

Source: TSG SA WG2
Title: CRs on 23.234 (WLAN)
Agenda item: 7.2.3
Document for: APPROVAL

The following CRs have been agreed by TSG SA WG2 and are requested to be approved by TSG SA plenary #26.

Note: the source of all these CRs is now SA2, even if the name of the originating company(ies) is still reflected on the cover page of all the attached CRs.

Tdoc	Title	Spec	CR	Rev	Cat	C_Ver	Rel	WI
<u>S2-043276</u>	Enhancements of Wd Interface	23.234	62	2	F	6.2.0	Rel-6	WLAN
<u>S2-043567</u>	Charging in WLAN interworking architecture	23.234	83	2	F	6.2.0	Rel-6	WLAN
<u>S2-043882</u>	Correction of online charging disconnect procedure	23.234	86	6	F	6.2.0	Rel-6	WLAN
<u>S2-043071</u>	Clarification on network selection	23.234	87	1	F	6.2.0	Rel-6	WLAN
<u>S2-043064</u>	Clarification on Wm reference point	23.234	88		F	6.2.0	Rel-6	WLAN
<u>S2-043073</u>	Correction of multiple service authorization requirement	23.234	89	1	F	6.2.0	Rel-6	WLAN
<u>S2-043079</u>	Removal of WLAN UE registration at tunnel establishment	23.234	90	2	F	6.2.0	Rel-6	WLAN
<u>S2-043078</u>	Providing configuration parameter to the WLAN UE during tunnel establishment	23.234	91	1	F	6.2.0	Rel-6	WLAN
<u>S2-043068</u>	Correction of references	23.234	92		F	6.2.0	Rel-6	WLAN
<u>S2-043566</u>	Removing tunnel redirection option	23.234	93	1	F	6.2.0	Rel-6	WLAN
<u>S2-043767</u>	Revision of PLMN selection procedure	23.234	94	1	F	6.2.0	Rel-6	WLAN
<u>S2-043772</u>	Revision of Ww reference point definition	23.234	95	2	F	6.2.0	Rel-6	WLAN
<u>S2-043885</u>	Supplement to the subscriber profile procedure	23.234	97	3	F	6.2.0	Rel-6	WLAN
<u>S2-043713</u>	Addition of reference	23.234	99	1	F	6.2.0	Rel-6	WLAN
<u>S2-043770</u>	Clarification of the procedure to disconnect the last tunnel	23.234	100	1	F	6.2.0	Rel-6	WLAN
<u>S2-043584</u>	Remove duplicated charging requirement for the PDG	23.234	101		F	6.2.0	Rel-6	WLAN
<u>S2-043884</u>	Consistent Wording, Spacing, and Grammar Readability Changes	23.234	102	3	D	6.2.0	Rel-6	WLAN
<u>S2-043886</u>	Rewording Readability Changes Section 1	23.234	104	3	F	6.2.0	Rel-6	WLAN
<u>S2-043883</u>	Rewording Readability Changes Section 3	23.234	105	3	F	6.2.0	Rel-6	WLAN
<u>S2-043909</u>	Section 5 Reordering	23.234	107	3	F	6.2.0	Rel-6	WLAN
<u>S2-043774</u>	3GPP WLAN User profile Update	23.234	109	2	F	6.2.0	Rel-6	WLAN

Tdoc	Title	Spec	CR	Rev	Cat	C_Ver	Rel	WI
<u>S2-043715</u>	Removal of unused references.	23.234	110	1	F	6.2.0	Rel-6	WLAN
<u>S2-043879</u>	Redraw of diagrams in section 7	23.234	111	1	D	6.2.0	Rel-6	WLAN
<u>S2-043881</u>	Editorial corrections	23.234	112	2	D	6.2.0	Rel-6	WLAN
<u>S2-043880</u>	Correction on Annex E	23.234	113	1	F	6.2.0	Rel-6	WLAN

CR-Form-v7.1

CHANGE REQUEST

23.234 CR 088 # rev **-** # Current version: **6.2.0**

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

Proposed change affects: UICC apps# ME Radio Access Network Core Network

Title:	# Clarification on Wm reference point		
Source:	# Siemens		
Work item code:	# WLAN	Date:	# 06/10/2004
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:	# Current version of specification 23.234 does not clearly say that W-APN is transported on the Wm reference point.
Summary of change:	# Besides some editorial corrections the change request clarifies that the requested W-APN is sent from PDG to AAA server and the authorized W-APN the other way round. In addition, an editors note is deleted.
Consequences if not approved:	# Unclear description of Wm reference point for stage 3 standardization.

Clauses affected:	# 5.6.1, 6.3.10										
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;">#</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">X</td> </tr> </table> Other core specifications # Test specifications # O&M Specifications #	Y	N	#	X	#	X	#	X		
Y	N										
#	X										
#	X										
#	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.

***** BEGIN OF 1st MODIFIED SECTION *****

5.5 Authentication methods

Authentication methods are discussed in TS 33.234 [6].

5.6 Service Authorization Principles for WLAN 3GPP IP Access

The home network decides whether visited service is allowed or not based on e.g. W-APN, the user subscription information, visited network capabilities and roaming agreement.

5.6.1 Accessing Home Network provided services

The following functionality and requirements have been identified:

- It shall be possible to support multiple service authorizations after a successful WLAN authentication/authorisation (i.e. EAP success).
- The Service authorisation procedure should, as far as possible, be independent from WLAN Access authentication and authorisation.
- The routing policy applied at WLAN Access Authentication and Authorisation may include policy determining whether the user has IP connectivity to the PDGs used for access to external IP networks.
- It shall be possible to permit access to different services simultaneously.
- Service authorization information shall be protected
- The Access Point Name (APN) concept defined in 3GPP TS 23.003 shall be used for WLAN interworking authorization (namely W-APN). In a service authorization procedure:
 - W-APN selection and authorization is an end-to-end procedure between the WLAN UE and the HPLMN (the service authorization decision is made by the 3GPP AAA Server based on [the requested W-APN and subscription information retrieved from the HSS/HLR, which includes e.g. the subscribed W-APNs](#)).

Editor's note: the use of subscription information is FFS.

- The WLAN UE shall use W-APN to indicate to the network the service or set of services it wants to access.
- The PDG selection shall be performed under control of the 3GPP Home Network by means of answers to DNS queries for the requested W-APN and tunnel redirection. The selection is based on the requested W-APN and user subscription information. The WLAN UE shall choose [the an](#) IP address of the PDG, if there is more than one PDG address in the answer to [the DNS queries](#).

The mechanism to select the PDG by the home network is out of scope of this specification, since it depends on the operator's preference.

- The PDG needs to know the authorized W-APN to select the external network, i.e. Wi interface.

5.6.2 Accessing Visited Network provided services

When accessing visited network provided services, additional principles below apply:

- In order for the WLAN UE to be able to use W-APNs in the VPLMN, the 3GPP AAA Server needs to pass to the 3GPP AAA Proxy the authorized W-APN and service related information which is required by the Visited Network to perform the service.
- The W-APN needs to be understood by both the Home and the Visited Networks.

- The V-PDG selection shall be under control of the 3GPP Visited Network by means of answers to DNS query for the requested W-APN and tunnel redirection. The selection is based on the authorized W-APN and service related information. The WLAN UE shall choose the IP address of the PDG if there is more than one PDG address in the answer to DNS query.

The mechanism to select the V-PDG by the Visited Network is out of scope of this specification, since it depends on the operator's preference.

- The selected PDG in the Visited Network needs to know the authorized W-APN to select the external network, i.e. Wi interface.

5.6.3 External IP Network selection

The WLAN UE can connect to different External IP networks, such as the Internet, an operator's IP network or a corporate IP network. The user may indicate a preferred IP network with a requested WLAN Access Point Name (W-APN). The Requested W-APN may also indicate a point of interconnection to the external IP network (i.e. PDG).

A W-APN is indicated by the WLAN UE in the tunnel establishment procedure between the WLAN UE and a PDG. It is then forwarded to the 3GPP AAA server/proxy in the same network as the PDG.

***** END OF 1st MODIFIED SECTION *****

***** BEGIN OF 2nd MODIFIED SECTION *****

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 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.

6.3.11 Wd reference point

***** END OF 2nd MODIFIED SECTION *****

CR-Form-v7.1

CHANGE REQUEST

23.234 CR 092 # rev **-** # Current version: **6.2.0**

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

Proposed change affects: UICC apps# ME Radio Access Network Core Network

Title:	# Correction of references		
Source:	# Siemens		
Work item code:	# WLAN	Date:	# 06/10/2004
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 numbering of the reference chapter in TS 23.234 is invalid. The references to EAP-SIM, EAP-AKA and network discovery drafts have to be updated.
Summary of change:	# Correct the numbering of the references in chapter 2 and a reference in chapter 5.11. Update references to IETF drafts EAP-SIM, EAP-AKA and network discovery.
Consequences if not approved:	# Incorrect references in stage 2 specification 23.234.

Clauses affected:	# 2, 5.11						
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="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> Test 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="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> O&M Specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	#	
Y	N						
<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.

***** BEGIN OF 1st MODIFIED SECTION *****

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TS 21.905: "Vocabulary for 3GPP Specifications".
- [2] 3GPP TS 22.101: "Service principles".
- [3] 3GPP TR 22.934: "Feasibility study on 3GPP system to WLAN interworking".
- [4] 3GPP TS 23.002: "Network architecture".
- [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] 3GPP TR 23.934: "3GPP system to WLAN Interworking; Functional and architectural definition".
- [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] 3GPP TS 29.329: "Sh Interface based on the Diameter protocol; Protocol details".
- [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] RFC2284: "PPP Extensible Authentication Protocol (EAP)"
- [17] RFC 2486: "The Network Access Identifier"
- [18] J. Caron, "DNS Based Roaming", <http://www.ietf.org/internet-drafts/draft-caron-dns-based-roaming-00.txt>, April 2002, (work in progress)
- [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-034, 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.

- [227] IETF Internet-Draft: "EAP AKA Authentication" draft-arkko-pppext-eap-aka-121 (~~October~~April 20034).
- [238] IETF Internet-Draft: "EAP SIM Authentication" draft-haverinen-pppext-eap-sim-132 (~~October~~April 20034).
- [249] 3GPP TS 23.228: " IP Multimedia Subsystem (IMS); Stage 2".
- ~~[10] 3GPP TS 32.252: "Telecommunication management; Charging management; Wireless Local Area Network (WLAN) charging".~~
- [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".

3 Definitions, symbols and abbreviations

***** END OF 1st MODIFIED SECTION *****

***** BEGIN OF 2nd MODIFIED SECTION *****

5.11 Charging

The following functionality and requirements have been identified:

- The WLAN Access Network shall be able to report the WLAN access usage to the appropriate 3GPP system (i.e. VPLMN in the roaming case and HPLMN in the non-roaming case).
- It shall be possible for the 3GPP system to control a specific ongoing WLAN access session for online charging purposes.
- It shall be possible for an operator to maintain a single prepaid account for WLAN, PS, CS, and IMS for a user.
- The 3GPP system shall be able to process the WLAN access resource usage information, and convert it into the format used in 3GPP networks (e.g. CDR).
- It shall be possible to correlate charging and accounting records generated in WLAN Access related nodes and records generated in 3GPP nodes.
- It shall be possible to apply offline charging and online charging mechanisms for the WLAN interworking with 3GPP network.

Additionally, for WLAN 3GPP IP Access:

- It shall be possible to generate per user charging information in the HPLMN and in the VPLMN irrespective of whether the service is provided in the HPLMN or in the VPLMN.
- WLAN Charging Information shall be collected for each WLAN UE by the WAG and the PDG that are serving the WLAN UE. The operator can control whether charging information shall be collected in the PDG on an individual WLAN UE and/or W-APN context basis by appropriately setting the Subscribed Charging Characteristics and/or W-APN Charging Characteristics in the HSS. The Charging Characteristics on the WLAN subscription and individually subscribed W-APNs are specified in 3GPP TS 32.252 [265].

5.12 AAA Protocol Requirements

***** END OF 2nd MODIFIED SECTION *****

CR-Form-v7

CHANGE REQUEST

23.234 CR 087 # rev 1 # Current version: 6.2.0

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

Proposed change affects: UICC apps# ME Radio Access Network Core Network

Title:	# Clarification on network selection		
Source:	# Samsung		
Work item code:	# WLAN	Date:	# 13/10/04
Category:	# F	Release:	# Rel-6
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)		2 (GSM Phase 2)
	A (corresponds to a correction in an earlier release)		R96 (Release 1996)
	B (addition of feature),		R97 (Release 1997)
	C (functional modification of feature)		R98 (Release 1998)
	D (editorial modification)		R99 (Release 1999)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)

Reason for change:	# The current text about network selection needs clarification to be in line with the SA1 specification.
Summary of change:	# Devide sections for manual selection and automatic selection for clarity. Clairfy use of I-WLAN identities' preference lists during the automatic selection. Remove redundant sentences.
Consequences if not approved:	# The use of I-WLAN identities' preference lists in the automatic mode is not clear and it can cause confusion.

Clauses affected:	# 5.4.2						
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>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	#
Y	N						
<input 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.

***** **FIRST MODIFIED SECTION** *****

5.4.2 I-WLAN Access Network Advertisement and Selection

5.4.2.1 Case of IEEE 802.11 WLANs

5.4.2.1.1 General

The following principles shall apply:

- Require no modifications of existing legacy APs.
- Have no impact on existing legacy clients (implies no modification of current broadcast SSIDs).
- Have low latency and overhead.
- The WLAN UE should be able to select the I-WLAN Access Network supporting the preferred PLMN.

In the case of IEEE 802.11 WLANs:

- Modification of current broadcast SSIDs shall not be required;
- Active scanning should be supported by the WLAN UE;
- Passive scanning shall be supported by the WLAN UE;
- Multiple SSIDs may be supported (i.e. only standard 802.11 capable APs are required).

5.4.2.1.2 WLAN Access Network Advertisement

A WLAN network name is provided in WLAN beacon signal in so-called SSID (Service Set ID) information element. There is also the possibility for a WLAN UE to actively solicit support for specific SSIDs by sending a probe request message and receive a reply if the access point does support the solicited SSID. Active and passive scanning are defined in IEEE 802.11 [21].

A WLAN AN may indicate that it provides 3G interworking without the involvement of any other network than the WLAN AN.

The above requirement may be met through explicit EAP-based procedures or through the generic Preferred SSID list procedures – for example Preferred SSID lists could include SSID formats defined by operators for the above purposes.

5.4.2.1.3 I-WLAN Access Network Selection

For purpose of selecting the preferred I-WLAN AN the WLAN UE may contain lists of I-WLAN identities' preferences. One list will contain the SSIDs preferred by the Home Network operator and one list contains the SSID's preferred by the user.

The Operator's preferred SSID list would be populated, for example, with the SSIDs commonly used by major hotspot operators with whom the Home Operator has a direct [or indirect \(through VPLMN in a roaming case\)](#) relationship.

[There are two modes in network selection, i.e. Manual mode and automatic mode](#)

[Manual mode](#)

In ~~the manual mode~~, the WLAN UE shall ~~try to find~~ ~~scan (passive scanning) for~~ all available SSIDs ~~through passive scanning and/or active scanning (when it is supported)~~, ~~in beacon channels it can discover~~. ~~The WLAN UE may also probe (active scanning) for additional available SSIDs from each of the WLAN networks that it has discovered.~~

~~In Manual mode~~ ~~o~~Once a list of all available SSIDs has been obtained, it shall be possible for the WLAN UE

to obtain a list of all available PLMNs from each SSID. When a list of PLMNs has been obtained from all SSIDs it shall present them to the user ~~to select one~~. The WLAN UE shall then associate with the SSID that supports the PLMN that is selected by the user.

Automatic Mode

In the automatic mode the procedure is as follows:

0. The WLAN UE scans for all available SSIDs using passive scan and/or active scan. If the WLAN UE contains the I-WLAN identities' preference lists, the scan should be done in the order of these lists. It is not required to continue the scanning after the highest priority SSID is found.
1. Start association and perform Network Discovery. When there is more than one available SSID and the WLAN UE contains I-WLAN identities' preference lists, the association shall be done in the order of these lists.
 - 1a) If authentication to HPLMN succeeds (i.e. EAP-Success is received), then stop this procedure.
 - 1b) If Network Advertisement information is received (i.e. EAP-Identity/Request is received), then store the list and start again step 1.

Repeat step 1 for all available SSIDs ~~following the order specified in the I-WLAN identities preference lists~~. If the scanning in step 0 was stopped due to the discovery of the highest priority SSID, but the HPLMN has not been found (e.g. because the SSID list is not updated or the selected SSID was a fake one), then the user should go back to step 0 and scan for all ~~available~~ remaining SSIDs.

Note that if an AP supporting HPLMN is found in the middle of the procedure, step 1a, then step 1 is stopped and association with the remaining available APs will not take place.
2. Use the lists of 'User Controlled PLMN Selector list for I-WLAN' and 'Operator Controlled PLMN Selector list for I-WLAN' and the lists from step 1b) to select the best matching PLMN. Note that the 'User Controlled PLMN Selector list for I-WLAN' has higher priority than the 'Operator Controlled PLMN Selector list for I-WLAN'. Then select the I-WLAN AN that supports the best match PLMN. If more than one I-WLAN AN supports the best matched PLMN, the I-WLAN AN having the highest priority SSID is selected, if 'I-WLAN identities' preference lists are available.
3. Associate with the AP selected in step 2 and attempt authentication with the best match PLMN. ~~An I-WLAN AN~~ may indicate that it provides 3G interworking without the involvement of any other network than the WLAN AN.

If such an indication is provided by the WLAN AN and if the WLAN UE supports the indication, then the WLAN UE shall use it at SSID selection as defined in 3GPP TS 24.234 [9].

