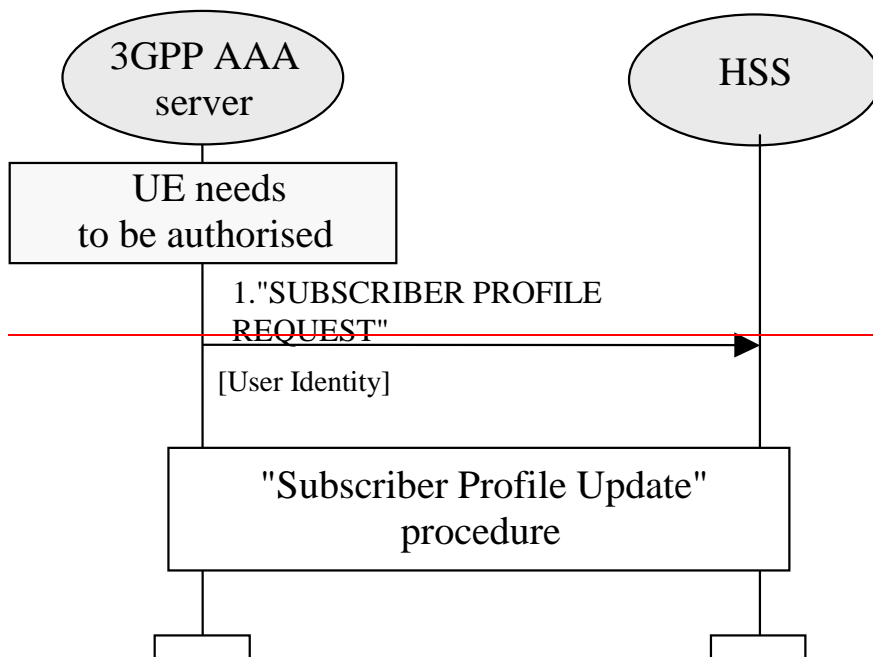


Figure A.2.2: Signalling example on Wx Reference Point for Subscriber Profile Retrieval

1. 3GPP AAA server detects that it requires the subscription profile for a given 3GPP subscriber. For example, this can happen when a new subscriber has accessed the 3GPP AAA Server for authentication.

3GPP AAA server sends "SUBSCRIBER PROFILE REQUEST" message to the HSS/HLR requesting the subscriber's profile to be downloaded to the 3GPP AAA server. In the message the subscriber is identified by a unique identifier which is used as the username part of the NAI identity.

In case of USIM authentication (EAP/AKA) the utilised unique identifier shall be the pseudonym (associated with the IMSI) allocated in the previous authentication or, in case of the very first authentication, the IMSI.

Editor's Note : it is ffs whether the temporary identifiers should instead of HSS/HLR be allocated in the 3GPP AAA Server, i.e. whether IMSI or Temporary identifier Is used as user identity over Wx.

2. At reception of "SUBSCRIBER PROFILE REQUEST" message, the HSS/HLR initiates a Subscriber Profile Update procedure towards the 3GPP AAA Server. The Subscriber Profile Update procedure is explained in the following clause.

A.2.3 Subscriber Profile Update

This signalling sequence is initiated by the HSS/HLR when subscriber profile needs to be sent to a 3GPP AAA server. This can be due to an explicit request from the 3GPP AAA Server or due to a modification or cancellation of subscription in the HSS/HLR.

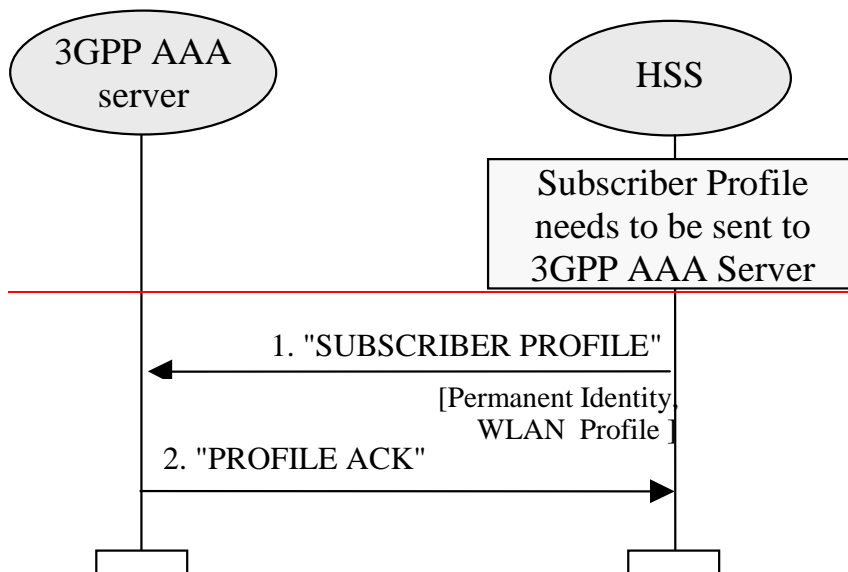


Figure A.2.3: Signalling example on Wx Reference Point for Subscriber Profile Update

1. HSS/HLR initiates the signalling when a subscriber profile needs to be sent to a 3GPP AAA server. This can be due to an explicit request from the 3GPP AAA Server or due to a modification or cancellation of subscription in the HSS/HLR.
 - HSS/HLR sends "SUBSCRIBER PROFILE" message to 3GPP AAA Server. For example, this message includes
 - Users permanent unique identifier. In case of USIM authentication (EAP/AKA) the utilised unique identifier shall be the IMSI
 - service authorisation information;
 - charging mechanism (offline / online);
 - in case of online charging the DNS name of the subscribers online charging system
 3GPP AAA Server stores the subscriber profile information.
2. 3GPP AAA Server acknowledges the reception of the subscriber profile information by sending "PROFILE ACK" message to the HSS/HLR.

A.2.4 WLAN Registration

This signalling sequence is initiated by the 3GPP AAA Server when a new subscriber has been authenticated and authorised by the 3GPP AAA server. The purpose of this procedure is to register the current 3GPP AAA Server address in the HSS/HLR.

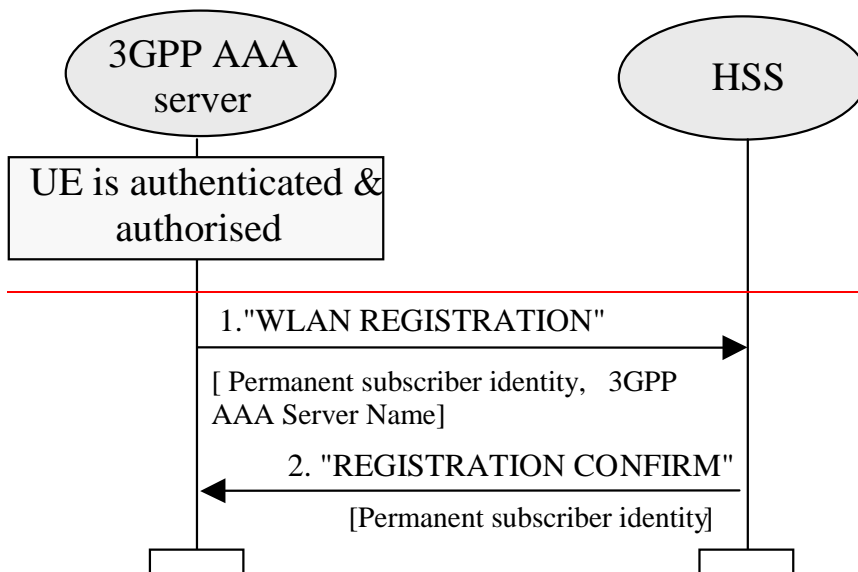


Figure A.2.4: Signalling example on Wx Reference Point for Subscriber Registration

1. 3GPP AAA server initiates the signalling when a new 3GPP subscriber has been authenticated and authorised by the 3GPP AAA server. 3GPP AAA server sends WLAN REGISTRATION message to the HSS/HLR. This message contains the address/name of the 3GPP AAA Server and the permanent subscriber identifier. In case of USIM authentication (EAP/AKA) the unique identifier shall be the IMSI.
2. HSS/HLR confirms the reception of the WLAN REGISTRATION message by REGISTRATION CONFIRM message.

A.2.5 Cancel Registration

This signalling sequence is initiated by a HSS when subscription has to be removed from 3GPP AAA Server. This can happen when the subscription is cancelled in HSS.

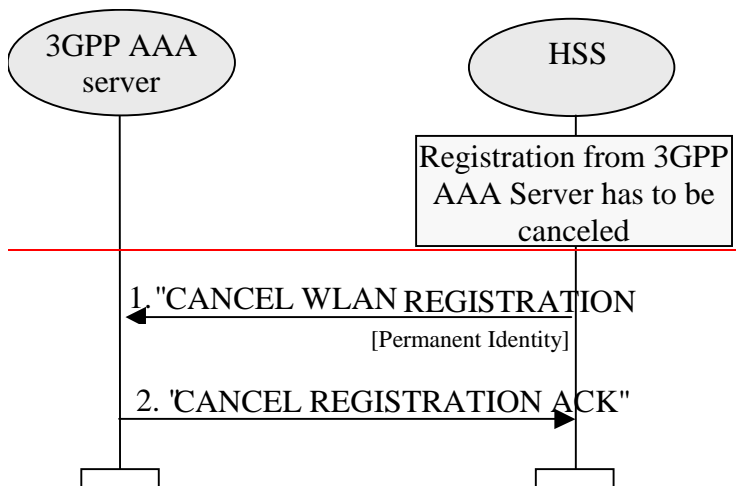


Figure A.2.5: Signalling example on Wx Reference Point for Registration Cancellation

1. HSS/HLR initiates the signalling when the registration of a 3GPP subscriber has to be cancelled from a 3GPP AAA server. Subscriber is identified by his permanent user identity.
2. 3GPP AAA Server confirms the reception of the CANCEL WLAN REGISTRATION message by CANCEL REGISTRATION ACK message.

A.2.6 Purge Function for WLAN interworking

The Purge function allows a 3GPP AAA server to inform the HSS that it has deleted the information of a disconnected (either logged off or exceptionally disconnected from the WLAN interworking service) subscriber. The 3GPP AAA server may, as an implementation option, delete the information of a subscriber immediately after the implicit or explicit logging off of the subscriber. Alternatively, the 3GPP AAA server may keep the information of the disconnected subscriber for some time, such as the subscriber profile and the authentication information retrieved from the HSS, so that the information can be reused at a later connection period without accessing the HSS.

When the 3GPP AAA server deletes the information of a subscriber, it shall initiate the Purge procedure as illustrated in the following figure. Each step is explained in the following.

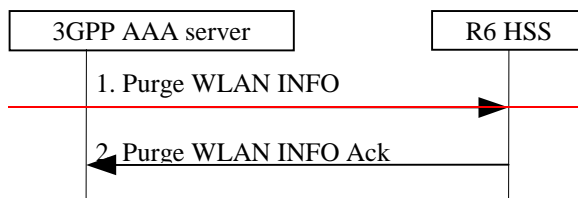


Figure A.2.6: Signalling example on Wx Reference Point for Purge Procedure

- 1) After deleting the information of a disconnected subscriber, the 3GPP AAA server sends a Purge WLAN INFO message to the HSS.
- 2) The HSS record a "WLAN INFO Purged" value and acknowledges with a Purge WLAN INFO Ack message.

A.3 Signalling Sequences examples for D' Reference Point

A.3.1 Authentication Information Retrieval

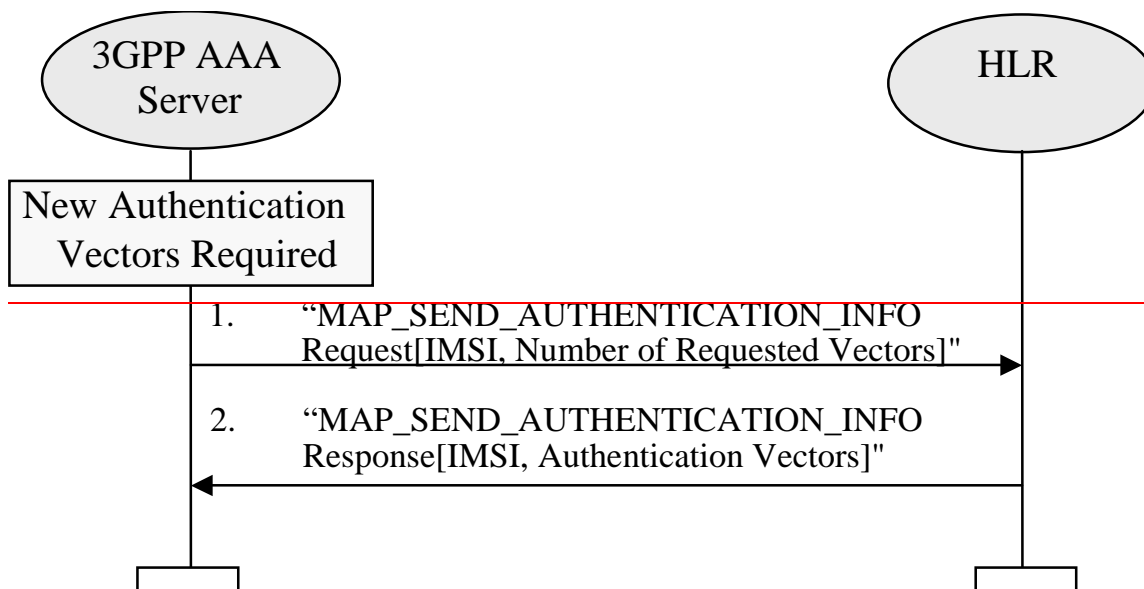


Figure A.3.1: Authentication Information Retrieval using D' interface

1. 3GPP AAA server detects that it requires new authentication vectors for a given 3GPP subscriber. This can happen for example, when a new 3GPP subscriber has accessed 3GPP AAA Server for authentication or when a new set of authentication information is required for one of the 3GPP subscribers already registered in the 3GPP AAA server.
- 3GPP AAA server sends "MAP_SEND_AUTHENTICATION_INFO Request" message to the HSS/HLR requesting a set of authentication vectors. In the message, the subscriber is identified by a unique identifier, IMSI.

- 2. HSS/HLR replies by a "MAP_SEND_AUTHENTICATION_INFO Response" message containing the requested authentication vectors.
- In case of UMTS AKA authentication, each authentication vector consists of RAND, XRES, AUTN, CK, and IK.

A.3.2 Subscriber Profile Retrieval

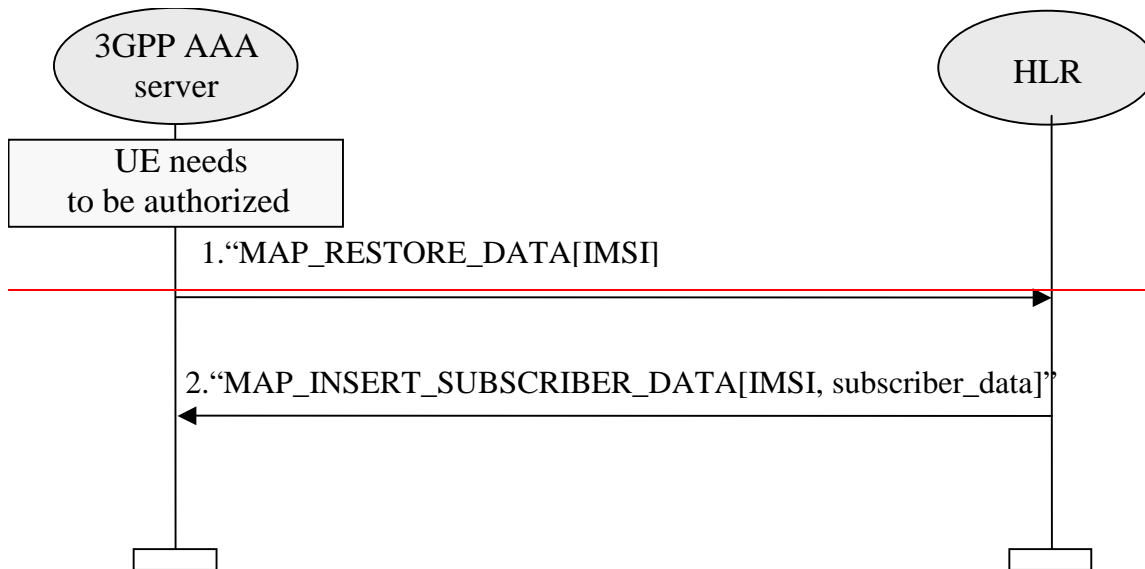


Figure A.3.2: Subscriber Profile Retrieval using D' interface

- 1. 3GPP AAA server detects that it requires the subscription profile for a given 3GPP subscriber. For example, this can happen when a new subscriber has accessed the 3GPP AAA Server for authentication.
- 3GPP AAA server sends "MAP_RESTORE_DATA" message to the HSS/HLR requesting the subscriber's profile to be downloaded to the 3GPP AAA server. In the message the subscriber is identified by IMSI.
- 2. At reception of "MAP_RESTORE_DATA" message, the HSS/HLR initiates a MAP_INSERT_SUBSCRIBER_DATA procedure towards the 3GPP AAA Server.

Since pre R6 Subscriber Data records in HLR do not have any standardized information related to WLAN subscription, the choice and interpretation of the retrieved data is left up to the operator.

A.4 Gr' Signalling Mechanisms to support WLAN service

A.4.1 Introduction

The following sections describe the use of existing GPRS parameters and signalling mechanisms to support the WLAN services when interworking with legacy HLRs.

The table shows a list of parameters in existing HLR and suggests possible use in context of WLAN operation. However actual use and interpretation is left to the operator.