The above requirement may be met through explicit EAP-based procedures or through the generic 'I-WLAN identities' preference lists procedures – for example I-WLAN identities preference lists could include SSID formats defined by operators for the above purposes.

******* END OF CHANGES *******

CHANGE REQUEST

23.234 CR 089 # rev 1 # Current version: 6.2.0

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	# Correction of multiple service authorization requirement		
Source:	# Siemens		
Work item code:	# WLAN	Date:	# 11/10/2004
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:	# Chapter 5.6.1 requires that multiple service authorizations must be possible after a successful WLAN authentication/authorization (i.e. EAP success). However, the second part of the sentence "after a successful WLAN authentication/authorization (i.e. EAP success)" is misleading as access and service authentication/authorization are independent of each other. The same applies to a requirement statement in chapter 5.1.
Summary of change:	# The second part of the first bullet point in 5.6.1 and the corresponding requirement on service authorization in chapter 5.1 are changed to indicate that serve authorization is performed after successful authentication.
Consequences if not approved:	# Misleading requirement for service authorization.

Clauses affected:	# 5.1, 5.6.1										
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> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><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 # Test specifications # O&M Specifications #	
Y	N										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<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.

***** BEGIN OF 1st MODIFIED SECTION *****

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~~[successful](#) 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 be able to support all 3GPP PS based services.
- 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.

***** END OF 1st MODIFIED SECTION *****

***** BEGIN OF 2nd MODIFIED SECTION *****

5.6 Service Authorization Principles for WLAN 3GPP IP Access

The home network decides whether visited service is allowed or not based on e.g. W-APN, the user subscription information, visited network capabilities and roaming agreement.

5.6.1 Accessing Home Network provided services

The following functionality and requirements have been identified:

- It shall be possible to support multiple service authorizations after ~~a~~-successful ~~WLAN authentication/authorisation (i.e. EAP success)~~.
- The Service authorisation procedure should, as far as possible, be independent from WLAN Access authentication and authorisation.
- The routing policy applied at WLAN Access Authentication and Authorisation may include policy determining whether the user has IP connectivity to the PDGs used for access to external IP networks.
- It shall be possible to permit access to different services simultaneously.
- Service authorization information shall be protected
- The Access Point Name (APN) concept defined in 3GPP TS 23.003 shall be used for WLAN interworking authorization (namely W-APN). In a service authorization procedure:
 - W-APN selection and authorization is an end-to-end procedure between the WLAN UE and the HPLMN (the service authorization decision is made by the 3GPP AAA Server *based on subscription information retrieved from the HSS/HLR*).

Editor's note: the use of subscription information is FFS.

- The WLAN UE shall use W-APN to indicate to the network the service or set of services it wants to access.
- The PDG selection shall be performed under control of the 3GPP Home Network by means of answers to DNS query for the requested W-APN and tunnel redirection. The selection is based on the requested W-APN

and user subscription information. The WLAN UE shall choose the IP address of the PDG if there is more than one PDG address in the answer to DNS query.

The mechanism to select the PDG by the home network is out of scope of this specification, since it depends on the operator's preference.

- The PDG needs to know the authorized W-APN to select the external network, i.e. Wi interface.

5.6.2 Accessing Visited Network provided services

***** END OF 2nd MODIFIED SECTION *****

CHANGE REQUEST

⌘ **23.234 CR 091** ⌘ rev **1** ⌘ Current version: **6.2.0** ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Providing configuration parameter to the WLAN UE during tunnel establishment		
Source:	⌘ Siemens		
Work item code:	⌘ WLAN	Date:	⌘ 13/10/2004
Category:	⌘ F	Release:	⌘ Rel-6
	<i>Use <u>one</u> of the following categories:</i> 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 .		<i>Use <u>one</u> of the following releases:</i> 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:	⌘ Chapter 5.6.1 and 5.6.2 of 23.234 on accessing home and visited network provided services do not contain any requirement that it must be possible to provide configuration parameter like remote IP address and DHCP or DNS server addresses to the WLAN UE during or after service authorisation. This is necessary so that stage 3 groups can specify an appropriate procedure on protocol level to fulfil this requirement and the WLAN UE is able to access IP based services in the PS domain or an external packet data network.
Summary of change:	⌘ Add a requirement in chapter 5.6.1 and 5.6.2 that it shall be possible to provide configuration parameter to the WLAN UE during or after service authorisation, e.g. remote IP address and addresses of DHCP and DNS servers in the PLMN.
Consequences if not approved:	⌘ Missing requirements for stage 3 leading to incomplete protocol specification.

Clauses affected:	⌘ 5.6.1, 5.6.2						
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="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> Test 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="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> O&M Specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<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.

***** BEGIN OF MODIFIED SECTION *****

5.5 Authentication methods

Authentication methods are discussed in TS 33.234 [6].

5.6 Service Authorization Principles for WLAN 3GPP IP Access

The home network decides whether visited service is allowed or not based on e.g. W-APN, the user subscription information, visited network capabilities and roaming agreement.

5.6.1 Accessing Home Network provided services

The following functionality and requirements have been identified:

- It shall be possible to support multiple service authorizations after a successful WLAN authentication/authorisation (i.e. EAP success).
- The Service authorisation procedure should, as far as possible, be independent from WLAN Access authentication and authorisation.
- The routing policy applied at WLAN Access Authentication and Authorisation may include policy determining whether the user has IP connectivity to the PDGs used for access to external IP networks.
- It shall be possible to permit access to different services simultaneously.
- It shall be possible to provide IP related configuration parameters to the WLAN UE during or after successful service authorisation. These configuration parameters may include e.g. the WLAN UE's remote IP address and addresses of DHCP and DNS servers in the HPLMN.
- Service authorization information shall be protected
- The Access Point Name (APN) concept defined in 3GPP TS 23.003 shall be used for WLAN interworking authorization (namely W-APN). In a service authorization procedure:
 - W-APN selection and authorization is an end-to-end procedure between the WLAN UE and the HPLMN (the service authorization decision is made by the 3GPP AAA Server *based on subscription information retrieved from the HSS/HLR*).

Editor's note: the use of subscription information is FFS.

- The WLAN UE shall use W-APN to indicate to the network the service or set of services it wants to access.
- The PDG selection shall be performed under control of the 3GPP Home Network by means of answers to DNS query for the requested W-APN and tunnel redirection. The selection is based on the requested W-APN and user subscription information. The WLAN UE shall choose the IP address of the PDG if there is more than one PDG address in the answer to DNS query.

The mechanism to select the PDG by the home network is out of scope of this specification, since it depends on the operator's preference.

- The PDG needs to know the authorized W-APN to select the external network, i.e. Wi interface.

5.6.2 Accessing Visited Network provided services

When accessing visited network provided services, additional principles below apply:

- In order for the WLAN UE to be able to use W-APNs in the VPLMN, the 3GPP AAA Server needs to pass to the 3GPP AAA Proxy the authorized W-APN and service related information which is required by the Visited Network to perform the service.
- The W-APN needs to be understood by both the Home and the Visited Networks.
- The V-PDG selection shall be under control of the 3GPP Visited Network by means of answers to DNS query for the requested W-APN and tunnel redirection. The selection is based on the authorized W-APN and service related information. The WLAN UE shall choose the IP address of the PDG if there is more than one PDG address in the answer to DNS query.

The mechanism to select the V-PDG by the Visited Network is out of scope of this specification, since it depends on the operator's preference.

- The selected PDG in the Visited Network needs to know the authorized W-APN to select the external network, i.e. Wi interface.

- It shall be possible to provide IP related configuration parameters to the WLAN UE during or after successful service authorisation. These configuration parameters may include e.g. the WLAN UE's remote IP address and addresses of DHCP and DNS servers in the VPLMN.

5.6.3 External IP Network selection

The WLAN UE can connect to different External IP networks, such as the Internet, an operator's IP network or a corporate IP network. The user may indicate a preferred IP network with a requested WLAN Access Point Name (W-APN). The Requested W-APN may also indicate a point of interconnection to the external IP network (i.e. PDG).

A W-APN is indicated by the WLAN UE in the tunnel establishment procedure between the WLAN UE and a PDG. It is then forwarded to the 3GPP AAA server/proxy *in the same network as the PDG*.

5.7 IP Connectivity for WLAN 3GPP IP Access

***** END OF MODIFIED SECTION *****

CHANGE REQUEST

23.234 CR 090 # rev **2** # Current version: **6.2.0**

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

Proposed change affects: UICC apps# ME Radio Access Network Core Network

Title:	# Removal of WLAN UE registration at tunnel establishment		
Source:	# Siemens		
Work item code:	# WLAN	Date:	# 13/10/2004
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:	# Chapter 7.9 of 23.234 requires that the 3GPP AAA server registers the WLAN UE at the HSS after successful authentication during tunnel establishment. Up to now it is not clarified what registration means in this context, nor what kind of information is stored in the HSS with respect to this kind of registration. This gives no clear guidance for stage 3 work. As the 3GPP AAA server address is stored in the HSS and the AAA server knows all relevant data regarding tunnel establishment, e.g. WLAN UE's remote IP address, PDG address, W-APN, there is no good reason why the HSS should be informed about the UE's registration status. In addition, there is no procedure defined in the TS that makes use of the tunnel registration information stored in the HSS. It is proposed to delete the current text and replace it by the explicit statement that the 3GPP AAA server registers itself, i.e. its address and the corresponding user identity, at the HSS.
Summary of change:	# Remove the editors note in chapter 7. Remove the requirement that the 3GPP AAA server registers the WLAN user at the HSS during tunnel establishment. Add an explicit requirement that the AAA server registers itself at the HSS. Make some editorial corrections.
Consequences if not approved:	# Unclear requirements for stage 3.

Clauses affected:	# 7, 7.9						
Other specs affected:	<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"/>						
	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications	<input checked="" 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.

***** BEGIN OF 1st MODIFIED SECTION *****

7 Procedures

Editor's note: the following procedure is FFS:

~~—Subscriber Registers.~~

7.1 I-WLAN and VPLMN Selection Procedure

***** END OF 1st MODIFIED SECTION *****

***** BEGIN OF 2nd MODIFIED SECTION *****

7.9 W-APN resolution and Tunnel establishment

This information flow presents the generic message exchange necessary in order to resolve the selected W-APN and establish a WLAN UE-Initiated tunnel for WLAN 3GPP IP Access purposes.

As a prerequisite of these procedures it is necessary to perform the following:

1. WLAN Access Authentication and Authorisation and provisioning of the WLAN UE's local IP address

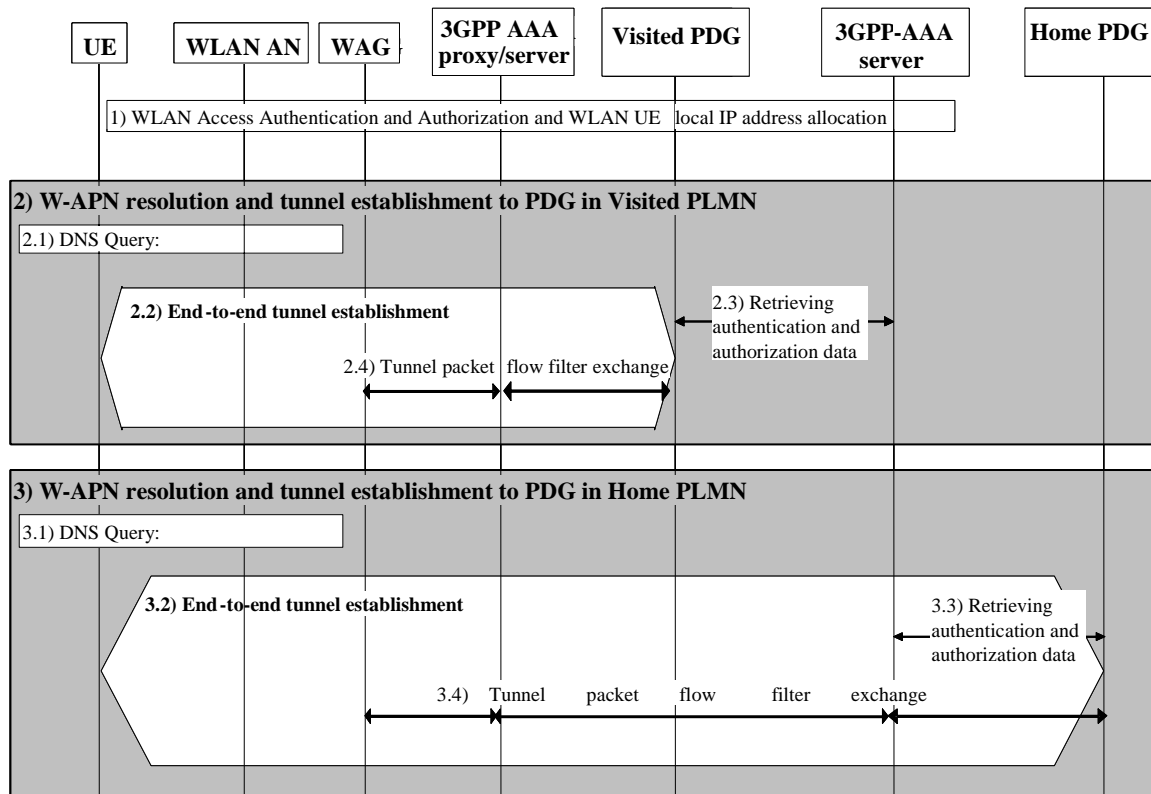


Figure 7.10: Example message flow to WLAN UE-Initiated tunnel establishment

When the user decides that he wants to access a service, the WLAN UE selects the W-APN network ID associated to the service requested by the user.

A detailed description of the W-APN resolution and the WLAN UE-Initiated Tunnel Establishment is given below.

2. Depending on internal configuration, the WLAN UE initiates W-APN resolution and tunnel establishment with a PDG in VPLMN.

Note: The configuration of the WLAN UE regarding W-APNs can be controlled by e.g. USIM Application Toolkit-based mechanisms.

- 2.1 WLAN UE constructs an FQDN using the W-APN Network Identifier and VPLMN ID as the Operator Identifier and performs a DNS query to resolve it. The DNS response will contain one or more IP addresses of equivalent PDGs that support the requested W-APN in the VPLMN according to standard DNS procedures.
If the VPLMN does not support the W-APN, then the DNS query returns a negative response. In this case, the WLAN UE continues with step 3.
- 2.2 The WLAN UE selects a PDG from the list received in step 2.1. If the DNS response contains IPv4 and IPv6 addresses, the WLAN UE has to select an address that has the same format as its own local IP address. If a PDG is finally selected, the establishment of an end-to-end tunnel is performed between the WLAN UE and this PDG. The WLAN UE shall include the W-APN and the user identity in the initial tunnel establishment request.
- 2.3 During the tunnel establishment, the PDG contacts the 3GPP AAA Server in the HPLMN via the 3GPP AAA proxy for authorization of the WLAN UE for the W-APN being requested by the WLAN UE and to retrieve the information required for the mutual authentication part of the tunnel establishment. As a result of successful mutual authentication the 3GPP AAA Server registers ~~the WLAN UE itself~~ at the HSS ([WLAN registration procedure](#)). This action may be omitted, if the ~~WLAN UE~~[3GPP AAA Server](#) is already registered at ~~this 3GPP AAA Server~~[the HSS](#).
The 3GPP AAA Server shall be able to check that the user requesting the tunnel establishment has been already successfully WLAN Access Authorized. Based on operator policy it shall be possible to turn this check on and off. The check may be based on the user's subscription data, e.g. the user's subscribed services. If the check is not successful, the tunnel establishment request is rejected.

If the WLAN UE is not allowed to use a visited-PDG to access the given W-APN, the AAA Server shall send a rejection message to the PDG and then the tunnel establishment shall be rejected by the PDG. The 3GPP AAA server shall provide PDG with the subscribed Charging Characteristics or W-APN Charging Characteristics. If it is not possible to establish the tunnel with any of the PDGs received from step 2.1, or the tunnel establishment failure reason is that the WLAN UE is not allowed to use a visited-PDG to access the given W-APN, then the WLAN UE continues with step 3.

- 2.4 During the tunnel establishment procedure, the PDG and the WAG exchange information via the 3GPP AAA Proxy in order to establish a filtering policy to allow the forwarding of tunnelled packets to the PDG. The 3GPP AAA Proxy requests the WAG to apply filtering policy based on information obtained from the PDG. The 3GPP AAA Proxy decides which filtering policy could be applied by the WAG according to local information (e.g. based on number of users, WAG capabilities, roaming agreement policy, etc).
3. Depending on internal configuration, or due to the failure of step 2.1 or 2.3, the WLAN UE initiates W-APN resolution and tunnel establishment with a PDG in HPLMN.
- 3.1 WLAN UE constructs an FQDN using W-APN Network Identifier and the HPLMN ID as the Operator Identifier, and performs a DNS query to resolve it. The DNS response will contain one or more IP addresses of equivalent PDGs that support the requested W-APN in the HPLMN according to standard DNS procedures.
- 3.2 The WLAN UE selects a PDG from the list received in step 3.1. If the DNS response contains IPv4 and IPv6 addresses, the WLAN UE has to select an address that has the same format as its own local IP address. If a PDG is finally selected, establishment of an end-to-end tunnel is performed between the WLAN UE and this PDG. The WLAN UE shall include the W-APN and the user identity in the initial tunnel establishment request.
- 3.3 During the tunnel establishment, the PDG contacts the 3GPP AAA Server in the HPLMN for authorization of the WLAN UE for the W-APN being requested by the WLAN UE and to retrieve the information required for the mutual authentication part of tunnel establishment. As a result of successful mutual authentication the 3GPP AAA Server registers ~~the WLAN user~~ itself at the HSS ([WLAN registration procedure](#)). This action may be omitted, if the ~~WLAN UE~~ 3GPP AAA Server is already registered at ~~this 3GPP AAA Server~~ the HSS. The 3GPP AAA Server shall be able to check that the user requesting the tunnel establishment has been already WLAN Access Authorized. Based on operator policy it shall be possible to turn this check on and off. The check may be based on the user's subscription data, e.g. the user's subscribed services. If the check is not successful, the tunnel establishment request is rejected.
- If the WLAN UE is not allowed to use a Home PDG to access the given W-APN according to his subscription, the AAA Server shall send a rejection message to the PDG and then the tunnel establishment shall be rejected by the Home PDG. The 3GPP AAA Server shall 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 shall provide PDG with the subscribed Charging Characteristics or W-APN Charging Characteristics.
- 3.4 During the tunnel establishment, the PDG and the WAG exchange information via the 3GPP AAA Server and 3GPP AAA Proxy in order to establish a filtering policy to allow the forwarding of tunnelled packets to the PDG. The 3GPP AAA server requests to the WAG to apply filtering policy based on information obtained from the PDG. The 3GPP AAA server decides which filtering policy could be applied by the WAG according to local information (e.g. based on number of user, WAG capabilities, roaming agreement policy, etc). The applied filtering policy is communicated to the Home-PDG.

7.9.1 Redirection

***** END OF 2nd MODIFIED SECTION *****

CHANGE REQUEST

⌘ **23.234 CR 062**_[ES3] ⌘ rev **2** ⌘ Current version: **6.2.0** ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Enhancements of Wd Interface	
Source:	⌘ Vodafone, T-Mobile	
Work item code:	⌘ WLAN	Date: ⌘ 11/10/2004
Category:	⌘ F 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 .	Release: ⌘ Rel-6 Use <u>one</u> 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 AAA protocol requirements included in this specification was intended to direct stage 3 development. Stage 3 development has now been completed and the requirements have been implemented. Some duplication exists of specification of AAA for WLAN with the WLAN stage 3 (3GPP TS 29.234). Therefore the requirements are no longer valid in the stage 2. The requirements may also cause ambiguity to those that are unfamiliar with the discussions that caused them to be added. Common AAA protocol requirement – This requirement is not worded correctly and should reflect the support of RADIUS on Wa/Wd (as specified in section 5.2 of TS 29.234) as the use of RADIUS on Wd would break the common AAA protocol requirement. Single protocol for Accounting requirement – This should be removed due to the support of RADIUS on Wa and Wd whilst existing charging architecture is based on Diameter Credit Control application (TS 32.296 & 32.299). The use of Diameter Credit Control is not possible on Wa and Wd. Support for interworking requirement – This is already specified in great detail in section 5.3 of TS 29.234 and such text may contradict existing text and possible future text and therefore the text should be generalised.
Summary of change:	⌘ Removal of the single Accounting protocol requirement from the stage 2. Generalisation of the interworking requirement and the common AAA protocol requirement
Consequences if	⌘ Duplicated protocol requirements remain in the stage 2 that are better placed

not approved: and indeed are already present in the stage 3 (TS 29.234).
Also, such requirements may prohibit support of "legacy" WLAN ANs that the requirements were supposed to benefit.

Clauses affected:	⌘	5.12										
Other specs affected:	⌘	<table border="1"> <tr> <td>Y</td> <td>N</td> </tr> <tr> <td></td> <td>X</td> </tr> <tr> <td></td> <td>X</td> </tr> <tr> <td></td> <td>X</td> </tr> </table>	Y	N		X		X		X	Other core specifications	⌘
		Y	N									
			X									
	X											
	X											
			Test specifications									
			O&M Specifications									
Other comments:	⌘											

How to create CRs using this form:

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

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.12 AAA Protocol Requirements

- As far as possible, a common AAA protocol shall be used across all AAA interfaces. This may not be possible for the Wa and Wd interfaces when the WLAN AN is using a legacy AAA protocol.~~A common AAA protocol shall be used for Authentication, Authorization and Accounting purposes in the WLAN Interworking Architecture within the 3GPP network.~~
- ~~The protocol used for Accounting purpose in the WLAN Interworking Architecture in the 3GPP network shall be the same as used by the 3GPP Charging Architecture eg. the AAA protocol used by the 3GPP IMS charging architecture;~~
- If protocol interworking is needed, then in the non-roaming case it shall be performed at the edge of the 3GPP network. For roaming, such interworking shall be performed either in the visited network or in the home network (dependent upon inter-operator roaming agreements).~~If interworking with a legacy AAA protocol is needed, then it shall be performed at the entry and exit point of the 3GPP network. In the case of roaming, such interworking shall be performed in the visited network. The legacy AAA protocol may not support all features of 3GPP AAA protocol. Therefore, this interworking might limit the usage of features existent in 3GPP AAA protocol but not existent in legacy AAA protocol(e.g. filtering rules).~~

CHANGE REQUEST

23.234 CR 093 # rev **1** # Current version: **6.2.0**

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

Proposed change affects: UICC apps# ME Radio Access Network Core Network

Title:	# Removing tunnel redirection option		
Source:	# Nokia, Siemens, Ericsson		
Work item code:	# WLAN	Date:	# 10/11/2004
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 SA2 the tunnel redirection has been introduced. The primary purpose of the tunnel redirection is the load-balancing, which can be provided in many other ways; e.g, via the DNS server that provides the PDGs' addresses to the UEs or a PDG implementation can provide transparent load-balancing. Another reason of the introduction of the redirection was that in this way operators should not advertise all of their PDGs via the DNS server. However it has been agreed that this method will not provide an increased security, since during the tunnel establishment procedure the end-user will get the real IP address of the PDG. From this point the same type of attacks can be performed against the PDG as its address would be advertised via the DNS server. In CN1 it has been identified that the tunnel redirection would require either changes to the selected tunneling protocol (IKE_V2) or 3GPP vendor specific work. The redirection function is not crucial (see the reasoning above) and its features can be provided by other means, therefore the redirection function is proposed to be removed from the specification.
Summary of change:	# The optional tunnel redirection procedure is removed.
Consequences if not approved:	# The tunneling protocol will contain unnecessary complexity, which may delay the specification and the implementation of 3GPP WLAN IP Access.

Clauses affected:	# 5.6.1, 5.6.2, 6.2.6, 7.9.1						
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;">X</td> <td style="text-align: center;"></td> </tr> </table> Other core specifications	Y	N	X		# 24.234
Y	N						
X							

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.

/***/** First amended sections **/***/

5.6.1 Accessing Home Network provided services

The following functionality and requirements have been identified:

- It shall be possible to support multiple service authorizations after a successful WLAN authentication/authorisation (i.e. EAP success).
- The Service authorisation procedure should, as far as possible, be independent from WLAN Access authentication and authorisation.
- The routing policy applied at WLAN Access Authentication and Authorisation may include policy determining whether the user has IP connectivity to the PDGs used for access to external IP networks.
- It shall be possible to permit access to different services simultaneously.
- Service authorization information shall be protected
- The Access Point Name (APN) concept defined in 3GPP TS 23.003 shall be used for WLAN interworking authorization (namely W-APN). In a service authorization procedure:
 - W-APN selection and authorization is an end-to-end procedure between the WLAN UE and the HPLMN (the service authorization decision is made by the 3GPP AAA Server *based on subscription information retrieved from the HSS/HLR*).

Editor's note: the use of subscription information is FFS.

- The WLAN UE shall use W-APN to indicate to the network the service or set of services it wants to access.
- The PDG selection shall be performed under control of the 3GPP Home Network by means of answers to DNS query for the requested W-APN ~~and tunnel redirection~~. The selection is based on the requested W-APN and user subscription information. The WLAN UE shall choose the IP address of the PDG if there is more than one PDG address in the answer to DNS query.

The mechanism to select the PDG by the home network is out of scope of this specification, since it depends on the operator's preference.

- The PDG needs to know the authorized W-APN to select the external network, i.e. Wi interface.

5.6.2 Accessing Visited Network provided services

When accessing visited network provided services, additional principles below apply:

- In order for the WLAN UE to be able to use W-APNs in the VPLMN, the 3GPP AAA Server needs to pass to the 3GPP AAA Proxy the authorized W-APN and service related information which is required by the Visited Network to perform the service.
- The W-APN needs to be understood by both the Home and the Visited Networks.
- The V-PDG selection is shall be under control of the 3GPP Visited Network by means of answers to DNS query for the requested W-APN ~~and tunnel redirection~~. The selection is based on the authorized W-APN and service related information. The WLAN UE shall choose the IP address of the PDG if there is more than one PDG address in the answer to DNS query.

The mechanism to select the V-PDG by the Visited Network is out of scope of this specification, since it depends on the operator's preference.

- The selected PDG in the Visited Network needs to know the authorized W-APN to select the external network, i.e. Wi interface.

/***** Next amended section *****/

6.2.6 Packet Data Gateway

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

3GPP PS based services are accessed via a Packet Data Gateway. 3GPP PS based services may be accessed via a Packet Data Gateway in the user's Home Network or a PDG in the selected VPLMN. The process of authorisation and service selection (e.g. W-APN selection) and subscription checking determines whether a service shall be provided by the home network or by the visited network. The resolution of the IP address of the Packet Data Gateway providing access to the selected service will be performed in the PLMN functioning as the home network (in the VPLMN or HPLMN). If the PDG is intended to support connections from WLAN UEs using IPv4 and IPv6 local addresses, it shall be equipped with a dual IP stack.

Successful activation of a selected service results in:

- Determination of the Packet Data Gateway IP address used by the WLAN UE;
- Allocation of a WLAN UE's remote IP address to the WLAN UE (if one is not already allocated);
- Registration of the WLAN UE's local IP address with the Packet Data Gateway and binding of this address with the WLAN UE's remote IP address.

The Packet Data Gateway:

- Contains routing information for WLAN-3G connected users;
- Routes the packet data received from/sent to the PDN to/from the WLAN-3G connected user;
- Performs address translation and mapping;
- Performs de-capsulation and encapsulation;
- accepts or rejects the requested W-APN according to the decision made by the 3GPP AAA Server;
- ~~redirects the tunnel establishment request towards another PDG if this is indicated to be done by the 3GPP AAA Server~~

Allows allocation of the WLAN UE's remote IP address;

- Relays the WLAN UE's remote IP address allocated by an external IP network to the WLAN UE, when external IP network address allocation is used.
- Performs registration of the WLAN UE's local IP address and binding of this address with the WLAN UE's remote IP address;
- Provides procedures for unbinding a WLAN UE's local IP address with the WLAN UE's remote IP address;
- Provides procedures for authentication and prevention of hijacking (i.e. ensuring the validity of the WLAN UE initiating any binding of the WLAN UE's local IP address with the WLAN UE's remote IP address, unbinding etc.)
- May filter out unauthorised or unsolicited traffic with packet filtering functions. All types of message screening are left to the operators' control, e.g. by use of Internet firewalls.
- Generates per user charging information.
- Delivers the mapping of a user identifier and a tunnel identifier to the AAA Proxy.
- Generates charging information related to user data traffic for offline and online charging purposes.

- May apply IP flow based bearer level charging [13], [15], e.g. in order to differentiate or suppress WLAN bearer charging for 3GPP PS based services.

Annex F describes how PDG functionality can be provided by re-using existing unmodified GGSN functionality.

// Next amended section /**/**

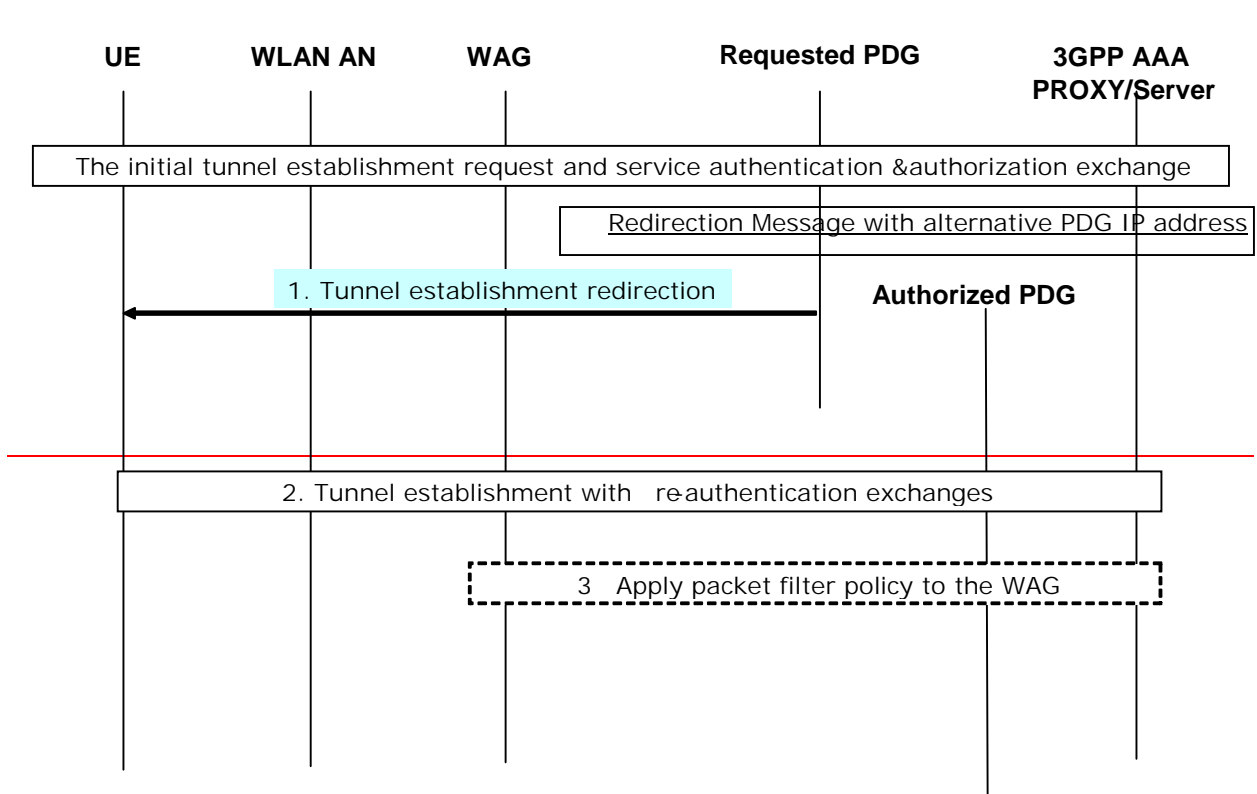
7.9.1 VoidRedirection

~~In the above procedures, the WLAN UE may not be authorised to access the requested W-APN through the selected PDG. This may occur for the following reasons:~~

- ~~(i) The requested W-APN is not supported by the network~~
- ~~(ii) The user is not subscribed to the requested W-APN~~
- ~~(iii) The PDG is in the VPLMN and the user's subscription indicates that VPLMN access is not allowed for the requested W-APN~~
- ~~(iv) The operator does not wish to include all PDG addresses in DNS and so (for example) all initial requests are handled by a default PDG which may not be the correct PDG for the requested W-APN~~
- ~~(v) The user has not supplied an explicit requested W-APN. This is treated as a request for the first appropriate subscribed W-APN, or for a network default W-APN (if a wildcard W-APN is included in the subscription), as per 23.060 Annex A.~~

~~In cases (i), (ii) and (iii), the request is simply rejected. In case (iii), the WLAN UE may attempt tunnel establishment to the HPLMN as described in Section 7.8.~~

~~In cases (iv) and (v) above, the AAA Server may determine that the user is authorised to access the W-APN through a different PDG. The 3GPP AAA Server then sends the IP address of the alternative PDG (i.e the authorized PDG) to the requested PDG. The IP address of the alternative PDG is then returned to the WLAN UE in the rejection message from PDG to WLAN UE. In this case the WLAN UE shall attempt a new tunnel establishment request to the provided PDG address.~~



~~Figure 7.11: Message flow of the tunnel establishment with redirection~~

~~During the step 2.3/3.3 in the procedure of clause 7.9, the 3GPP AAA Server authorizes the service to the WLAN UE, and sends the authorization information to the requested PDG. If requested PDG is not authorized to provide the service then the AAA server sends a new PDG (Authorized PDG) address and the authorized W-APN, then the following steps performed:~~

- ~~1. The requested PDG sends tunnel redirection request to the UE with service authorization information (authorized PDG address and authorized W-APN).~~
- ~~2. The WLAN UE sends an end-to-end tunnel establishment request to the Authorized PDG. Then end-to-end tunnel establishment begins between the Authorized PDG and the WLAN UE. A full or fast re-authentication method should be used during this tunnel establishment.~~
- ~~3. The Authorized PDG provides filtering information to the WAG as it is specified in clause 7.9.~~

CHANGE REQUEST

23.234 CR 083 # rev 2 # Current version: 6.2.0

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	# Charging in WLAN interworking architecture		
Source:	# Nokia, Huawei		
Work item code:	# WLAN, CH-FBC	Date:	# 10/11/2004
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 charging reference points for WLAN 3GPP IP Access are missing. The naming of the offline charging elements are not inline with the Release 6 charging architecture [TS32.240], and the definition of the charging elements is missing.
Summary of change:	# It is proposed to introduce new reference points between the PDG and the OCS and between the PDG and the Offline Charging System. The names of the charging functions are corrected and their definitions are added. An editorial clean up of the changed charging procedures is also provided.
Consequences if not approved:	# The charging for WLAN 3GPP IP Access will not be possible. The specification will contradict to the Release 6 charging architecture.

Clauses affected:	# 2, 3.2, 3.3, 6.1.1, 6.1.2, 6.2.2, 6.2.3, 6.3.5, 7.7, 7.8 new clauses: 6.2.8, 6.2.9, 6.3.15, 6.3.16						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px;">Y</td> <td style="width: 20px;">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="width: 20px;">Y</td> <td style="width: 20px;">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> Test 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="width: 20px;">Y</td> <td style="width: 20px;">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> O&M Specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	#	
Y	N						
<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.

/***** 1st Ammended Section: New reference */

2 References

[aa] [3GPP TS 32.252: "Telecommunication management; Charging management; Wireless Local Area Network \(WLAN\) charging"](#).