Table A.4.1: HLR Parameters and use for WLAN Interworking

Existing GPRS parameter	Possible WLAN use
IMSI	Subscribers Identity
PDP Context subscription record	Services Subscriber has access to
VPLMN Address Allowed	Subscriber's ability to use service while roaming

SGSN Number, SGSN Address	Indicate the serving 3GPP AAA Server
Authentication Vectors	Authentication and ciphering

~~Following procedures are relevant between 3GPP AAA Server and HLR with respect to the information identified above. These messages are exchanged over the Gr' interface:~~

- ~~— Authentication information retrieval via infoRetrieval procedure~~
- ~~— Subscriber Information retrieval via gprsLocationUpdate procedure~~
- ~~— Deletion of subscription via cancellLocation procedure.~~

~~It is important to note that use of gprsLocationUpdate procedure from WLAN will detach the subscriber from GPRS.~~

~~Further proprietary work with possible impact to existing HLR and/or SGSNs is necessary to support simultaneous connections when Gr' signalling is used for WLAN purposes.~~

~~A.4.2 InfoRetrieval procedure:~~

~~Using this procedure the 3GPP AAA server can request for the Authentication Vectors for the user (IMSI) by initiating SEND AUTHENTICATION INFO message to HLR. HLR/AuC validates the user (IMSI) and generates Authentication Vectors and responds back with SEND AUTHENTICATION INFO ACK message that contains the generated Authentication Vectors.~~

~~The infoRetrieval (Authentication) procedure is illustrated in Figure X below.~~

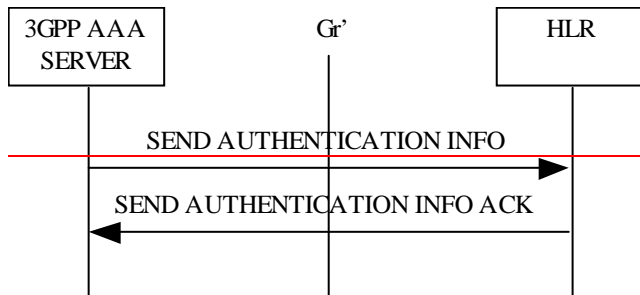


Figure A.4.1: infoRetrieval procedure

~~A.4.2 GprsLocationUpdate procedure:~~

~~Using this procedure the 3GPP AAA server can update the HLR with the local storage area information of the user and request HLR for the subscriber information (services, roaming, etc). 3GPP AAA server initiates this procedure by sending UPDATE LOCATION message with the local storage area information. HLR sends the subscriber information through INSERT SUBSCRIBER DATA, which 3GPP AAA server acknowledges. HLR repeats the above procedure until all the data is sent. On successful completion of above procedure HLR responds with UPDATE LOCATION ACK message.~~

~~The gprsLocationUpdate (Subscriber Information retrieval) procedure is illustrated in Figure X.1 below.~~

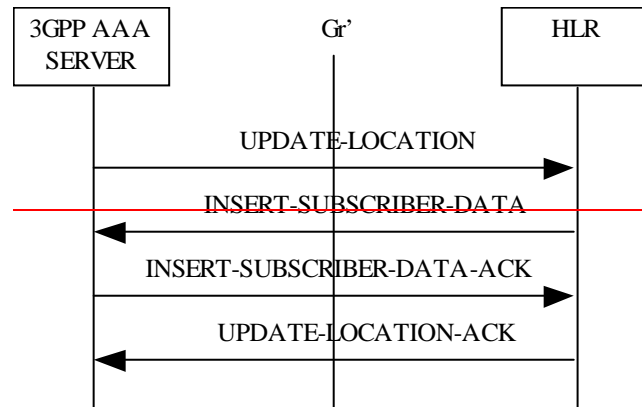


Figure A.4.2: ~~gprsLocationUpdate procedure~~

~~A.5 Example of Authentication procedures~~

~~A.5.1 EAP/AKA Procedure~~

~~USIM based authentication may be based on existing AKA method. In the case of WLAN-3GPP system interworking, this method should be supported by a generic authentication mechanism (independently of the underlying WLAN standard), e.g. EAP. EAP/AKA authentication mechanism is described in Internet Draft draft-arkko-pppext-eap-aka. The current version is 05 (draft-arkko-pppext-eap-aka-05.txt). The following procedure is based on EAP/AKA authentication mechanism:~~

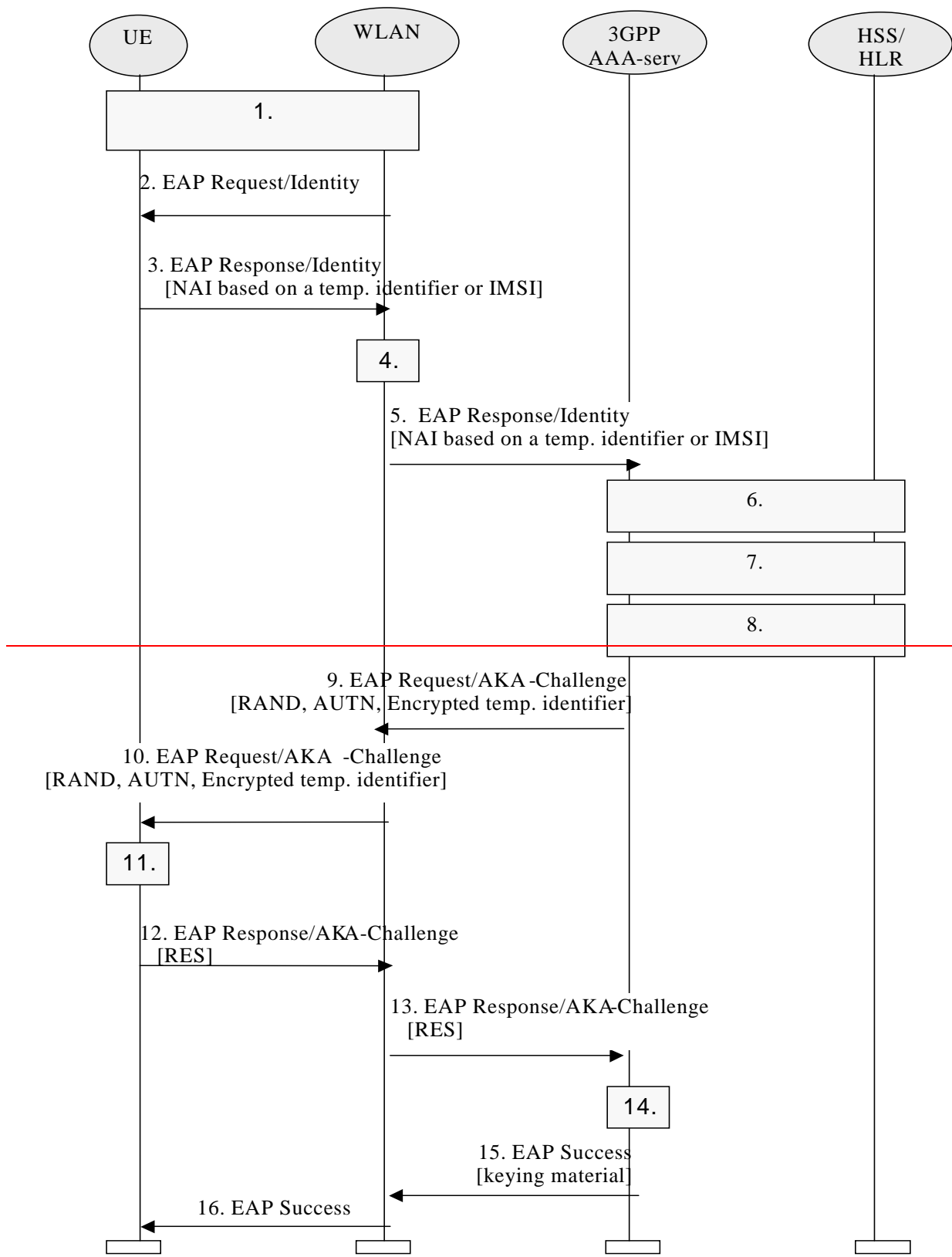


Figure A.5.1: Authentication based on EAP-AAA scheme

1. After WLAN connection establishment, Extensible Authentication Protocol is started with a WLAN technology specific procedure (out of scope for 3GPP).—

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

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

3. The WLAN UE starts EAP AKA authentication procedure by sending an EAP Response/Identity message. The WLAN UE sends its identity complying with Network Access Identifier (NAI) format specified in RFC 2486 [17]. NAI contains the temporary identifier allocated to WLAN UE in previous authentication if available and valid. Otherwise, the NAI shall contain the IMSI.

NOTE 1: generating an identity conforming to NAI format from IMSI is defined in EAP/AKA draft (draft-arkko-pppext-eap-aka-05.txt).

4. The 3GPP AAA Server is chosen based on the NAI.—

NOTE 2: Diameter/RADIUS proxy chaining and/or Diameter referral can 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 checks that it has an authentication vector available (RAND, AUTN, XRES, IK, CK) for the subscriber from previous authentication. If not, a set of authentication quintuplets is retrieved from HSS/HLR. If a temporary identifier is provided, it is mapped to the corresponding IMSI.

7. 3GPP 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 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. The extra keying material is required in order to pass the encrypted and integrity protected temporary identifier to the WLAN UE. The keying material may also be used for WLAN technology specific confidentiality or integrity protection.—

A new temporary identifier is chosen and encrypted. Temporary identifier format is FFS.

9. 3GPP AAA Server sends RAND, AUTN, and encrypted temporary identifier to WLAN in EAP Request/AKA Challenge message.