[bb] [3GPP TS 32.296: "Telecommunication management; Charging management; Online Charging System \(OCS\) applications and interfaces"](#)

/***** Next amended sections *****/

3.2 Symbols

For the purposes of the present document the following symbols apply:

D'	Reference point between a pre-R6 HSS/HLR and a 3GPP AAA Server
Dw	Reference point between a 3GPP AAA Server and an SLF
Gr'	Reference point between a pre-R6 HSS/HLR and a 3GPP AAA Server
Wa	Reference point between a WLAN Access Network and a 3GPP AAA Server/Proxy (charging and control signalling)
Wd	Reference point between a 3GPP AAA Proxy and a 3GPP AAA Server (charging and control signalling)
Wf	Reference point between an Offline Charging System CGw/CCF and a 3GPP AAA Server/Proxy
Wg	Reference point between a 3GPP AAA Server/Proxy and WAG
Wi	Reference point between a Packet Data Gateway and an external IP Network
Wm	Reference point between a Packet Data Gateway and a 3GPP AAA Server or 3GPP AAA proxy
Wn	Reference point between a WLAN Access Network and a WLAN Access Gateway
Wp	Reference point between a WLAN Access Gateway and a Packet Data Gateway
Wo	Reference point between a 3GPP AAA Server and an OCS
Wu	Reference point between a WLAN UE and a Packet Data Gateway
Wx	Reference point between an HSS and a 3GPP AAA Server
Wy	Reference point between a PDG and an OCS
Wz	Reference point between a PDG and an Offline Charging System

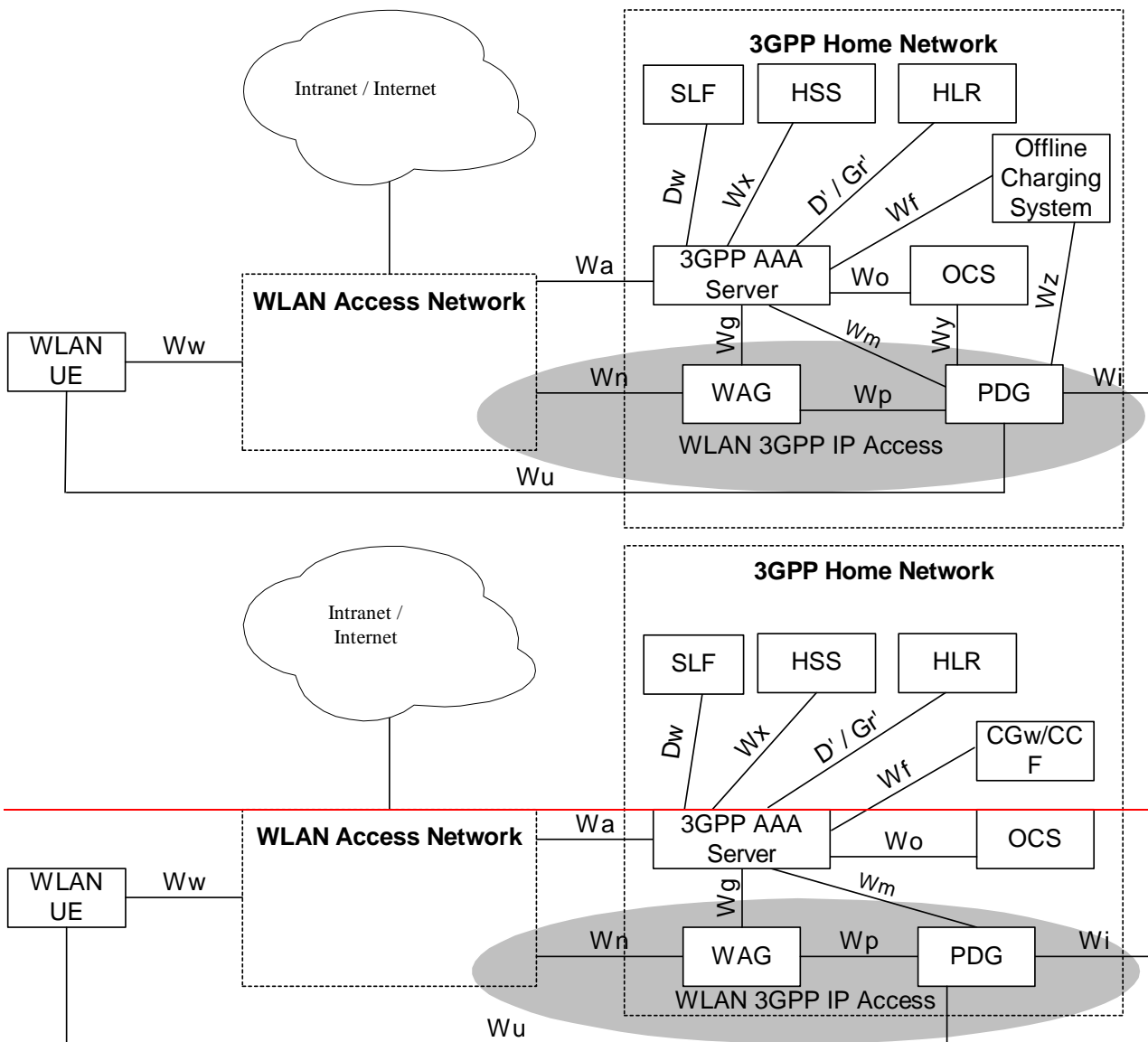
3.3 Abbreviations

AAA	Authentication, Authorisation and Accounting
ACL	Access Control List
AKA	Authentication and Key Agreement
AP	Access Point
APN	Access Point Name
CCF	Charging Collection Function
CGw	Charging Gateway
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
FQDN	Fully Qualified Domain Name
GGSN	Gateway GPRS Support Node
GTP	GPRS Tunnelling Protocol
HLR	Home Location Register
HPLMN	Home PLMN
HSS	Home Subscriber Server
IEEE	Institute of Electrical and Electronics Engineers

IP	Internet Protocol
IP-SM-GW	IP Short Message Gateway
ISP	Internet Service Provider
I-WLAN	Interworking WLAN
NAI	Network Access Identifier
NAT	Network Address Translation
OCS	Online Charging System
PDA	Personal Digital Assistant
PDG	Packet Data Gateway
PLMN	Public Land Mobile Network
SIM	Subscriber Identity Module
SSID	Service Set ID
VLAN	Virtual Local Area Network
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
USIM	UMTS SIM
SSID	Service Set Identifier
VPLMN	Visited PLMN
WAG	WLAN Access Gateway
W-APN	WLAN APN
WLAN	Wireless Local Area Network
WLAN AN	WLAN Access Network
WLAN UE	WLAN User Equipment

/*/** Next amended sections **/***/**

6.1.1 Non Roaming WLAN Inter-working Reference Model



Note: The shaded area refers to WLAN 3GPP IP Access functionality.

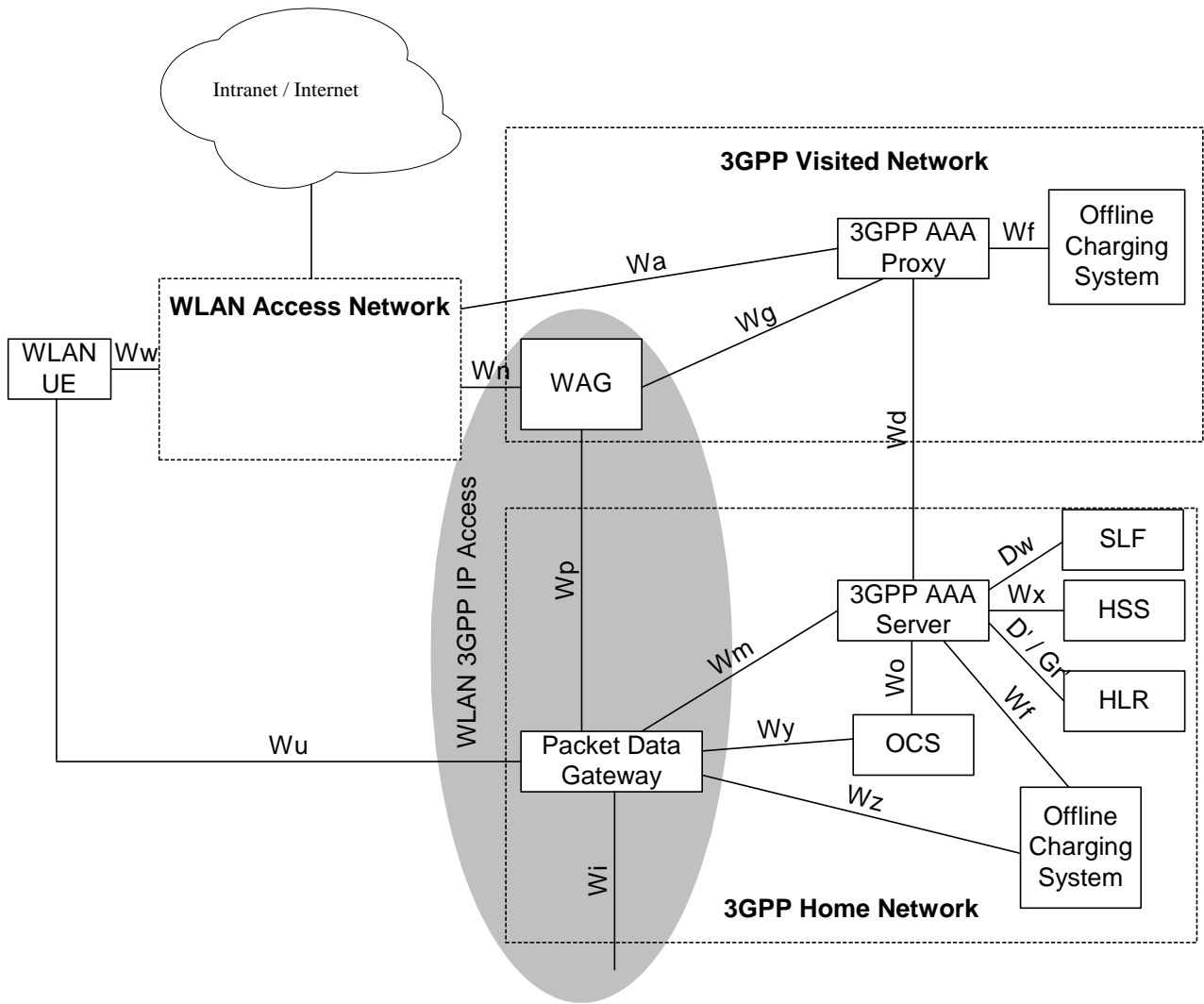
Figure 6.1: Non-roaming reference model

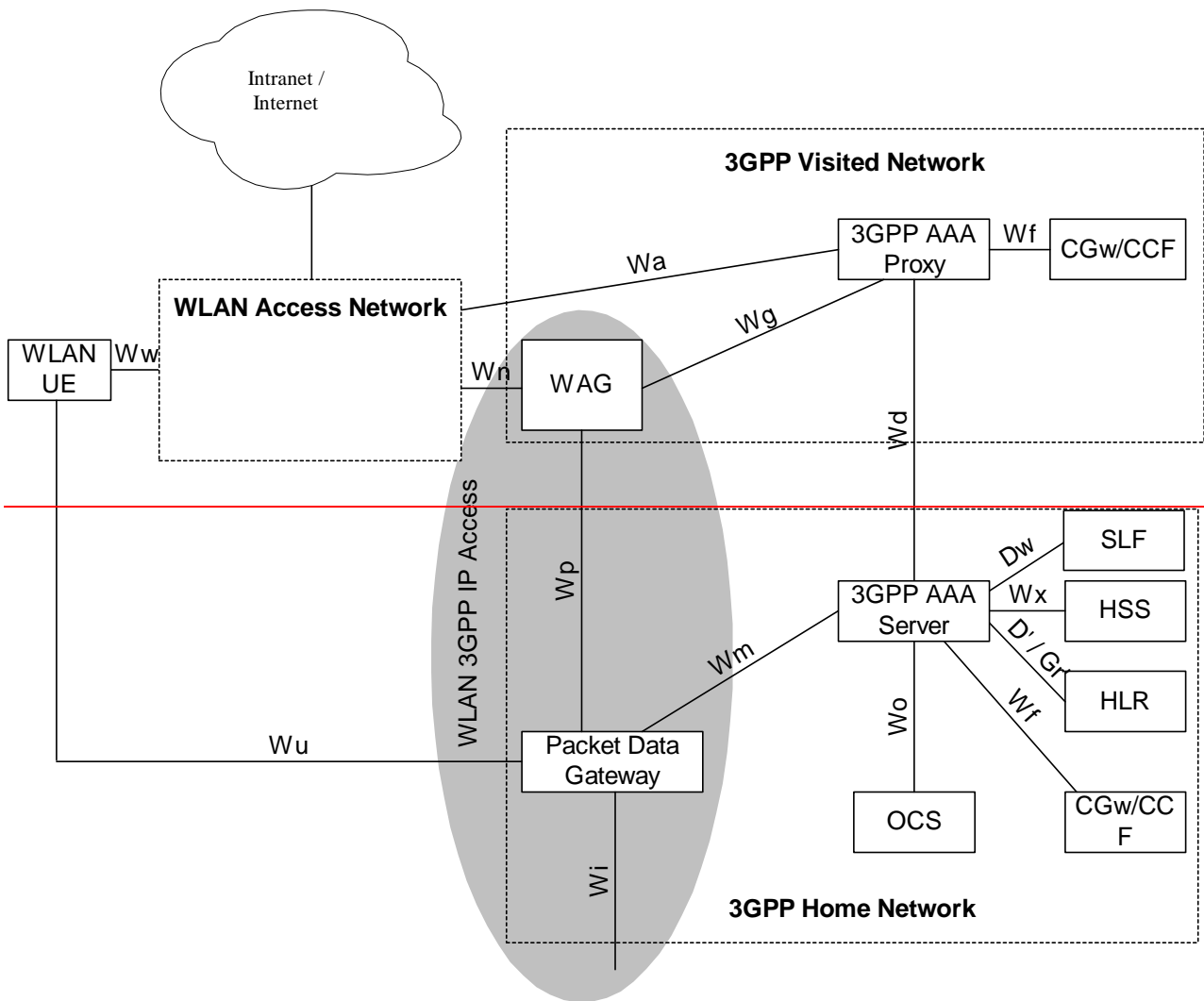
6.1.2 Roaming WLAN Inter-working Reference Model

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 home 3GPP network interfaces to other 3GPP networks via the inter-operator Wd reference point.

The 3GPP AAA proxy relays access control signalling and accounting information to the home 3GPP AAA Server using the Wd reference point.

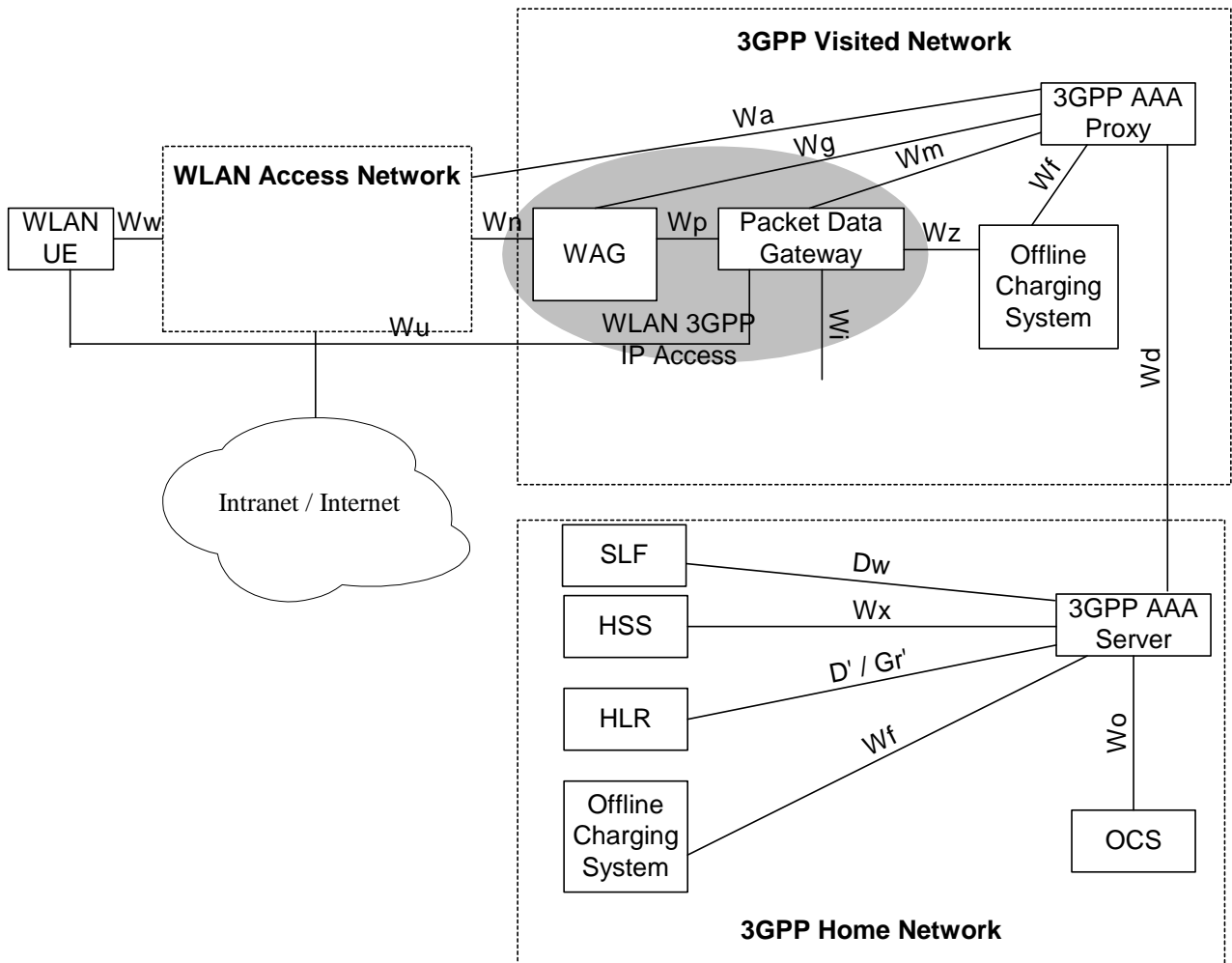
It can also issue charging records to the visited network [CGw/CCF-Offline Charging System](#) when required. The 3GPP network interfaces to WLAN Access Networks via the Wa reference point.