10. The WLAN 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 (not shown in this example). If AUTN is correct, the USIM computes RES, IK and CK.

WLAN UE derives required additional keying material from IK and CK. WLAN UE decrypts temporary identifier and saves it to be used on next authentication.

12. WLAN UE sends EAP Response/AKA Challenge containing calculated RES to WLAN

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

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

15. If the comparison in step 14 is successful, then 3GPP AAA Server sends the EAP Success message to WLAN. The 3GPP AAA Server includes the derived keying material in the message. WLAN stores the keying material to be used in communication with the authenticated WLAN UE.

16. WLAN 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 share session key material.

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

~~NOTE 4: Temporary identifier is only used for authentication purpose. User identification on the data path is done by the Access Point in a way that is proper to the WLAN.~~

~~A.5.2 — EAP SIM procedure~~

~~SIM based authentication shall be based on existing GSM AKA method but shall include enhancements for network authentication. In the case of WLAN 3GPP system interworking, this method should be supported by a generic authentication mechanism (independently of the underlying WLAN standard), e.g. EAP.~~

~~EAP SIM authentication mechanism is described in Internet Draft draft haverinen_pppext_eapsim. The current version is 06 (draft haverinen_pppext_eap_sim_06.txt).~~

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

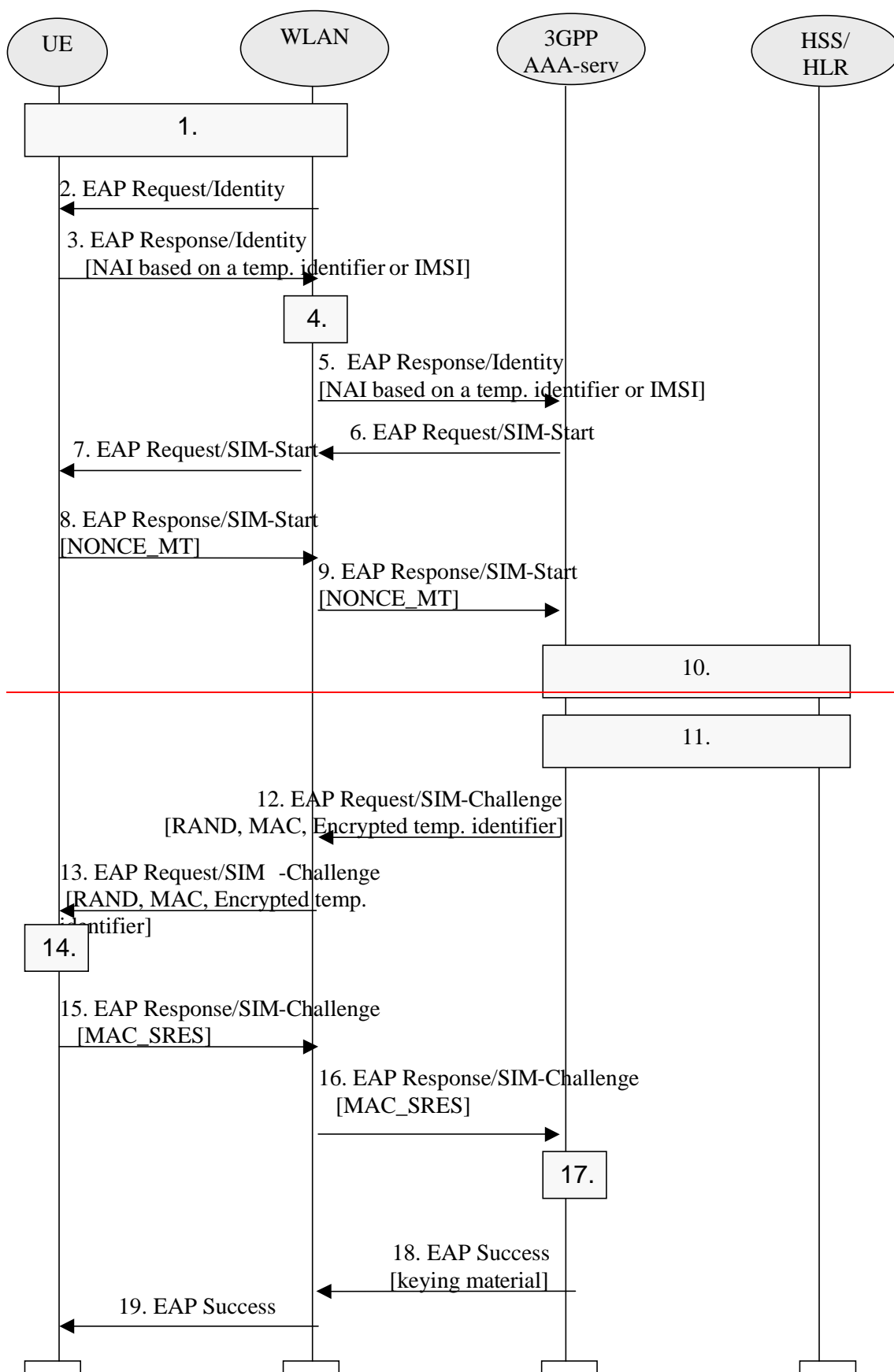


Figure A.5.2: Authentication based on EAP SIM scheme

1. After WLAN connection establishment, Extensible Authentication Protocol is started with a WLAN technology-specific procedure (out of scope for 3GPP).

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

~~EAP packets are transported over the WLAN interface encapsulated within a WLAN technology specific protocol.~~

~~3. The WLAN UE starts EAP-SIM authentication procedure by sending an EAP Response/Identity message. The WLAN UE sends its identity complying to Network Access Identifier (NAI) format specified in RFC 2486. NAI contains the temporary identifier allocated to WLAN UE in previous authentication if available and valid. Otherwise, the NAI shall contain the IMSI.~~

~~NOTE 1: generating an identity conforming to NAI format from IMSI is defined in EAP/SIM (draft-haverinen-pppext-eap-sim-06.txt).~~

~~4. The 3GPP AAA Server is chosen based on the NAI.~~

~~NOTE 2: Diameter/RADIUS proxy chaining and/or Diameter referral can 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 guesses, based on the NAI, that the subscriber is a GSM user; hence it sends the EAP Request/SIM-Start packet to WLAN.~~

~~7. WLAN 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~~

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

~~10. 3GPP AAA Server checks that it has N (usually two or three) available authentication triplets (RAND, SRES, Kc) for the subscriber from previous authentication. Several triplets are required in order to generate longer session keys. If N triplets are not available, a set of authentication triplets is retrieved from HSS/HLR. If a temporary identifier is provided, it is mapped to the corresponding IMSI.~~

~~Although this step is presented after step 9 in this example, 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. 3GPP 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 be 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. The extra keying material is required in order to calculate a network authentication value and to pass the encrypted and integrity protected temporary identifier to the WLAN UE. The keying material may also be used for WLAN technology specific confidentiality or integrity protection.~~

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

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

~~3GPP AAA Server sends RAND, MAC, and encrypted temporary identifier to WLAN in EAP Request/SIM-Challenge message.~~

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

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

~~This computing gives N SRES and Kc values.~~

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

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

~~WLAN UE decrypts temporary identifier and saves it to be used on next authentication.~~

~~WLAN UE calculates a combined response value MAC_SRES from the N SRES responses.~~

~~15. WLAN UE sends EAP Response/SIM Challenge containing calculated MAC_SRES to WLAN~~

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

~~17. 3GPP AAA Server compares its copy of the MAC_SRES with the received MAC_SRES.~~

~~18. If the comparison in step 17 is successful, then 3GPP AAA Server sends the EAP Success message to WLAN. The 3GPP AAA Server includes the derived keying material in the message. WLAN stores the keying material to be used in communication with the authenticated WLAN UE.~~

~~19. WLAN 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 share session key material.~~

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

~~NOTE 4: Temporary identifier is only used for authentication purpose. User identification on the data path is done by the Access Point in a way that is proper to the WLAN~~

~~NOTE 5: the derivation of the value of N is for further study~~

~~A.5.3 Alternative EAP initialisation~~

The following figure shows an example where the realm identifying the 3GPP AAA server is retrieved by a method linked with the WLAN technology. Once the Diameter connection is initialized, the 3GPP AAA server can start the EAP identity request phase if necessary.

Editor's Note: the application of this procedure to IEEE 802.11 needs to be studied further.

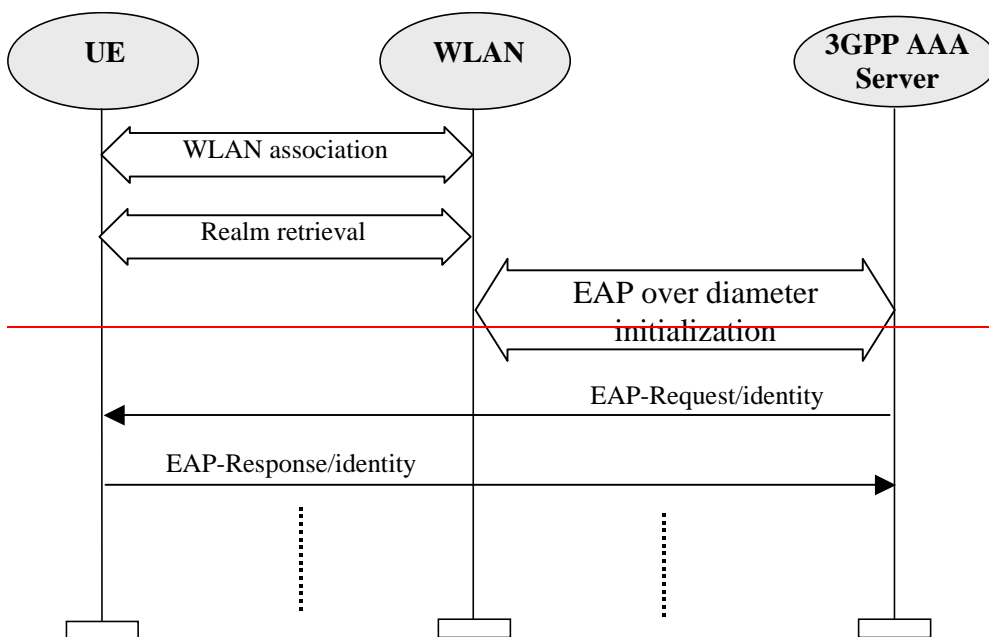


Figure A.5.3: End-to-end EAP initialisation session

A.5.4 Re-authentication message sequence chart

The message sequence chart below illustrates the operation on re-authentication.

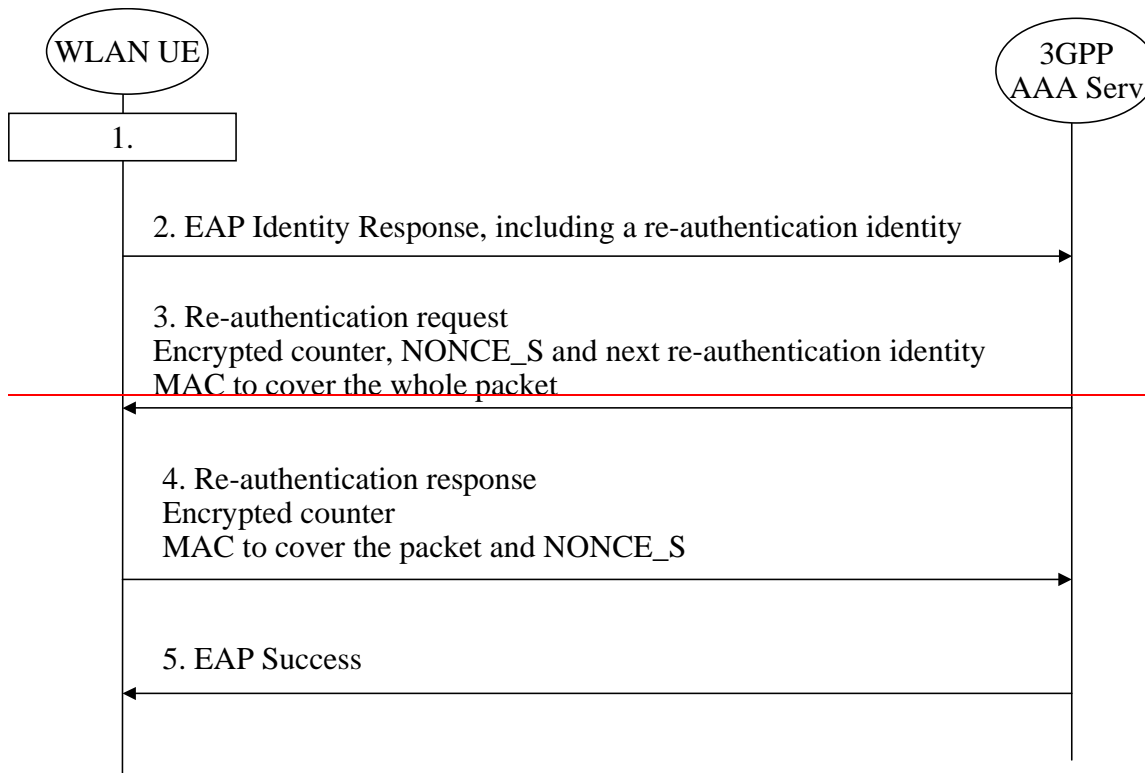


Figure A.5.4: Re-authentication signalling sequence

1. Either the WLAN UE or the WLAN initiates the authentication procedure with WLAN technology specific means. The WLAN UE is requested to send its identity

2. WLAN UE wishes to use the re-authentication procedure and therefore uses a re-authentication identity

- 3. ~~3GPP AAA server recognizes the re-authentication identity and agrees on using re-authentication. The 3GPP AAA server sends a re-authentication request (of the EAP type EAP/SIM or EAP/AKA) to the WLAN UE. The request contains an encrypted counter, an encrypted server challenge (NONCE_S) and a Message Authentication Code to cover the whole packet. The packet may also include an encrypted next re-authentication identity for next re-authentication~~
- 4. ~~WLAN UE verifies the Message Authentication Code and checks that the counter value is fresh. If successful, the WLAN UE responds with a re-authentication response packet that includes the counter value encrypted and a Message Authentication Code that covers the EAP packet and the server challenge NONCE_S~~
- 5. ~~3GPP AAA server verifies the Message Authentication Code and the counter. If successful, the 3GPP AAA server sends EAP Success to the WLAN UE.~~
- ~~WLAN UE and 3GPP AAA Server derive new session keys. 3GPP AAA Server sends the session keys to WLAN.~~

****** End of 3rd set of changes ******

****** Start of 4th set of changes ******

Annex E (informative):

~~Information on the discussed tunnel switching alternative~~ Void

Editor's Note: The content of this annex does not contain any information relevant to the normative part of this specification and is intended to be removed at a later stage once Stage 3 work is more stable.

~~E.1 Non Roaming WLAN Inter-working Reference Model~~

~~The 3GPP WLAN Interworking reference model in the non roaming case is shown in Figure E.1.1.~~

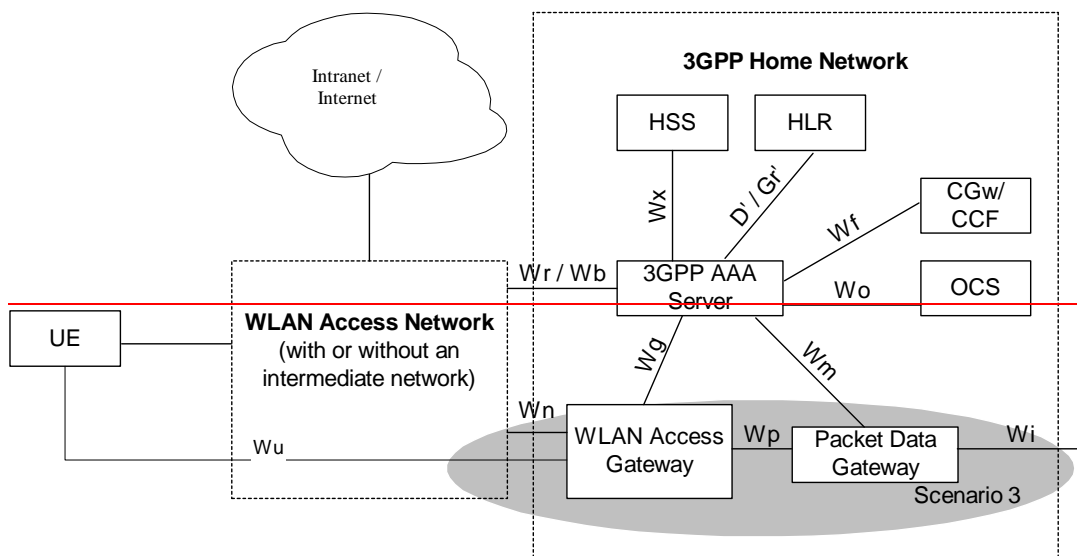


Figure E.1.1: Non-Roaming Reference Model

E.2 ~~Roaming WLAN Inter-working Reference Model~~

~~Figure E.2.1 shows the 3GPP WLAN interworking reference model in the roaming case.~~

~~The home network is responsible for access control. Charging records can be generated in the Visited and/or the Home 3GPP Networks. The Wx and Wo reference points are intra-operator. The 3GPP network interfaces to other 3GPP networks, WLANs, and intermediate networks via the Wa reference point.~~

~~The 3GPP AAA Proxy relays access control signalling and accounting information to the Home 3GPP AAA Server.~~

~~It can also issue charging records to the Visited Network's CGw/CCF when required.~~