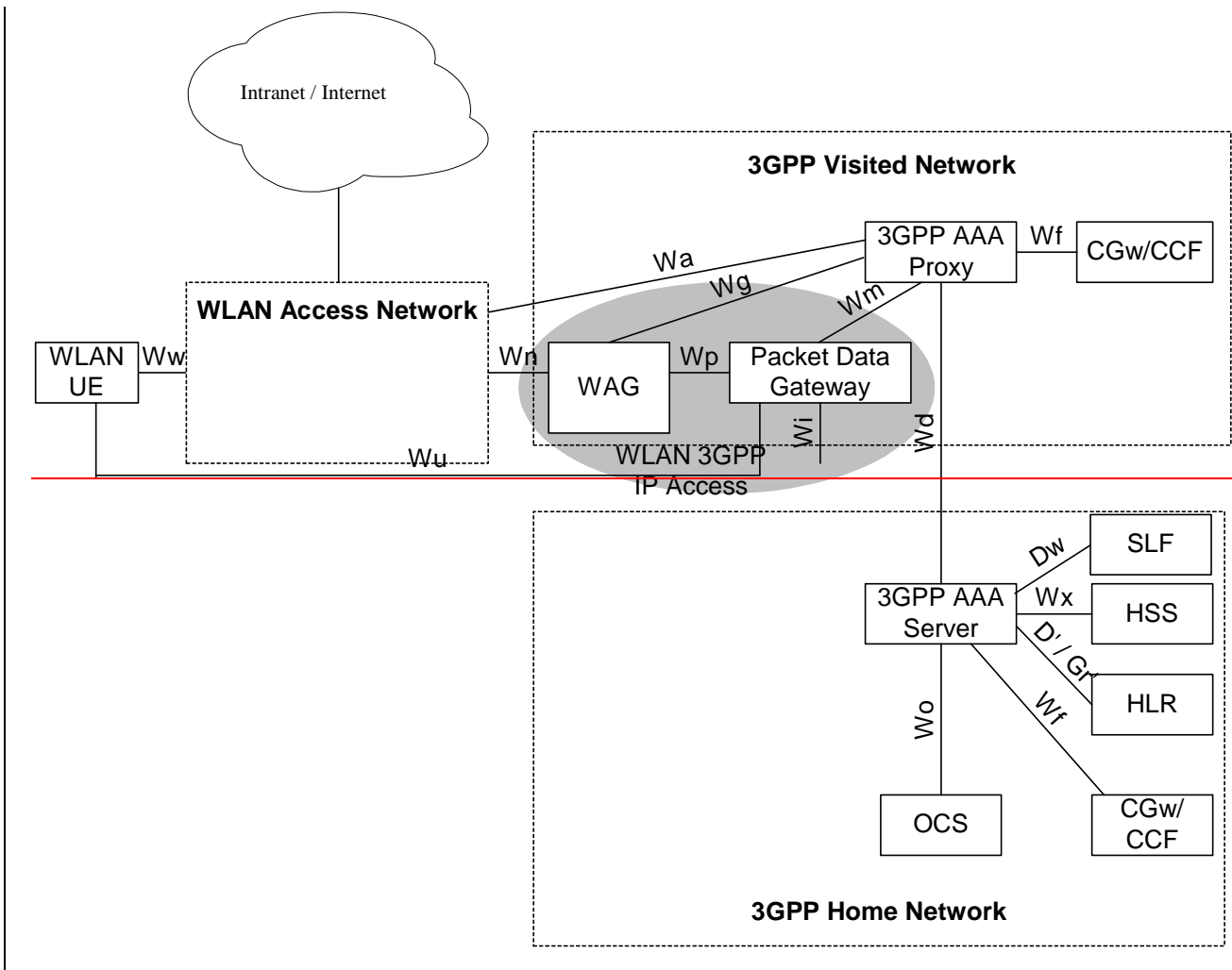




Note: The shaded area refers to WLAN 3GPP IP Access functionality.

Figure 6.2a: Roaming reference model - 3GPP PS based services provided via the 3GPP Home Network





Note: The shaded area refers to WLAN 3GPP IP Access functionality.

Figure 6.2b: Roaming reference model - 3GPP PS based services provided via the 3GPP Visited Network

// Next amended sections /**/**

6.2.2 3GPP AAA Proxy

The 3GPP AAA Proxy represents a proxying and filtering function that resides in the Visited 3GPP Network. The 3GPP AAA Proxy functions include:

- Relaying the AAA information between WLAN and the 3GPP AAA Server.
- Enforcing policies derived from roaming agreements between 3GPP operators and between WLAN operator and 3GPP operator
- Providing access scope limitation information to the WLAN based on authorization information from the Home network
- Reporting per-user charging/accounting information to the VPLMN ~~CCF/CGw~~ [Offline Charging System](#) for roaming users
- Service termination (O&M initiated termination from visited network operator)

- Protocol conversion when the Wa and Wd reference points do not use the same protocol

For WLAN 3GPP IP Access only:

- 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.
- Receiving authorization information related to subscriber requests for W-APNs in the Home or Visited network
- Authorization of access to Visited network W-APNs according to local policy
- Receiving the suitable policy enforcement information from AAA-Server and provides it to the WAG in VPLMN.
- May provide suitable routing enforcement information to WLAN AN.

The 3GPP AAA Proxy functionality can reside in a separate physical network node, it may reside in the 3GPP AAA Server or any other physical network node.

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.
- Communicates authorization information to the WLAN 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 ~~CCF/CG~~[wOffline 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 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.

/*/*/*/*/*/*/*/* New sections /*/*/*/*/*/*/*/*

6.2.8 Offline Charging System

The Offline Charging System is within the 3GPP network. The mapping of the Offline Charging System in the Release 6 charging architecture is specified in 3GPP TS 32.252 [aa].

6.2.9 Online Charging System

The Online Charging System (OCS) is located within the 3GPP network. The OCS is described in 3GPP TS 32.296 [bb].

// Next amended sections /**/**

6.3.5 Wf reference point

The Wf reference point is located between 3GPP AAA Server/Proxy and 3GPP Offline Charging System~~Gateway-Function (CGF)/Charging Collection Function (CCF)~~. The prime purpose of the protocols crossing this reference point is to transport/forward offline charging information towards 3GPP operator's Offline Charging System ~~Gateway/Charging collection function~~ located in the visited network or home network where the subscriber is residing.

The information forwarded to the Offline Charging System~~Gateway/Charging collection function~~ is typically used for:

- Generating bills for offline charged subscribers by the subscribers' home operator.
- Calculation of inter-operator accounting from all roaming users. This inter operator accounting is used to settle the payments between visited and home network operator and/or between home/visited network and WLAN.

The functionality of the reference point is to transport:

- WLAN access-related charging data per WLAN user.

// New sections /**/**

6.3.15 Wy reference point

The Wy reference point is used by a PDG to communicate with an Online Charging System (OCS). The purpose of the protocol(s) crossing this reference point is to transport online charging related information about WLAN 3GPP IP Access so as to perform credit control for the online charged subscriber.

6.3.16 Wz reference point

The Wz reference point is used by a PDG to communicate with an Offline Charging System. The purpose of the protocol(s) crossing this reference point is to transport offline charging related information about WLAN 3GPP IP Access.

// New sections /**/**

7.7 Charging offline charged subscribers

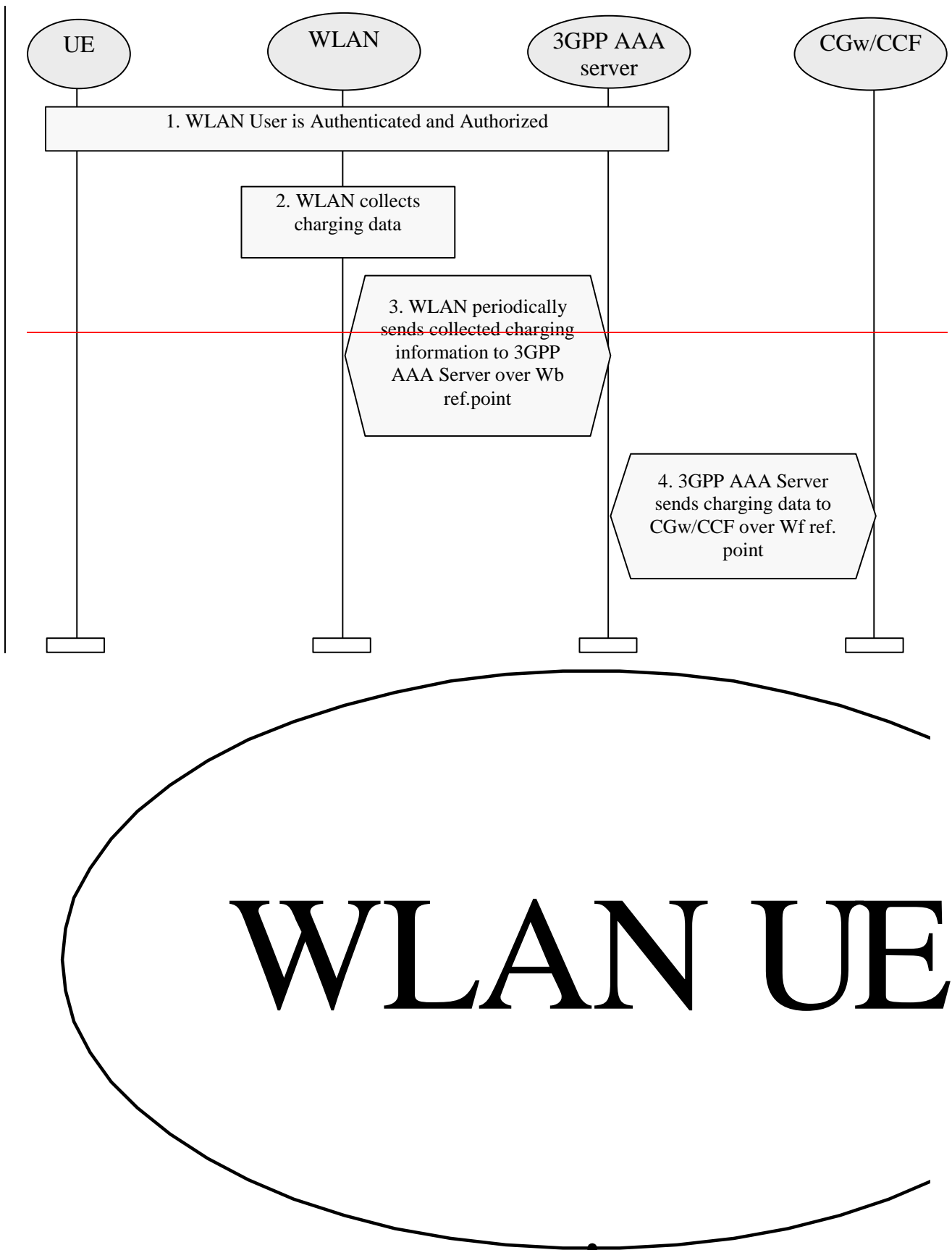
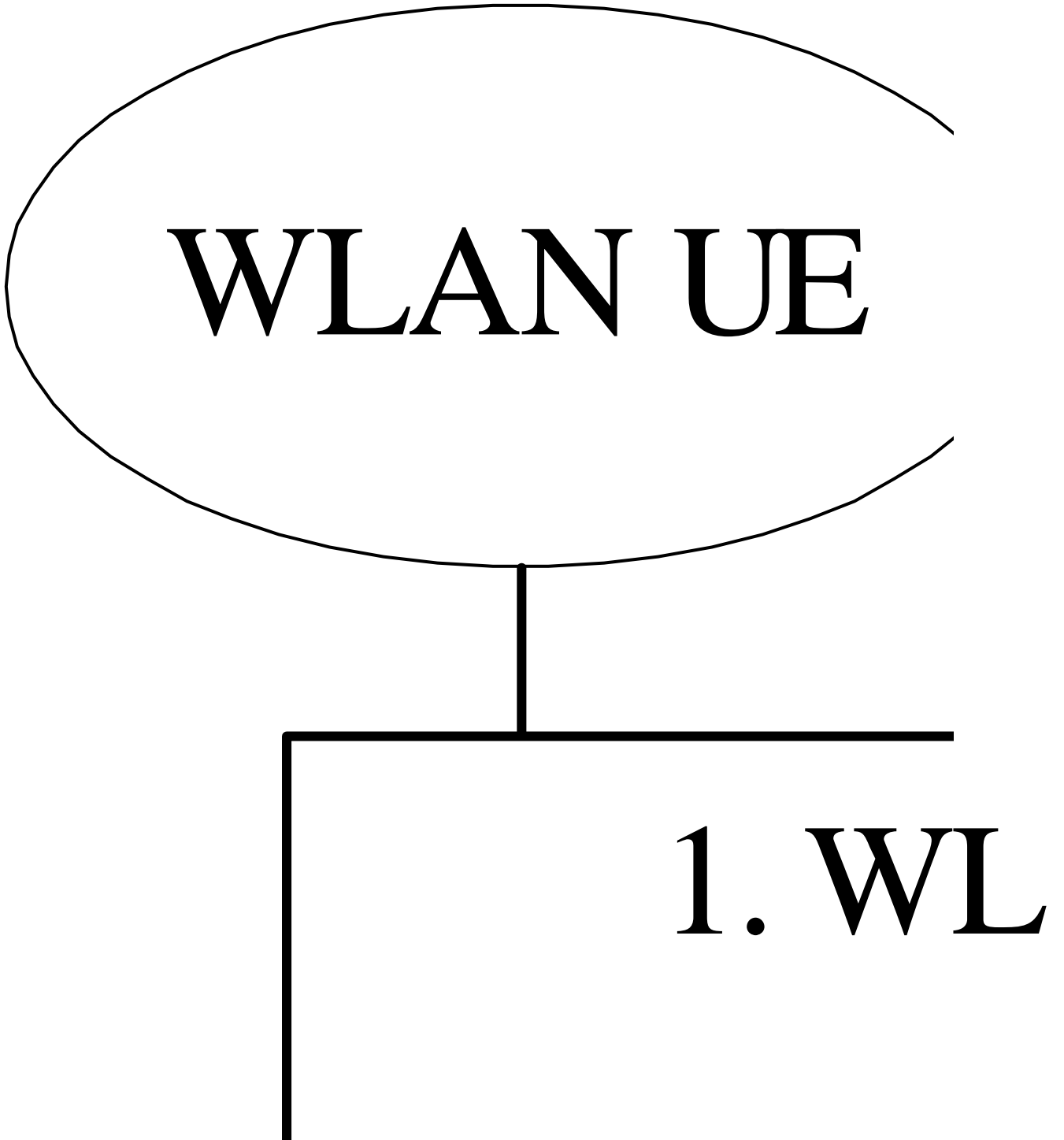


Figure 7.8: Charging Procedure for Offline Charged Subscribers

1. [The](#) WLAN user is authenticated and authorized for WLAN access. User profile is downloaded into 3GPP AAA ~~server~~[Server](#). Part of the profile is information that the user is to be offline charged.
2. [The](#) WLAN ~~access-network~~[AN](#) collects charging data related to access or services locally consumed.
3. [The](#) WLAN ~~access-network~~[AN](#) periodically forwards collected charging information to the 3GPP AAA ~~server~~[Server](#) over Wb reference point.
4. [The](#) 3GPP AAA ~~server~~[Server](#) forwards charging information to the [Online Charging System](#)~~CGw/CCF~~ over the Wf reference point.

Note: In visited network the 3GPP AAA Proxy may also periodically report the usage of resources to the local ~~CGw/CCF~~[Online Charging System](#) over [the](#) Wf reference point.

7.8 Charging online charged subscribers



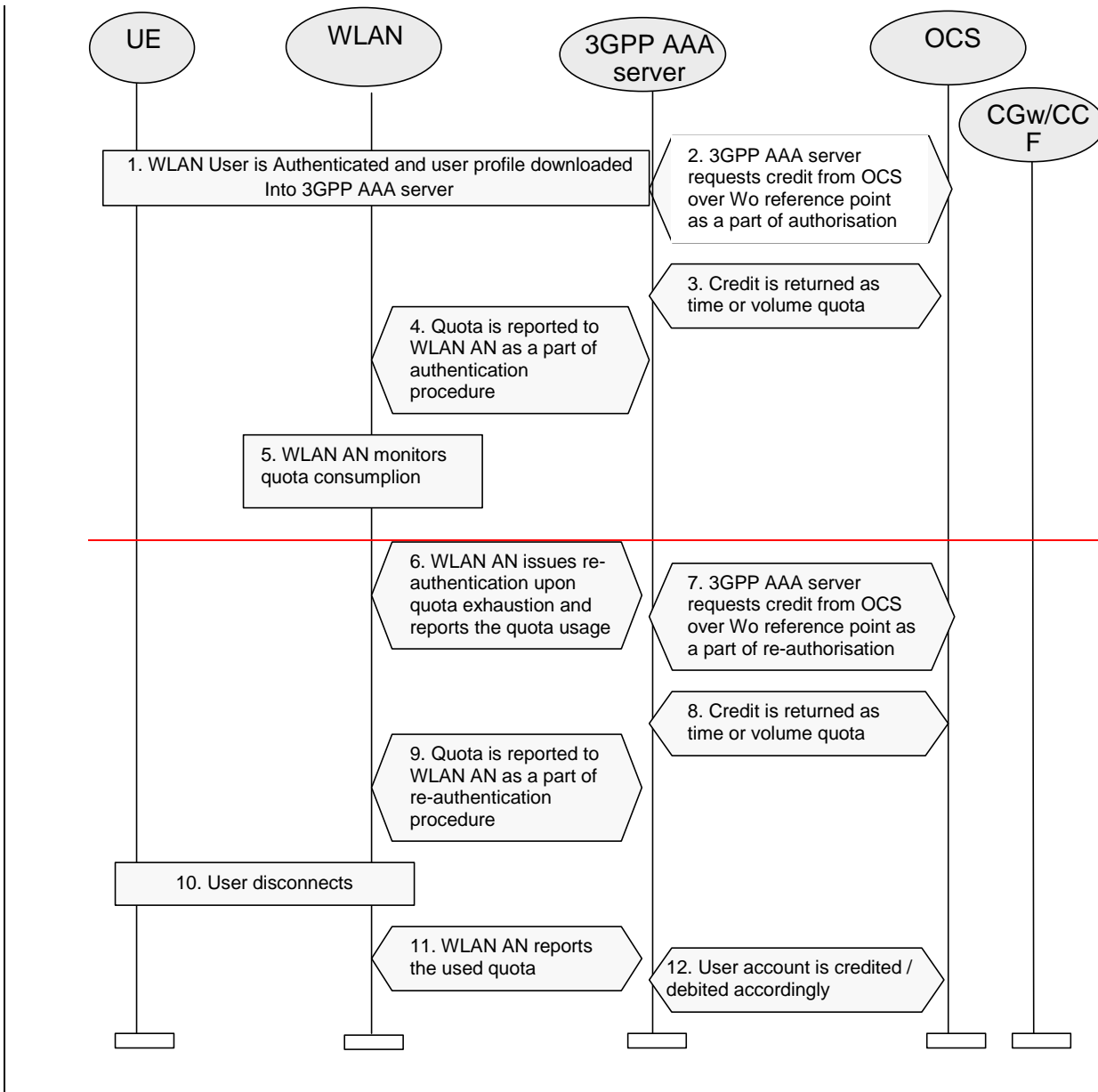


Figure 7.9: Charging Procedure for Online Charged Subscribers

1. The WLAN user is authenticated and authorized for WLAN access. User profile is downloaded into 3GPP AAA server. Part of the profile is information that the user is to be online charged.
2. The 3GPP AAA server requests online charging credit from the OCS.
3. The OCS returns credit as time and/or volume quota.
4. The Allocated quota is indicated to the WLAN AN.
5. The WLAN AN monitors the quota consumption.
6. When quota is almost used, the WLAN AN issues re-authentication message over Wa reference point. Used quota is indicated in the request.
7. The 3GPP AAA Server requests more credit from the OCS.
8. The OCS returns credit as time and/or volume quota.
9. The Allocated new quota is indicated to the WLAN AN.
10. The User disconnects from WLAN AN.

11. [The](#) WLAN AN reports the used quota to [the](#) 3GPP AAA Server over Wa reference point.

12. [The](#) ~~User~~-[user](#) account is debited / credit according the usage information in the final message.

Note: In visited network the 3GPP AAA Proxy may also periodically report the usage of resources to the local ~~CGw/CCF~~[Online Charging System](#) over Wf reference point. In home network the 3GPP AAA Server may also report the usage to the ~~CGw/CCF~~[Online Charging System](#) over the Wf reference point using offline charging procedures for statistical or other purposes.

CHANGE REQUEST

⌘ **23.234 CR 101** ⌘ rev **-** ⌘ Current version: **6.2.0** ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Remove duplicated charging requirement for the PDG		
Source:	⌘ Siemens		
Work item code:	⌘ WLAN	Date:	⌘ 15/11/2004
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:	⌘ Requirement to generate per user charging information is duplicated in chapter 6.2.6 of TS 23.234.		
Summary of change:	⌘ Remove duplicated charging requirement for the PDG in chapter 6.2.6.		
Consequences if not approved:	⌘ Misleading and confusing requirements for stage 3 work.		

Clauses affected:	⌘ 6.2.6										
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;"> </td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;"> </td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;"> </td> <td style="text-align: center;">X</td> </tr> </table>	Y	N		X		X		X	Other core specifications ⌘ Test specifications O&M Specifications	⌘
Y	N										
	X										
	X										
	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.

***** BEGIN OF MODIFIED SECTION *****

6.2.6 Packet Data Gateway

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

3GPP PS based services are accessed via a Packet Data Gateway. 3GPP PS based services may be accessed via a Packet Data Gateway in the user's Home Network or a PDG in the selected VPLMN. The process of authorisation and service selection (e.g. W-APN selection) and subscription checking determines whether a service shall be provided by the home network or by the visited network. The resolution of the IP address of the Packet Data Gateway providing access to the selected service will be performed in the PLMN functioning as the home network (in the VPLMN or HPLMN). If the PDG is intended to support connections from WLAN UEs using IPv4 and IPv6 local addresses, it shall be equipped with a dual IP stack.

Successful activation of a selected service results in:

- Determination of the Packet Data Gateway IP address used by the WLAN UE;
- Allocation of a WLAN UE's remote IP address to the WLAN UE (if one is not already allocated);
- Registration of the WLAN UE's local IP address with the Packet Data Gateway and binding of this address with the WLAN UE's remote IP address.

The Packet Data Gateway:

- Contains routing information for WLAN-3G connected users;
- Routes the packet data received from/sent to the PDN to/from the WLAN-3G connected user;
- Performs address translation and mapping;
- Performs de-capsulation and encapsulation;
- accepts or rejects the requested W-APN according to the decision made by the 3GPP AAA Server;
- redirects the tunnel establishment request towards another PDG if this is indicated to be done by the 3GPP AAA Server

Allows allocation of the WLAN UE's remote IP address;

- Relays the WLAN UE's remote IP address allocated by an external IP network to the WLAN UE, when external IP network address allocation is used.
- Performs registration of the WLAN UE's local IP address and binding of this address with the WLAN UE's remote IP address;
- Provides procedures for unbinding a WLAN UE's local IP address with the WLAN UE's remote IP address;
- Provides procedures for authentication and prevention of hijacking (i.e. ensuring the validity of the WLAN UE initiating any binding of the WLAN UE's local IP address with the WLAN UE's remote IP address, unbinding etc.)
- May filter out unauthorised or unsolicited traffic with packet filtering functions. All types of message screening are left to the operators' control, e.g. by use of Internet firewalls.

~~Generates per user charging information.~~

- Delivers the mapping of a user identifier and a tunnel identifier to the AAA Proxy.
- Generates charging information related to user data traffic for offline and online charging purposes.
- May apply IP flow based bearer level charging [13], [15], e.g. in order to differentiate or suppress WLAN bearer charging for 3GPP PS based services.

Annex F describes how PDG functionality can be provided by re-using existing unmodified GGSN functionality.

6.2.7 Subscription Locator Function (SLF)

***** END OF MODIFIED SECTION *****

CHANGE REQUEST

23.234 CR 099 # rev 1 # Current version: 6.2.0

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	#	Addition of reference	
Source:	#	ZTE Corporation	
Work item code:	#	WLAN	Date: # 5/11/2004
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 section F3.0, some messages are used as references from TS 29060, but this TS does not list in the reference section. And the description on the reference is by brackets and editor notes, it is not formal.
Summary of change:	#	Addition of reference 29060, and modification of relative sentences.
Consequences if not approved:	#	The reference is not formal.

Clauses affected:	#	Annex F3.0								
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;">#</td> <td style="text-align: center;">X</td> </tr> </table> Other core specifications # <table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">#</td> <td style="width: 20px; text-align: center;">X</td> </tr> </table> Test specifications <table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">#</td> <td style="width: 20px; text-align: center;">X</td> </tr> </table> O&M Specifications	Y	N	#	X	#	X	#	X
Y	N									
#	X									
#	X									
#	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.

***** BEGIN OF 1st MODIFIED SECTION *****

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
 - For a specific reference, subsequent revisions do not apply.
 - For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.
- [1] 3GPP TS 21.905: "Vocabulary for 3GPP Specifications".
 - [2] 3GPP TS 22.101: "Service principles".
 - [3] 3GPP TR 22.934: "Feasibility study on 3GPP system to WLAN interworking".
 - [4] 3GPP TS 23.002: "Network architecture".
 - [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] 3GPP TR 23.934: "3GPP system to WLAN Interworking; Functional and architectural definition".
 - [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] 3GPP TS 29.329: "Sh Interface based on the Diameter protocol; Protocol details".
 - [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] RFC2284: "PPP Extensible Authentication Protocol (EAP)"
 - [17] RFC 2486: "The Network Access Identifier"
 - [18] J. Caron, "DNS Based Roaming", <http://www.ietf.org/internet-drafts/draft-caron-dns-based-roaming-00.txt>, April 2002, (work in progress)
 - [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 29.060: "GPRS; GTP across the Gn and Gp interface"](#)

***** END OF 1st MODIFIED SECTION *****

***** BEGIN OF 2nd MODIFIED SECTION *****

F.3 Gn' considerations

Editor's note: The Gn' procedures shall comprise a subset of the Gn reference point procedures. There shall be no enhancements to Gn applied.

F.3.0 General

A minimum set of interworking procedures over the Gn' reference point would include the following messages [from the Gn reference point messages and procedures specified in 3GPP TS 29.060 \[27\]](#):

- Create PDP Context Request / Response;
- Update PDP Context Request / Response;
- Delete PDP Context Request / Response;
- Error Indication;
- Version Not Supported;
- GTP Ppayload Fforwarding (~~specified in 29.060~~).

~~Note: — The messages above form a true subset of the Gn reference point messages and procedures.~~

The TTG must be provided with information, e.g. MCC and MNC of the VPLMN, needed to include the RAI Information Element within the messaging to the GGSN to enable simple position based billing and to enable the HPLMN to restrict certain content to those countries depending on that country's legal requirements.

The assignment of the remote IP address should be done from a pool of IP address belonging to the GGSN/RADIUS server or at least "address range coordinated" with those to enable correct routing on Gi. The End-user-address IE must be provided in the Create PDP Context Request. If address assignment is done by the GGSN/RADIUS, the IE shall be empty in the request message (indicating dynamic address assignment by GGSN/RADIUS), which makes the GGSN/RADIUS assign and return an IP address in the Response message.

The NSAPI value to be provided over the Gn' reference point is allocated in the TTG, see subclause F.5.

If a certain charging profile should be applied in GGSN the Charging Characteristics IE may be included. In that case this information needs to be available in the TTG. The Charging Characteristics may be used to give special charging for WLAN in the GGSN. The Charging Characteristic is defined per subscriber and is stored in HLR. For GPRS the Charging Characteristic is sent to SGSN at attach and is forwarded to GGSN at PDP context creation. For WLAN interworking, the TTG may for example get this information from HLR via the 3GPP AAA Server.

***** END OF 2nd MODIFIED SECTION *****

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.234 CR 110** ⌘ rev **1** ⌘ Current version: **6.2.0** ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Removal of unused references		
Source:	⌘ Ericsson		
Work item code:	⌘ WLAN	Date:	⌘ 15/11/2004
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:	⌘ During editorial cleanup of TS 23.234 it was spotted that many of the listed references are not used on the specification. In order to improve the quality, it is suggested to remove these.
Summary of change:	⌘ Removal of unused references.
Consequences if not approved:	⌘ Unused references listed in the specification.

Clauses affected:	⌘ 2						
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"/>						
	<input checked="" type="checkbox"/>	Test specifications					
	<input checked="" type="checkbox"/>	O&M Specifications					
Other comments:	⌘ Note that CR 92 (S2-043068) also updates section 2.						

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 changes ****

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] ~~3GPP TS 21.905: "Vocabulary for 3GPP Specifications"~~[.void](#)
- [2] ~~3GPP TS 22.101: "Service principles"~~[.void](#)
- [3] ~~3GPP TR 22.934: "Feasibility study on 3GPP system to WLAN interworking"~~[.void](#)
- [4] ~~3GPP TS 23.002: "Network architecture"~~[.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] ~~3GPP TR 23.934: "3GPP system to WLAN Interworking; Functional and architectural definition"~~[.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] ~~3GPP TS 29.329: "Sh Interface based on the Diameter protocol; Protocol details"~~[.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] ~~RFC2284: "PPP Extensible Authentication Protocol (EAP)"~~[.void](#)
- [17] RFC 2486: "The Network Access Identifier"
- [18] ~~J. Caron, "DNS Based Roaming", <http://www.ietf.org/internet-drafts/draft-caron-dns-based-roaming-00.txt>, April 2002, (work in progress)~~[.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-01, work in progress.~~[void](#)
- [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.
- [7] IETF Internet-Draft: "EAP AKA Authentication" draft-arkko-pppext-eap-aka-11 (October 2003).
- [8] IETF Internet-Draft: "EAP SIM Authentication" draft-haverinen-pppext-eap-sim-12 (October 2003).
- [9] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".
- [10] 3GPP TS 32.252: "Telecommunication management; Charging management; Wireless Local Area Network (WLAN) charging".
- [25] 3GPP TS 22.234: "Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking"

**** End of changes ****

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.234 CR 094** ⌘ rev **1** ⌘ Current version: **6.2.0** ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Revision for PLMN selection procedure		
Source:	⌘ Telecom Italia S.p.A., Reasearch In Motion		
Work item code:	⌘ WLAN	Date:	⌘ 17/11/2004
Category:	⌘ F	Release:	⌘ Rel-6
	<i>Use <u>one</u> of the following categories:</i> 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 .		<i>Use <u>one</u> of the following releases:</i> 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:	⌘ Present TS 23.234 has some text not aligned to the PLMN selection procedures. So the CR proposes to improve the text in order to have coherent definition through the whole TS.
Summary of change:	⌘ New text has been added in section 5.4.3.2 stating that network advertisement information is returned to the WLAN UE by the first AAA Proxy/Server.
Consequences if not approved:	⌘ Misunderstanding due to not coherent requirements

Clauses affected:	⌘ 5.4.3.2						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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"/>						
	<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.

First Changes

5.4.3 PLMN Advertisement and Selection

5.4.3.1 General

The following principles shall be used in PLMN Advertisement and Selection:

- This procedure takes place after association with an AP
- The user shall be able to select the Visited Network
- Use the NAI for routing of AAA messages.
- Have low latency and overhead.
- Use existing EAP mechanisms, if possible.
- Be extensible to permit advertisement of WLAN characteristics other than the PLMNIDs of roaming partners.

5.4.3.2 Network Advertisement

Network advertisement information enumerates the roaming partners and associated NAI realms. This information shall be provided to the WLAN UE when the WLAN is unable to route an authentication request from the WLAN UE based on the initial NAI (e.g. when the WLAN AN receives a NAI with an unknown realm) and when the WLAN UE explicitly requests Network advertisement information. [The network advertisement information is returned from the first hop AAA functionality. The first hop AAA functionality may be located either in the WLAN AN or in the PLMN in case no AAA functionality is in the WLAN AN. The provisioning of this AAA functionality is an implementation issue and does not put new requirements on 3GPP AAA Proxy/Server.](#) Details on the usage and coding of Network advertisement information are included in 3GPP TS 24.234 [9].

End of First Changes

CHANGE REQUEST

⌘ **23.234 CR 100** ⌘ rev **1** ⌘ Current version: **6.2.0** ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Clarification of the procedure to disconnect the last tunnel		
Source:	⌘ Siemens		
Work item code:	⌘ WLAN	Date:	⌘ 17/11/2004
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:	⌘ Description of AAA server and HSS behaviour in case of disconnection of the last tunnel (chapter 7.10.3 in 23.234) is unclear.
Summary of change:	⌘ Clarify that the AAA server may notify the HSS about deletion of the UE's registration state. In this case the HSS de-registers the AAA server.
Consequences if not approved:	⌘ Unclear description for upcoming stage 3 work.

Clauses affected:	⌘ 7.10.3										
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;"> </td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;"> </td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;"> </td> <td style="text-align: center;">X</td> </tr> </table> Other core specifications ⌘ Test specifications ⌘ O&M Specifications ⌘	Y	N		X		X		X		
Y	N										
	X										
	X										
	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.

***** BEGIN OF MODIFIED SECTION *****

7.10.3 Disconnection of the last tunnel for a WLAN UE

If the PDG detects that the disconnected tunnel is the last tunnel between the PDG and the WLAN UE, then all the WLAN UE related authorization and profile information could be removed from the PDG during the tunnel disconnection process.

In case the 3GPP AAA server decides to disconnect the WLAN UE from the WLAN after ~~the~~ disconnection of the tunnel, a disconnection procedure will proceed as described in section 7.6 (steps 3-4).

After the WLAN UE was disconnected from the WLAN, ~~if the 3GPP AAA Server decides to remove the WLAN UE's information from the 3GPP AAA Server~~, the 3GPP AAA Server notifies the HSS using the Wx procedure "Purge" that the WLAN UE's registration in the 3GPP AAA Server has been ~~cancelled~~ deleted. In this case ~~The~~ the HSS ~~removes the state related to that~~ de-registers the 3GPP AAA Server (WLAN de-registration procedure), ~~e.g., the address of the serving 3GPP AAA Server for the identified subscriber.~~

7.11 The WLAN UE initiated WLAN AN Access disconnection

***** END OF MODIFIED SECTION *****

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.234 CR 095** ⌘ rev **2** ⌘ Current version: **6.2.0** ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Revision for Ww reference point definition		
Source:	⌘ Telecom Italia S.p.A.		
Work item code:	⌘ WLAN	Date:	⌘ 15/11/2004
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:	⌘ Presently the TS 23.234 defines functionalities over the Ww interface, such as for example the authentication. The specific functionalities defined by 3GPP do not impact Layer 1 and Layer 2 requirements for IEEE 802.11. Hence the CR proposes to improve the text in order to specify that Layer 1 and Layer 2 requirements for IEEE 802.11 are out of the scope of 3GPP, but requirements impacting authentication and network selection functionalities are within 3GPP scope.
Summary of change:	⌘ New sentence to the definition of the Ww has been added, in order to state that the functionalities of the reference point are not in the scope of 3GPP as far as layer L1/L2 IEEE 802.11 specifications are concerned. It is also stated that the transport of authentication on top of EAP and the transport of information related to network selection is within the scope of 3GPP. In fact authentication performed by EAP-SIM or EAP-AKA and procedure for PLMN selection has been defined on top of IEEE 802.1x.
Consequences if not approved:	⌘ Misunderstanding due to not coherent requirements .