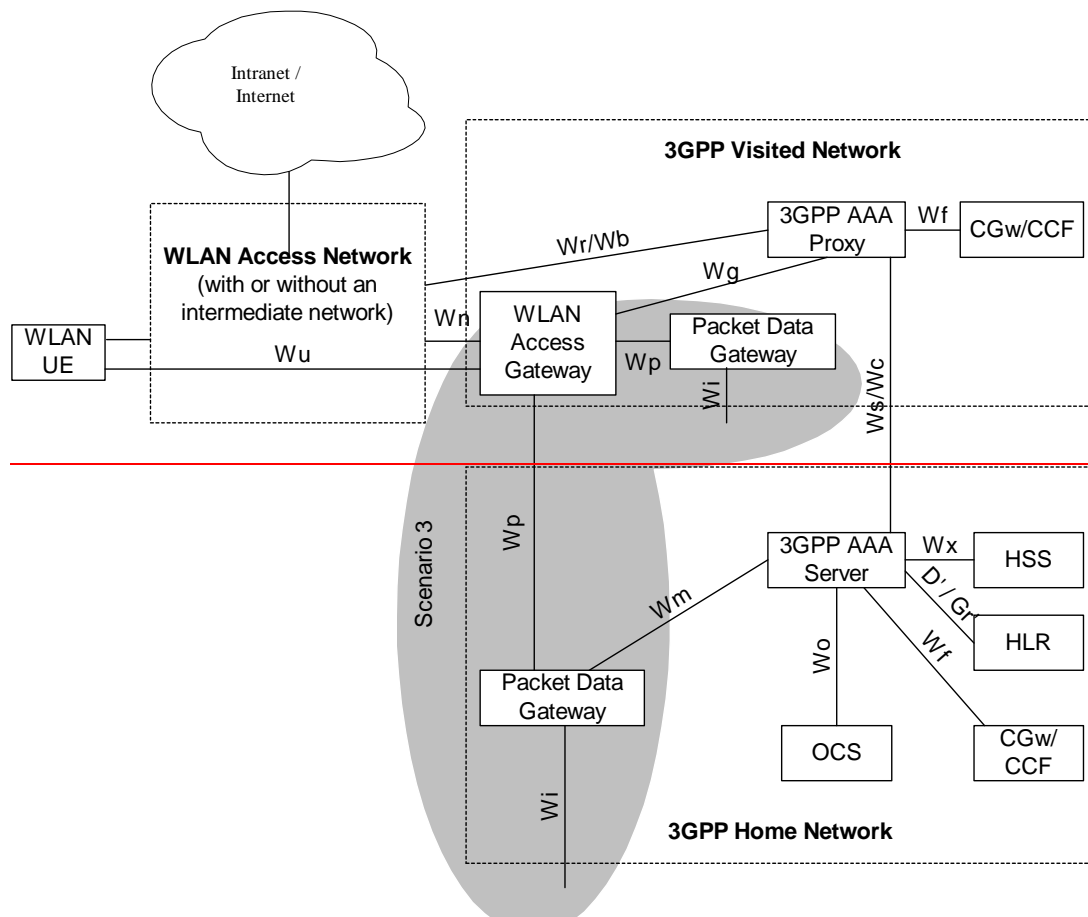


Figure E.2.1: Roaming Reference Model

E.3 ~~WAG Description~~

~~Support of the WAG for WLAN 3GPP IP Access is mandatory for both roaming and non-roaming cases.~~

~~The WAG shall:~~

- ~~— Support the setup of a secure tunnel initiated by the WLAN UE, and cooperate with the PDG to supply required parameters (e.g. DNS address, DHCP address, etc) from the destination network to the WLAN UE.~~
- ~~— Resolve the address of the PDG from the W-APN information supplied by the WLAN UE and verified with the 3G AAA Server.~~
- ~~— Set up a tunnel to the appropriate PDG(s).~~
- ~~— Route packets between the WLAN UE initiated tunnel and the tunnel to the PDG.~~

- ~~— Serve as a firewall for the network connecting the WAG and PDG, allowing only trusted packets into the 3G network.~~
- ~~— Update user status information in the 3G AAA Server.~~
- ~~— Generate accounting information, especially when located in the VPLMN.~~

~~E.4 — Wu Reference Point~~

~~The reference point Wu is located between the WLAN UE and the WAG. The purpose of this reference point is to transport tunnelled user data traffic securely between the WLAN UE and the 3GPP network to provide PS based services to the WLAN UE. In roaming cases, the Wu reference point is terminated between the WLAN UE and the WAG in the VPLMN. The WLAN may apply a routing enforcement policy, if necessary, to ensure packets are routed only to the WAG.~~

~~This reference point is not required to be used when no 3G PS based Services are provided and a direct connection to external IP network (Internet/Intranet) exists in which case the user data can be directly routed from the WLAN access network without passing 3GPP network, as it is the WLAN Direct IP Access.~~

~~No specific tunnelling protocol is specified for the Wu reference point, but the current working assumption is that the WLAN UE will be able to use an existing VPN client.~~

~~E.5 — Wn Reference Point~~

~~Reference point Wn is located between the WLAN Access Network and the WAG for user data traffic.~~

~~E.6 — Wp Reference Point~~

~~Reference point Wp is located between the WAG and the PDG. This reference point serves the purpose of transporting tunnelled WLAN user data between WAG and the PDG. The tunnel may not need to be encrypted if the transport network (e.g. GRX) is trusted. Since the network entities connected by Wp serves a similar purpose as the connecting network entities of the Gn/Gp interface in GPRS; the GTP protocol would be considered as a candidate for the Wp reference point.~~

****** End of changes ******

CR-Form-v7.1

CHANGE REQUEST

23.234 CR 117 rev 1 Current version: 6.3.0

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:	Charging in WAG		
Source:	3GPP TSG_SA WG2		
Work item code:	WLAN	Date:	27/01/2005
Category:	F	Release:	Rel-6
Use <u>one</u> 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 <u>one</u> of the following releases: Ph2 (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) Rel-7 (Release 7)	

Reason for change:	In the current TS there is an editor's note that the per tunnel charging in the WAG is FFS. On the other hand the TS clarifies this issue quite well: 1) According to clause 6.2.2 one of the AAA proxy function is: "Receiving per-tunnel charging information based on the tunnel identifier from the WAG and mapping of a user identifier and a tunnel identifier from the PDG; generating per user charging records for roaming users." 2) According to clause 6.2.5 the WAG "Performs collection of per tunnel accounting information, e.g. volume count (byte count) and elapsed time, to be used for inter-operator settlements." 3) According to clause 6.3.6 the Wg reference point is used to "Transport per-tunnel based charging information from the WAG to the AAA Proxy, only for roaming scenario."
Summary of change:	Clause 6.2.5.2 is removed with the editor's note. A clarification is added to 6.2.5 that the per-tunnel charging information collection is needed for the roaming scenario when the PDG is in the home network, and the WAG forwards the charging information to the local AAA proxy.
Consequences if not approved:	An invalid editor's note remains in the TS.

Clauses affected:	6.2.5				
Other specs	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr> <td style="text-align: center;">Y</td> <td style="text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Y	N				
<input type="checkbox"/>	<input checked="" type="checkbox"/>				

affected:

<input checked="" type="checkbox"/>	Test specifications
<input checked="" type="checkbox"/>	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.

****** Start of first set of changes ******

6.2.5 WLAN Access Gateway

The WLAN Access Gateway applies to a WLAN 3GPP IP Access enabled system.

The WLAN Access Gateway is a gateway via which the data to/from the WLAN Access Network shall be routed via a PLMN to provide a WLAN UE with 3G PS based services in a WLAN 3GPP IP Access enabled system.

The WLAN Access Gateway shall reside in the VPLMN in the roaming case, and in the HPLMN in the non-roaming case.

The WLAN Access Gateway:

- Allows VPLMN to generate charging information for users accessing via the WLAN AN in the roaming case.
- Enforces routing of packets through the PDG.
- Performs collection of per tunnel accounting information, e.g. volume count (byte count) and elapsed time, to be used for inter-operator settlements [in case of the roaming scenario when the Wu reference point is between the WLAN UE and a PDG in the home network \(Figure 6.2a\). The charging information is forwarded to the 3GPP AAA proxy in the visited network via the Wg reference point.](#)
- Filters out packets based on unencrypted information in the packets. Packets should only be forwarded if they:
 1. are part of an existing tunnel or
 2. are expected messages from the WLAN UEs. This includes service requests, and tunnel establishment messages.

Since the WAG does not have a full trust relationship with the WLAN UE, it is not able to stop all messages. However, messages from an unknown IP address can easily be discarded. Other approaches may be used as well. Additional types of message screening are left to the operators' control. Furthermore, Network Address Translators within the WLAN may modify the source address of IP packets from the WLAN UEs. The modified source address can be reliably associated to a WLAN UE by the PDG during tunnel establishment and provided to the WAG via the 3GPP AAA Server/Proxy. Before this point, all tunnel establishment packets shall be routed by the WAG except those which are possibly discarded due to certain Firewall rules implemented on the WAG.

Note: per tunnel accounting generation in the WAG is not required when the WAG and PDG are in the same network, i.e. the non-roaming case.

The WAG may implement policy enforcement before tunnel establishment to enhance the firewall against unwanted packets go through the PLMN, for example, to forbid the roaming WLAN UE from sending tunnel establishment to PLMN other than its HPLMN; to forbid packets from unauthorized WLAN UE.

The WAG shall implement policy enforcement after tunnel establishment.