Clauses affected:	⌘ 6.3.13						
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="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> Test 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="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> O&M Specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<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.

First Changes

6.3.13 Ww reference point

6.3.13.1 General Description

The reference point Ww connects the WLAN UE to the WLAN Access Network per IEEE 802.1x [19] specifications. The definition of IEEE Physical and Medium Access Control layers protocols (e.g. Layer 1 and Layer 2 defined by IEEE 802.11 standards) is out of the scope of 3GPP.

6.3.13.2 Functionality

The functionality of the reference point is based on per IEEE 802.1x specifications [19]; and it is intended to transport signalling messages including:

- parameters for authentication signalling between the 3GPP AAA Server and the WLAN UE;
- parameters for identification of the operator networks for roaming purposes (i.e. PLMN list).

~~Note: Ww is defined by IEEE 802 and provided here for information only. Any modification to the interface is strictly considered outside the scope of 3GPP.~~

End of the first Changes

CHANGE REQUEST

⌘ **23.234 CR 109** ⌘ rev **2** ⌘ Current version: **6.2.0** ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ 3GPP WLAN User profile Update		
Source:	⌘ Ericsson, HP, Telecom Italia, Samsung		
Work item code:	⌘ WLAN	Date:	⌘ 18/11/2004
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:	⌘ Local Access parameter indicates whether or not the user has Direct access to external IP networks by scenario 2. However, the name of the parameter is confusing, as it was discussed in the last SA2 meeting. In addition, some editorial updated are made to the text.
Summary of change:	⌘ Replace Local-Access parameter by WLAN-Direct-IP-Access_parameter .
Consequences if not approved:	⌘ Misunderstanding of the WLAN 3GPP IP Access functionality.

Clauses affected:	⌘ 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;">Y</td> <td style="padding: 2px;"></td> </tr> <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>	Y	N	Y			X		X	Other core specifications	⌘ 29.234
	Y	N									
	Y										
		X									
	X										
		Test specifications									
		O&M Specifications									
Other comments:	⌘ There is a similar CR 004 in CN4 (N4-041527).										

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.

**** First modified section ****

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 3GPP AAA server via Wx reference point. The profile shall contain the following data items: Detailed work on these parameters is expected in stage 3 work.

1. IMSI

~~User identification~~

2. MSISDN

~~User identification, for example used for charging purposes~~

3. Operator determined barring of 3GPP-WLAN interworking subscription

4. Operator determined barring of 3GPP WLAN [3GPP tunneling-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 [aAccounting sServer iIdentifier\(s\)](#)

The Subscribed Charging Characteristics will implicitly define the charging mode to be applied and, for every case, the ~~charging node~~ [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 [aAccounting sServer iIdentifier](#) defined in item 6 must be considered.

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

Indications 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.

~~oW-APN Subscribed remote IP address~~

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

8. [WLAN Direct IP access](#) ~~Local access~~ allowed

[Indication if the user is allowed to use WLAN Direct IP access](#). ~~Indicates the local services that the user is allowed to have direct access to from the WLAN Access Network, e.g. Internet, corporate Intranets. This is indicated in the form of a list of Local Service Identifiers~~

~~NOTE:—Local Service Identifiers are not passed outside the 3GPP system—access to services within the WLAN is restricted by means of access scope limitations applied on the Wa reference point.~~

~~NOTE:—In the roaming case, Local Service Identifiers must be agreed between Home and Visited operators. A Local Service Identifier for Internet access should be specified at Stage 3. A Local Service Identifier for each corporate network should be specified at Stage 3.~~

9. Roaming allowed

Indication~~es~~ if the user is allowed to use [a WLAN AN connected to an VPLMN](#).~~3GPP WLAN Interworking in an WLAN AN that have no direct connection to the home PLMN.~~

3GPP TSG-SA WG2 Meeting #43
 Seoul, Korea.15th - 19th November 2004.

Tdoc #s2-043879

CR-Form-v7.1	
CHANGE REQUEST	
# 23.234 CR 111 # rev 1 #	Current version: 6.2.0 #

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	# Redraw of diagrams in section 7		
Source:	# Huawei		
Work item code:	# WLAN	Date:	# 10/11/2004
Category:	# D	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:	# Make all the diagrams consistent in styles		
Summary of change:	# Re-draw all the diagrams in section 7		
Consequences if not approved:	# The daigrams are not consistent in styles and not easy to read, some editorial errors in the section 7 texts are cleaned up.		

Clauses affected:	# 7.1, 7.2, 7.3, 7.4, 7.5, 7.9, 7.10, 7.12										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;">Y</td> <td style="text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">X</td> </tr> </table> Other core specifications # Test specifications # O&M Specifications #	Y	N	#	X	#	X	#	X		
Y	N										
#	X										
#	X										
#	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.

**** Start of changes ****

7 Procedures

Editor's note: the following procedure is FFS:

- *Subscriber Registers.*

7.1 I-WLAN and VPLMN Selection Procedure

7.1.1 Initial network selection

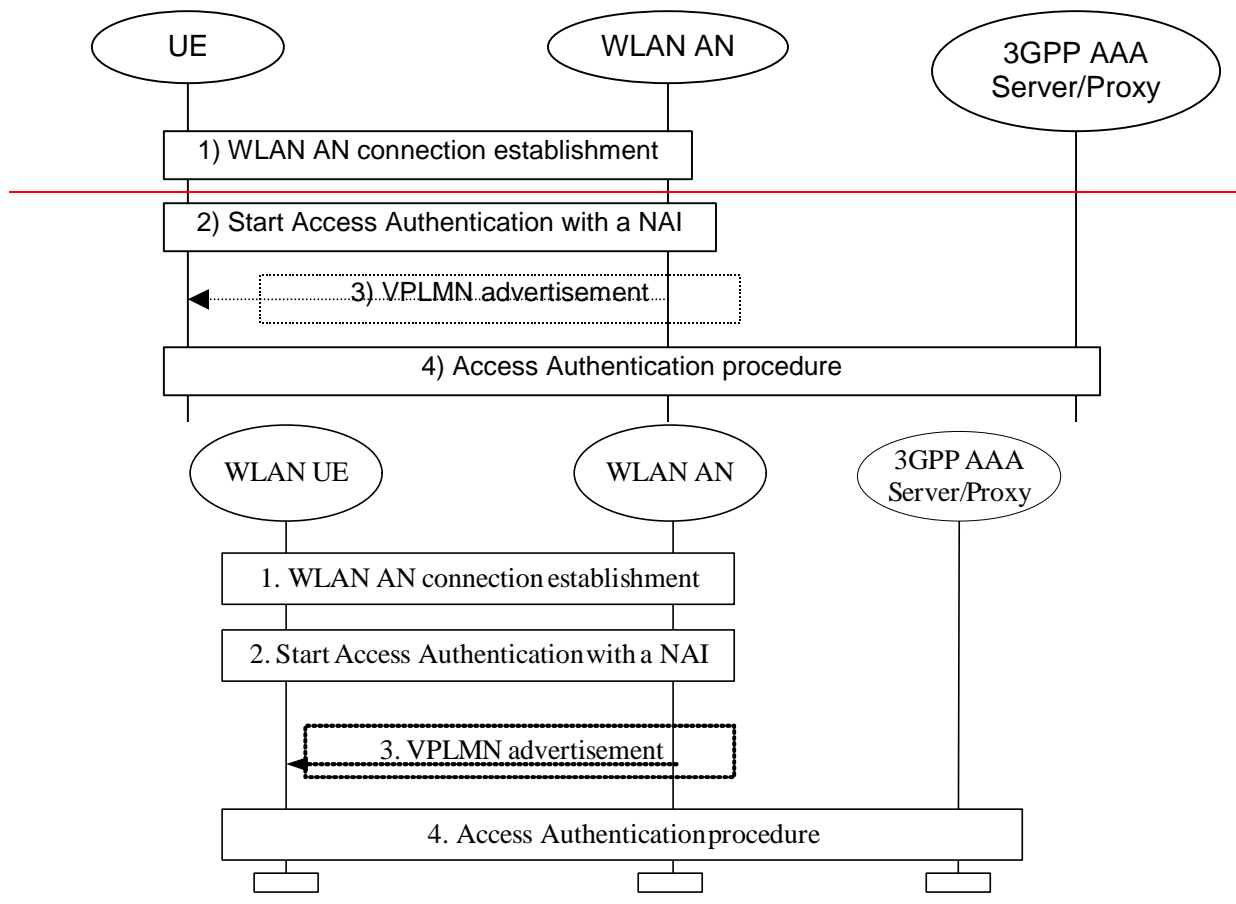


Figure 7.1: I-WLAN and VPLMN selection procedure

1. The WLAN UE selects a WLAN AN and establishes the WLAN connection with a WLAN technology specific procedure (e.g. in IEEE 802.11 it starts an association procedure). The details of the selection of the WLAN AN are specified in 3GPP TS 24.234 [9].
2. The Authentication procedure is initiated in a WLAN technology specific way and as a part of this process, the WLAN UE sends a NAI to the WLAN AN. The NAI shall be constructed as it is specified in 3GPP TS 23.003 [5].

3. If the WLAN AN is not able to route the authentication request (e.g. in the case where the WLAN AN receives an initial NAI with an unknown realm), the WLAN AN sends a response to the WLAN UE that provides information about the 3GPP networks to which the WLAN AN is able to route authentication requests.

From this point the WLAN UE may continue the access authentication with the selected WLAN AN using a different NAI (step 2) or may start access authentication with another available WLAN AN (step 1) or may stop. The details of the WLAN UE behaviour are specified in 3GPP TS 24.234 [9]. If the WLAN UE continues the access authentication with the selected WLAN AN, it shall select a VPLMN among the 3GPP networks indicated in the response received from the WLAN AN and build the new NAI as a roaming NAI indicating this VPLMN.

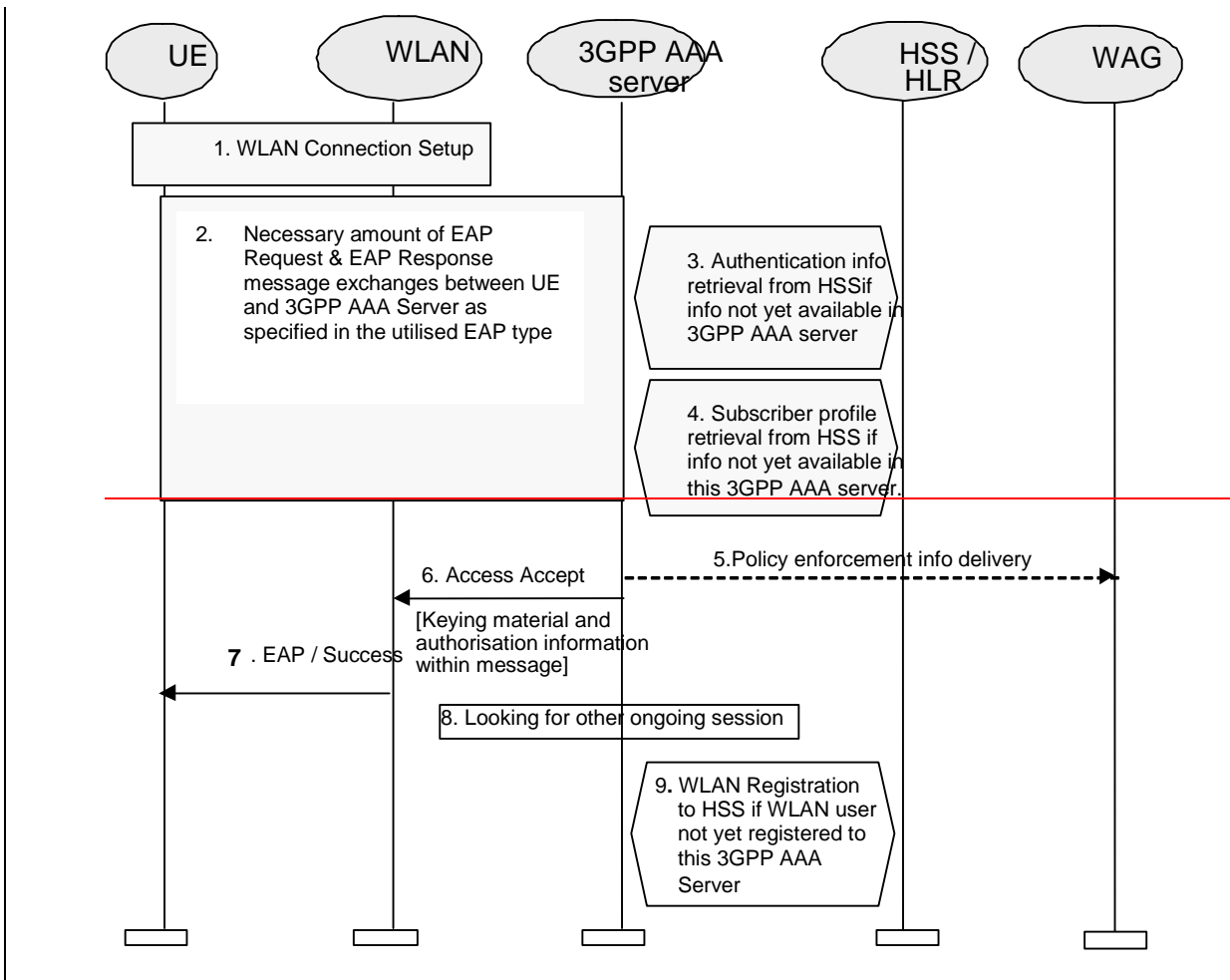
4. The WLAN AN routes the AAA message to the 3GPP AAA Server or 3GPP AAA Proxy based on the NAI and the access authentication is performed as it is specified in 3GPP TS24.234 [9].

7.1.2 Network re-selection

When the WLAN UE changes from the current serving PLMN to another PLMN with or without change of the WLAN AN, it needs to use a new NAI corresponding to the new PLMN in a new authentication initiated by the WLAN UE or the WLAN AN.

The 3GPP AAA Server may then receive a new authentication with PLMN selection different from the current active connection. For example, the WLAN UE lost radio in the first WLAN AN, then it changed to another WLAN AN with a different PLMN selection before the previous WLAN AN detected that the user is lost, or the WLAN UE started the new authentication before the disconnection of the previous connection. In this case, the 3GPP AAA Server shall initiate a disconnection to the currently active connection after the success of the new authentication and authorization process.

7.2 WLAN Access Authentication and Authorisation



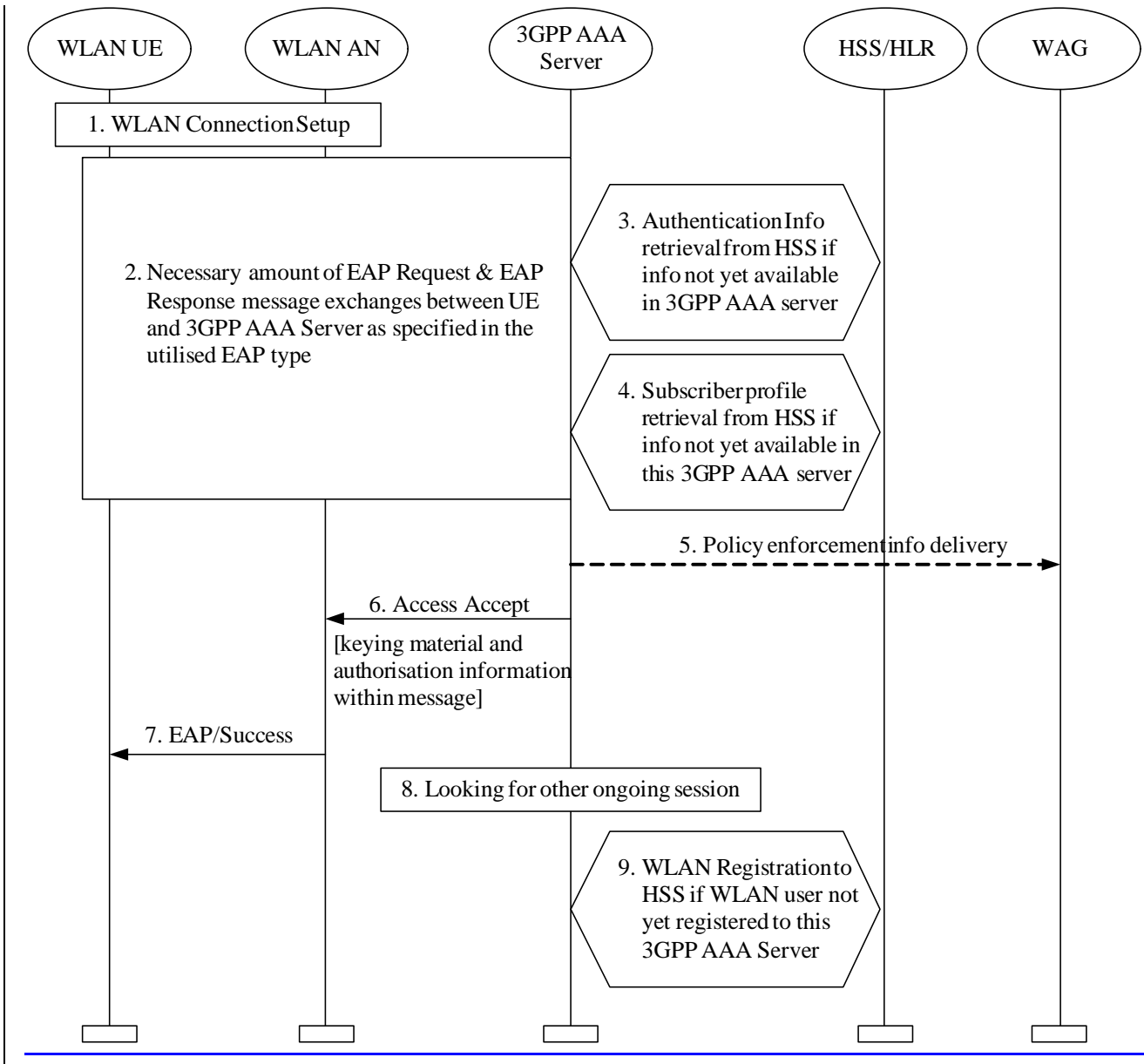


Figure 7.2: Authentication and authorisation procedure

1. WLAN connection is established with a WLAN technology specific procedure (out of scope for 3GPP).
2. The EAP authentication procedure is initiated in WLAN technology specific way.
 All EAP packets are transported over the WLAN interface encapsulated within a WLAN technology specific protocol.
 All EAP packets are transported over the Wa reference point.
 A number of EAP Request and EAP Response message exchanges is executed between 3GPP AAA Server and WLAN UE. The amount of round trips depends e.g. on the utilised EAP type. Information stored in and retrieved from HSS may be needed to execute certain EAP message exchanges.
- 3 Information to execute the authentication with the accessed user is retrieved from HSS. This information retrieval is needed only if necessary information to execute the EAP authentication is not already available in 3GPP AAA Server. To identify the user the *username* part of the provided NAI identity is utilised. During the information retrieval the HSS/HLR checks if there is a 3GPP AAA ~~server~~Server already registered to serve for the user. In case the HSS/HLR detects that another 3GPP AAA ~~server~~Server has already registered for this user, it shall provide the current 3GPP AAA ~~server~~Server with the previously registered 3GPP AAA ~~server~~Server address. The authentication signalling is then routed to the previously registered 3GPP AAA ~~server~~Server.