After tunnel establishment, the following procedures apply at the WAG:

- If service is provided through a PDG in the HPLMN the WAG:
 - Ensures that all packets from the WLAN UE are routed to the HPLMN.
 - Ensures that packets from the authorised WLAN UEs are only routed to the appropriate PDG in the HPLMN and that packets from other sources than that PDG are not routed to the WLAN UE.
- If service is provided through a PDG in the VPLMN the WAG:
 - Ensures that all packets from the WLAN UE are routed to the VPLMN.
 - Ensures that packets from the authorised WLAN UEs are only routed to the appropriate PDG in the VPLMN and that packets from other sources than that PDG are not routed to the WLAN UE.

6.2.5.1 Policy Enforcement

Information regarding the selected PDG, including whether the PDG is in the HPLMN or the VPLMN is provided by the HPLMN to the VPLMN.

In the roaming case, the PDG information is delivered from the 3GPP AAA Server to the 3GPP AAA Proxy.

Within the VPLMN, policy enforcement information is delivered to the WAG.

Note: Whether information regarding one or all PDGs is provided will likely impact the signalling which supports the activation of a further W-APN. Delivering information of all valid PDGs may limit impacts on signalling for further W-APN establishment.

The policy enforcement delivered during initial authentication (before the tunnel establishment) will be bound to a user's AAA signalling. The WAG requires functionality to be able to associate this information to a user's traffic. As an implementation option, this functionality can be achieved by allocating the local IP Address by VPLMN.

The binding of the policy to a user's traffic allows the WAG to drop un-authorized packets sent to/from a user.

6.2.5.2 ~~Per-tunnel Charging Generation~~[Void](#)

~~Editor's Note: The details of per-tunnel charging generation in the WAG is FFS.~~

****** End of changes ******

CR-Form-v7.1

CHANGE REQUEST

23.234 CR 118 rev 1 Current version: 6.3.0

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:	Correction of Requirements for 3GPP PS based services		
Source:	3GPP TSG_SA WG2		
Work item code:	I-WLAN	Date:	28/01/2005
Category:	F	Release:	Rel-6
	Use <u>one</u> 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 <u>one</u> of the following releases: Ph2 (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) Rel-7 (Release 7)

Reason for change:	Currently, 3GPP-WLAN interworking does not support all 3GPP PS based services when WLAN 3GPP IP access is used (e.g. MBMS, MMS etc.)..
Summary of change:	Relieve the unachieved requirements
Consequences if not approved:	Inconsistency between the requirements and the actual specifications

Clauses affected:	5.1				
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Y	N				
<input type="checkbox"/>	<input checked="" type="checkbox"/>				
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input checked="" type="checkbox"/>				
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> O&M Specifications	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input checked="" type="checkbox"/>				
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.

5.1 Access Control Requirements

The following functional requirements have been identified:

- Legacy WLAN terminals should be supported. However software upgrades may be required for e.g. security reasons.
- Minimal impact on the user equipment, i.e. client software.
- Minimal impact on existing WLAN networks.
- The need for operators to administer and maintain end user software shall be minimized.
- Existing SIM and USIM shall be supported.
- Authentication shall rely on (U)SIM based authentication mechanisms.
- R6 USIM may include new functionality if necessary e.g. in order to improve privacy.
- Changes in the HSS/HLR/AuC shall be minimized.
- SLF node shall be used in the same way as defined in 3GPP TS 23.228 [24] to find the address of the HSS that holds the subscriber data for a given user identity when multiple and separately addressable HSSs have been deployed by the network operator.
- Methods for key distribution to the WLAN access network shall be supported.
- The WLAN connection established for a 3GPP subscriber shall have no impact to the capabilities of having simultaneous PS and CS connections for the same subscriber.
- WLAN Access Authorization shall occur upon the success of the authentication procedure. It shall take into account the user's subscription profile and optionally information about the WLAN AN, such as WLAN AN operator name, WLAN AN location information (e.g., country, telephone area code, city), WLAN AN throughput (e.g., maximum and minimum bandwidth guarantees for both ingress and egress traffic). This information is used to enable use-case scenarios like location based authentication/authorization, location based billing / customer care, and location based service offerings.
- It shall be possible to indicate to the user of the results of authorization requests.
- Results of WLAN Access Authorization requests shall be indicated to the WLAN, so that the WLAN can take appropriate action.
- The WLAN Access Authorization mechanism shall be able to inform the user and WLAN immediately of any change in service provision.
- This TS proposes solutions for operators who want to interwork their WLAN with an existing pre-R6 HLR/HSS.

Additional access control requirements for WLAN 3GPP IP Access:

- Service Authorization shall occur after the WLAN Access Authentication/Authorization procedure.
- Service based policy control shall be possible for the services authorized for the user.
- Access to 3GPP PS based services shall be provided via WLAN. The interworking architecture shall [provide IP connectivity to](#) be able to support all 3GPP PS based services. [3GPP PS based services which use more than IP connectivity \(e.g. SMS, MMS, MBMS\) could require additional entities and interfaces not specified in this document.](#)
- Access to PS based services normally provided by the 3GPP PS Core Network shall be provided via WLAN. WLAN access to these services shall support the same features as those supported via the 3GPP PS Core Network according to operator choice, e.g. private addressing schemes, external address allocation, secure tunneling to private external network. Quality of Service shall be supported when accessing these services via WLAN, although some limitations may exist because of the WLAN AN.

- A WLAN inter-working system supporting both WLAN Direct IP Access and WLAN 3GPP IP Access shall be able to support WLAN UEs operating in the WLAN Direct IP Access mode only, e.g. according to subscription.
- A combined access capable user should be able to choose between a WLAN Direct IP Access only” or a WLAN 3GPP IP Access, when the network allows it.- When the WLAN inter-working system does not support access to 3GPP PS based services, the WLAN UE shall be able to detect it.
- A WLAN 3GPP IP Access capable WLAN inter-working system shall be able to mandate all flows for 3G PS based services to be routed to the HPLMN or the VPLMN, e.g. according to subscription. This routing enforcement shall not rely on the WLAN UE client.

Note: This may mandate additional functionality existing in the WLAN AN

- The technical solution for access control to local IP networks from WLAN shall be decoupled from WLAN Access Control.

CR-Form-v7.1

CHANGE REQUEST

23.234 CR 120 rev - Current version: **6.3.0**

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:	Parameter storage for I-WLAN		
Source:	3GPP TSG_SA WG2		
Work item code:	WLAN	Date:	27/01/2005
Category:	F	Release:	Rel-6
	Use <u>one</u> 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 <u>one</u> of the following releases: Ph2 (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) Rel-7 (Release 7)

Reason for change:	The parameter storage for I-WLAN is specified in TS23.008 (N4-041572). An LS from CN4 was received (S2-050029), which requested the removal of overlapping text from TS23.234 to avoid maintenance problems in the future. The purpose of this CR is to act as it is requested by CN4.
Summary of change:	The overlapping text is removed and a reference to 23.008 is added.
Consequences if not approved:	There will be overlapping clauses in TS23.234 and TS23.008, which makes the maintenance work difficult.

Clauses affected:	2, 6.5										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Y</td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="padding: 2px;"><input type="checkbox"/></td> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="padding: 2px;"><input type="checkbox"/></td> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="padding: 2px;"><input type="checkbox"/></td> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	
	Y	N									
	<input type="checkbox"/>	<input checked="" type="checkbox"/>									
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Test specifications									
<input type="checkbox"/>	<input checked="" type="checkbox"/>	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.

****** Start of 1st 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] void
- [2] void
- [3] void
- [4] void
- [5] 3GPP TS 23.003: "Numbering, addressing and identification".
- [6] 3GPP TS 23.040: "Technical Realisation of the Short Message Service (SMS)"
- [7] 3GPP TS 23.060: "GPRS; Service description".
- [8] void
- [9] 3GPP TS 24.234: "3GPP System to WLAN Interworking; UE to Network protocols; Stage 3".
- [10] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".
- [11] void
- [12] 3GPP TS 31.102: "Characteristics of the USIM Application."
- [13] 3GPP TS 32.225: "Telecommunication management; Charging management; Charging data description for the IP Multimedia Subsystem (IMS)."
- [14] 3GPP TS 33.234: "WLAN Interworking Security."
- [15] 3GPP TS 23.125: "Overall High Level Functionality and Architecture Impacts of Flow Based Charging"
- [16] void
- [17] RFC 2486: "The Network Access Identifier"
- [18] void
- [19] IEEE Std 802.1X-2001 IEEE Standard for Local and metropolitan area networks— Port-Based Network Access Control
- [20] IETF Internet-Draft: "Network Discovery and Selection within the EAP Framework". draft-adrangi-eap-network-discovery-and-selection-03, work in progress.
- [21] IEEE Std 802.11-1999, Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, IEEE, Sep. 1999.

- [22] IETF Internet-Draft: "EAP AKA Authentication" draft-arkko-pppext-eap-aka-12 (April 2004).
- [23] IETF Internet-Draft: "EAP SIM Authentication" draft-haverinen-pppext-eap-sim-13 (April 2004).
- [24] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".
- [25] 3GPP TS 22.234: "Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking".
- [26] 3GPP TS 32.252: "Telecommunication management; Charging management; Wireless Local Area Network (WLAN) charging".
- [27] 3GPP TS 32.296: "Telecommunication management; Charging management; Online Charging System (OCS) applications and interfaces".
- [28] 3GPP TS 29.060: "GPRS; GTP across the Gn and Gp interface".
- [29] [3GPP TS 23.008: "Organization of subscriber data"](#)

**** End of 1st set of changes ****

**** Start of 2nd set of changes ****

6.5 WLAN user profile

The WLAN user profile shall reside in HSS (if the operator is using a legacy HLR, the WLAN user profile may reside in the 3GPP AAA Server) and be retrieved ~~from~~ by 3GPP AAA server via Wx reference point. The parameters stored in the network elements for I-WLAN, which includes the parameters of the WLAN user profile, are defined in clause 3B of TS23.008 [29]. ~~The profile shall contain the following data items: Detailed work on these parameters is expected in stage 3 work.~~

~~1. IMSI~~

~~2. MSISDN~~

~~3. Operator determined barring of 3GPP WLAN Interworking subscription~~

~~4. Operator determined barring of 3GPP WLAN 3GPP IP Access~~

~~— This allows operator to disable all W-APNs at one time. If there is a conflict between this item and the "operator determined barring" of any W-APN, the most restrictive will prevail.~~

~~5. Maximum session duration (optional)~~

~~— Used for re-authentication purposes. If this field is not used, the WLAN AN will apply default time intervals.~~

~~6. Subscribed Charging Characteristics and Accounting Server Identifier(s)~~

~~— The Subscribed Charging Characteristics will implicitly define the charging mode to be applied and, for every case, the accounting server where the accounting information is to be reported.~~

~~7. List of authorized W-APNs (optional)~~

~~— List of W-APNs for which the user will have services available. These W-APNs may correspond to services in the home network or in the visited network.~~

~~For each W-APN it shall be possible to define:~~

~~— W-APN Charging Characteristics and Accounting Server Identifier (optional)~~

~~If these parameters are not present, the W-APN Charging Characteristics and Accounting Server Identifier defined in item 6 must be considered.~~

~~W-APN remote IP address (optional)~~

~~Indication of the static remote IP address. If this parameter is present, the 3GPP AAA Server shall download it to the PDG in the W-APN authorization procedure, so the PDG shall use this static IP address. Otherwise, the remote IP address shall be allocated dynamically.~~

~~Operator determined barring for W-APN. As the service requirements defined in 3GPP TS 22.234. Those W-APNs which have a complete barring, shall not be sent to the 3GPP AAA Server from HSS.~~

~~8. WLAN Direct IP access allowed~~

~~Indication if the user is allowed to use WLAN Direct IP access.~~

~~9. Roaming allowed~~

~~Indication if the user is allowed to use a WLAN AN connected to an VPLMN.~~

****** End of changes ******

CR-Form-v7.1

CHANGE REQUEST

☞ **23.234 CR 121** ☞ rev **2** ☞ Current version: **6.3.0** ☞

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:	☞ Add the functionality of subscriber profile updating description		
Source:	☞ 3GPP TSG_SA WG2		
Work item code:	☞ WLAN	Date:	☞ 01/02/2005
Category:	☞ F	Release:	☞ Rel-6
	Use <u>one</u> 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 <u>one</u> of the following releases: Ph2 (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) Rel-7 (Release 7)

Reason for change:	☞ In the current specification, the clause 7.3 has been described the functionality of subscriber profile updating, but in the relational clauses on references points and network elements, there are not corresponding words to describe it.
Summary of change:	☞ Add the functionality of subscriber profile updating descriptions in the relevant clauses.
Consequences if not approved:	☞ Misunderstanding due to not coherent requirements

Clauses affected:	☞ 6.2.3, 6.3.1.1, 6.3.10						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Y</td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="padding: 2px;">X</td> <td style="padding: 2px;"></td> </tr> </table>	Y	N	X		Other core specifications	☞ 29.234
	Y	N					
	X						
<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px;">X</td> </tr> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px;">X</td> </tr> </table>		X		X	Test specifications		
	X						
	X						
<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px;">X</td> </tr> </table>		X	O&M Specifications				
	X						
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.

*****BEGINNING OF THE FIRST EDIT*****

6.2.3 3GPP AAA Server

The 3GPP AAA server is located within the 3GPP network. There should be only one 3GPP AAA Server for a WLAN attached subscriber. The 3GPP AAA Server:

- Retrieves authentication information and subscriber profile (including subscriber's authorization information) from the HLR/HSS of the 3GPP subscriber's home 3GPP network.
- Authenticates the 3GPP subscriber based on the authentication information retrieved from HLR/HSS. The authentication signaling may pass through AAA proxies.
- Updates the WLAN access authorisation information when user's service subscription is modified when requested by HSS/HLR.
- Communicates (including updates) authorization information to the WLAN AN potentially via AAA proxies.
- Registers its (the 3GPP AAA server) address or name with the HLR/HSS for each authenticated and authorized 3GPP subscriber.
- Initiates the Purge procedure when the 3GPP AAA server deletes the information of a subscriber.
- May act also as a AAA proxy (see above).
- Maintains the WLAN UE's WLAN-attach status.
- Provides the WLAN UE's WLAN-attach status to other entities (which are out of the scope of this TS).
- Generates and reports per-user charging/accounting information about WLAN Direct IP Access to the HPLMN Offline Charging System.
- Transfer a subscriber's authentication to a 3GPP AAA Server when it is requested by HSS/HLR.

For WLAN 3GPP IP Access:

- Communicates (including updates) service authorization information (e.g. authorized W-APN, necessary keying material for tunnel establishment and user data traffics) to the PDG. AAA proxies if the PDG is located in VPLMN.
- Provides the PDG with the WLAN UE's remote IP address, received from the HSS, when static remote IP address allocation is used.
- Provides the AAA-Proxy with suitable policy enforcement information.
- Provides suitable policy enforcement information to WAG in HPLMN.
- May provide suitable routing enforcement information to WLAN AN.

*****ENDING OF THE FIRST EDIT*****

*****BEGINNING OF THE SECOND EDIT*****

6.3.1 Wa reference point

6.3.1.1 General description

The Wa reference point connects the WLAN Access Network, possibly via intermediate networks, to the 3GPP Network (i.e. the 3GPP AAA Proxy in the roaming case and the 3GPP AAA server in the non-roaming case). The prime purpose of the protocols crossing this reference point is to transport authentication, authorization and charging-related information in a secure manner. The reference point has to accommodate also legacy WLAN Access Networks.

Legacy logical nodes outside of 3GPP scope that terminate or proxy the Wa reference point signalling and do not support 3GPP AAA protocol shall require signalling conversion between the legacy AAA protocol and the 3GPP AAA protocol.

EAP authentication shall be transported over the Wa reference point.

6.3.1.2 Functionality

The functionality of the reference point is to transport AAA frames:

- Carrying data for authentication signalling between WLAN UE and 3GPP Network.
- Carrying data for authorization ([including the authorization information update](#)) signalling between WLAN AN and 3GPP Network. These data may include a well-defined identification of the WLAN AN.
- Carrying charging signalling per WLAN user to enable offline and/or online charging. To minimize the requirements put on the WLAN Access Network, the use of online charging over Wa is optional and depends on the agreement between the operators of the WLAN AN and the 3GPP PLMN.
- Enabling the identification of the operator networks amongst which the roaming occurs.
- Carrying keying data for the purpose of radio interface integrity protection and encryption.
- May carry Routing Enforcement information from the PLMN to ensure that all packets sent to/from the WLAN UE for PS based services are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case) appropriately.
- When such functionality is supported by the WLAN AN, purging a user from the WLAN access for immediate service termination
- Providing access scope limitation information to the WLAN based on the authorised services for each user (for example, IP address filters)

*****ENDING OF THE SECOND EDIT*****

*****BEGINNING OF THE THIRD EDIT*****

6.3.10 Wm reference point

The Wm reference point applies to WLAN 3GPP IP Access.

This reference point is located between 3GPP AAA Server and Packet Data Gateway respectively between 3GPP AAA Proxy and Packet Data Gateway. The functionality of this reference point is to enable:

- The 3GPP AAA Server/Proxy to retrieve tunneling attributes and WLAN UE's IP configuration parameters from/via Packet Data Gateway.
- The 3GPP AAA Server to provide the PDG with the WLAN UE's remote IP address, received from the HSS, when static remote IP address allocation is used.

- The 3GPP AAA Server to provide the PDG with charging data (subscribed Charging Characteristics or W-APN Charging Characteristics) for 3GPP PS based services charging
- Carrying messages between PDG and AAA Server in support of the user authentication exchange which takes place between WLAN UE and 3GPP AAA server/proxy.
- Carrying messages for user authorization ([including authorization information update](#)) between PDG and 3GPP AAA server/proxy. These messages transport e.g. the requested W-APN from PDG to 3GPP AAA server/proxy and eventually the authorized W-APN from 3GPP AAA server/proxy to PDG.
- Carrying authentication data for the purpose of tunnel establishment, tunnel data authentication and encryption.
- Carrying mapping of a user identifier and a tunnel identifier sent from the PDG to the AAA Proxy through the AAA Server.

*****ENDING OF THE THIRD EDIT*****