- 4 Subscribers WLAN related profile is retrieved from HSS. This profile includes e.g. the authorisation information and permanent identity of the user. Retrieval is needed only if subscriber profile information is not already available in 3GPP AAA Server.
5. Optionally, the 3GPP AAA ~~server~~Server (or the 3GPP AAA ~~proxy~~Proxy in roaming case) may send the policy enforcement information to the WAG in the PLMN that the WLAN UE selected in case VPLMN is to allocate the local IP Address for the WLAN UE.

Note: Additional process, such as allocating the IP address, may be necessary during or before this step to be performed.

- 6 If the EAP authentication and authorisation was successful, then 3GPP AAA Server sends Access Accept message to WLAN. In this message 3GPP AAA Server includes EAP Success message, keying material derived from the EAP authentication as well as connection authorisation information (e.g. NAS Filter Rule or Tunnelling attributes) to the WLAN.
WLAN stores the keying material and authorisation information to be used in communication with the authenticated WLAN UE.

NOTE: In the roaming case, authorisation information is passed from 3GPP AAA Server to 3GPP AAA Proxy in the form of Local service identifiers (see Section 6.5)

- 7 WLAN informs the WLAN UE about the successful authentication and authorisation with the EAP Success message.
- 8 The 3GPP AAA Server checks if there is a different previously established authentication session of the WLAN user, e.g., a session that uses a different WLAN UE or roaming in a different WLAN AN or in a different VPLMN. If yes then 3GPP AAA ~~server~~Server shall close the previously established session ("Session abort procedure" over Wa) to avoid multiple WLAN direct IP access sessions.
- 9 3GPP AAA ~~server~~Server registers the WLAN users 3GPP AAA ~~Server~~Server to the HSS. In registration messages the subscriber is identified by his permanent identity. This registration is needed only if the subscriber is not already registered to this 3GPP AAA ~~Server~~Server.

7.3 Subscriber Profile Update

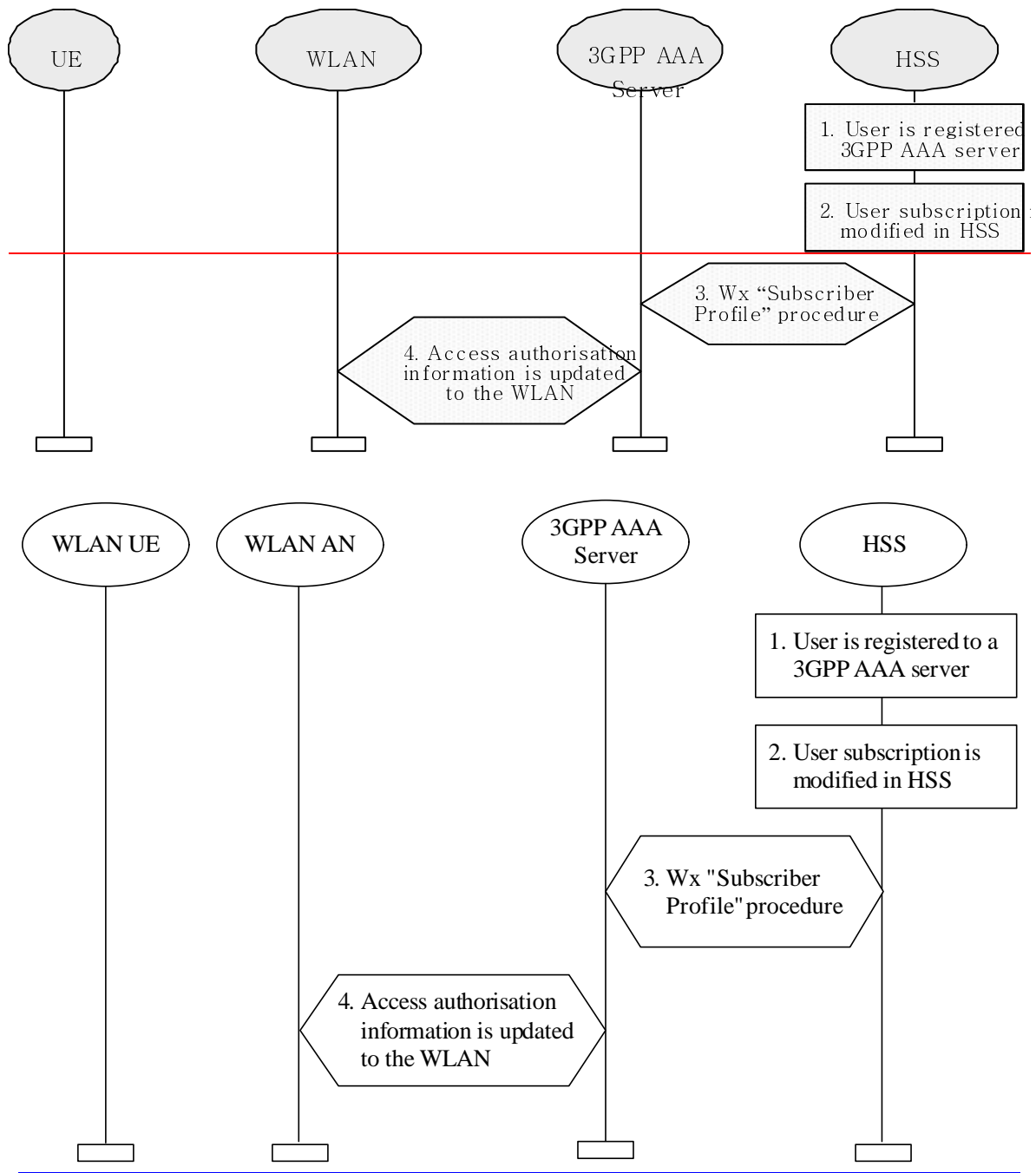


Figure 7.3: Subscriber Profile and access authorization info Update Procedure

1. User is registered to a 3GPP AAA ~~server~~Server
2. Subscribers subscription is modified in the HSS e.g. via O&M.
3. HSS updates the profile information stored in the registered 3GPP AAA ~~server~~Server by Wx reference point procedure "Subscriber Profile".
4. The WLAN access authorisation information of the associated connection is updated to WLAN as necessary.

7.3.1 Access and service Authorization information update procedure

This procedure is for WLAN 3GPP IP Access.

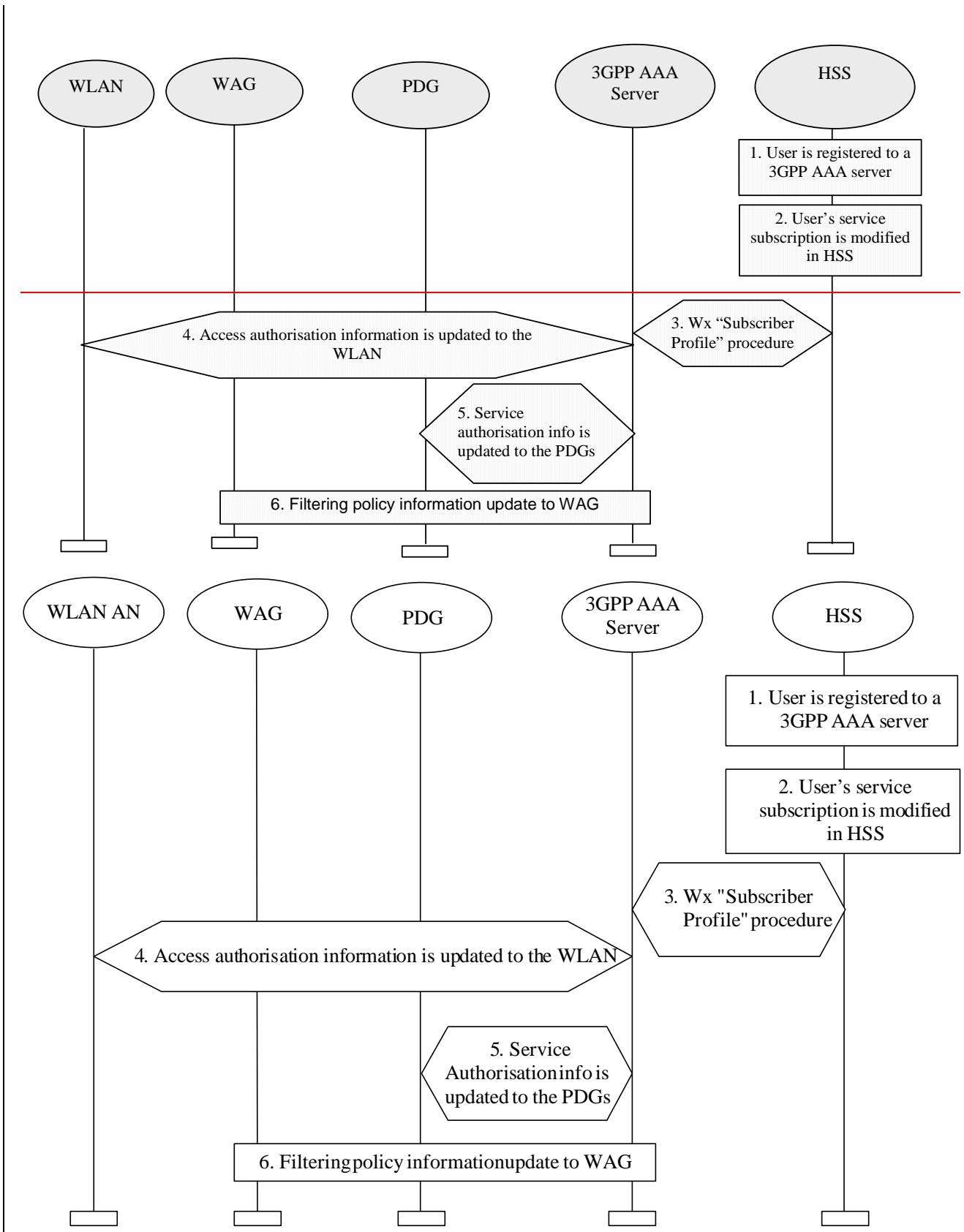


Figure 7.4: Authorization information Update Procedure

1. User is registered to a 3GPP AAA ~~server~~Server
2. User's service subscription is modified in the HSS e.g. via O&M,

3. HSS updates the profile information stored in the registered 3GPP AAA ~~server~~Server by Wx reference point procedure "Subscriber Profile".
4. The WLAN access authorisation information of the associated connection is updated to WLAN AN if necessary.
5. The service authorisation information of the activated services is updated to PDGs if necessary. A deactivation of service may be initiated if the subscriber lost the authorization of the activated service.
6. The filtering policy information of the activated services is updated to WAG if necessary.

Note: The de-registration may be initiated by the 3GPP AAA ~~server~~Server to the HSS as necessary, i.e., the 3GPP -AAA ~~server~~Server determines that the WLAN UE is unable to access any service upon the updated authorization.

7.4 Cancelling WLAN Registration

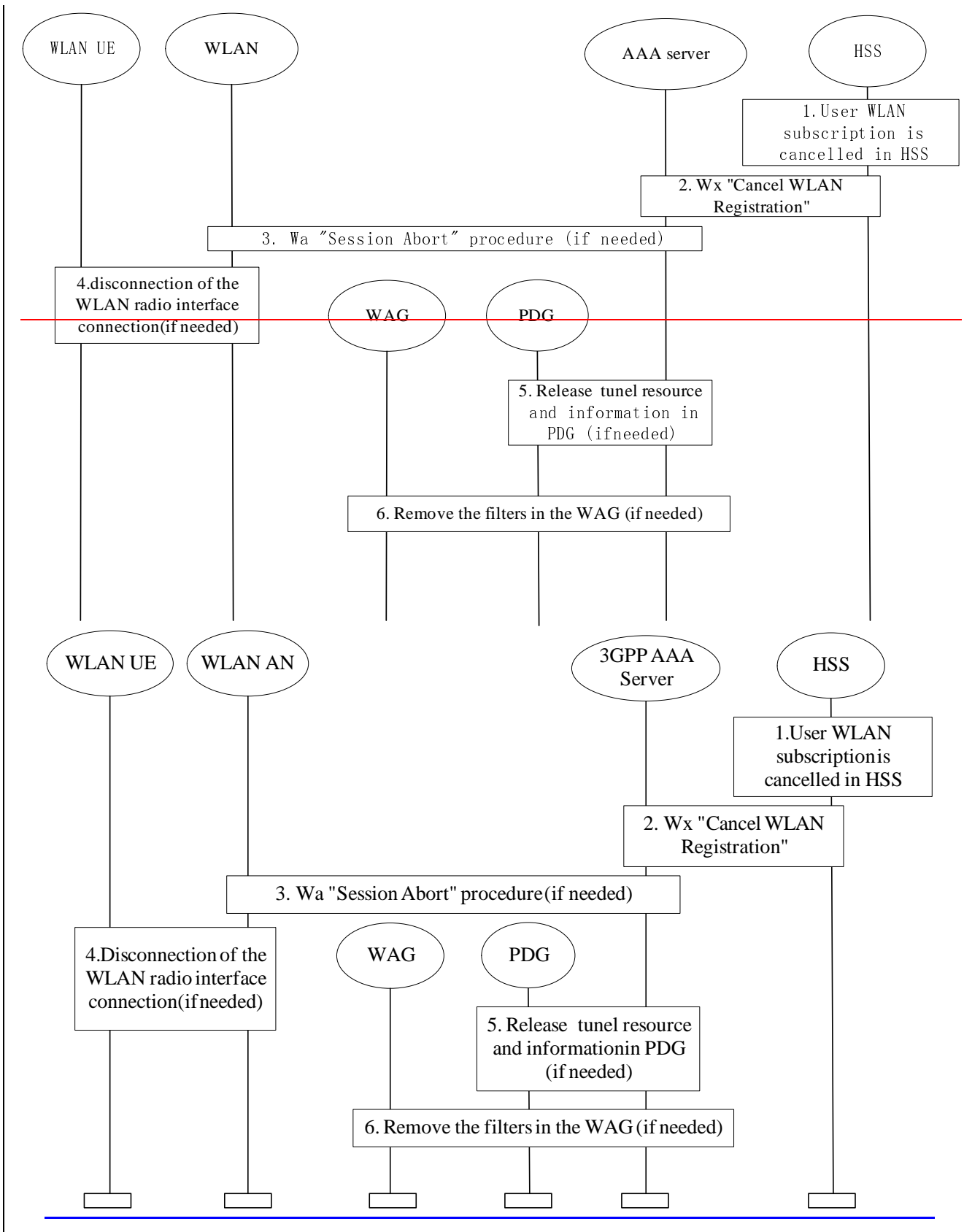


Figure 7.5: Cancellation of WLAN Registration Procedure

1. The 3GPP subscribers WLAN subscription is cancelled in HSS.

2. HSS cancels subscribers WLAN registration in the 3GPP AAA Server by Wx reference point procedure "Cancel WLAN Registration". In the messages subscriber is identified by his permanent identity.
3. If the subscriber's WLAN access connection still exists, Wa reference point procedure "Session Abort" procedure is executed towards WLAN.
4. If the radio connection still exists, WLAN disconnects the radio interface connection by WLAN technology specific mechanisms.
5. If the subscriber's tunnel connection with one or several PDG(s) exists, the 3GPP AAA ~~server~~Server/~~proxy~~Proxy informs the PDG(s) over the Wm reference point, to remove the tunnel related information and resource.
6. The filters, which were deployed to WAG for the tunnel(s) during the tunnel establishment, are removed.

7.5 Disconnecting a Subscriber by WLAN

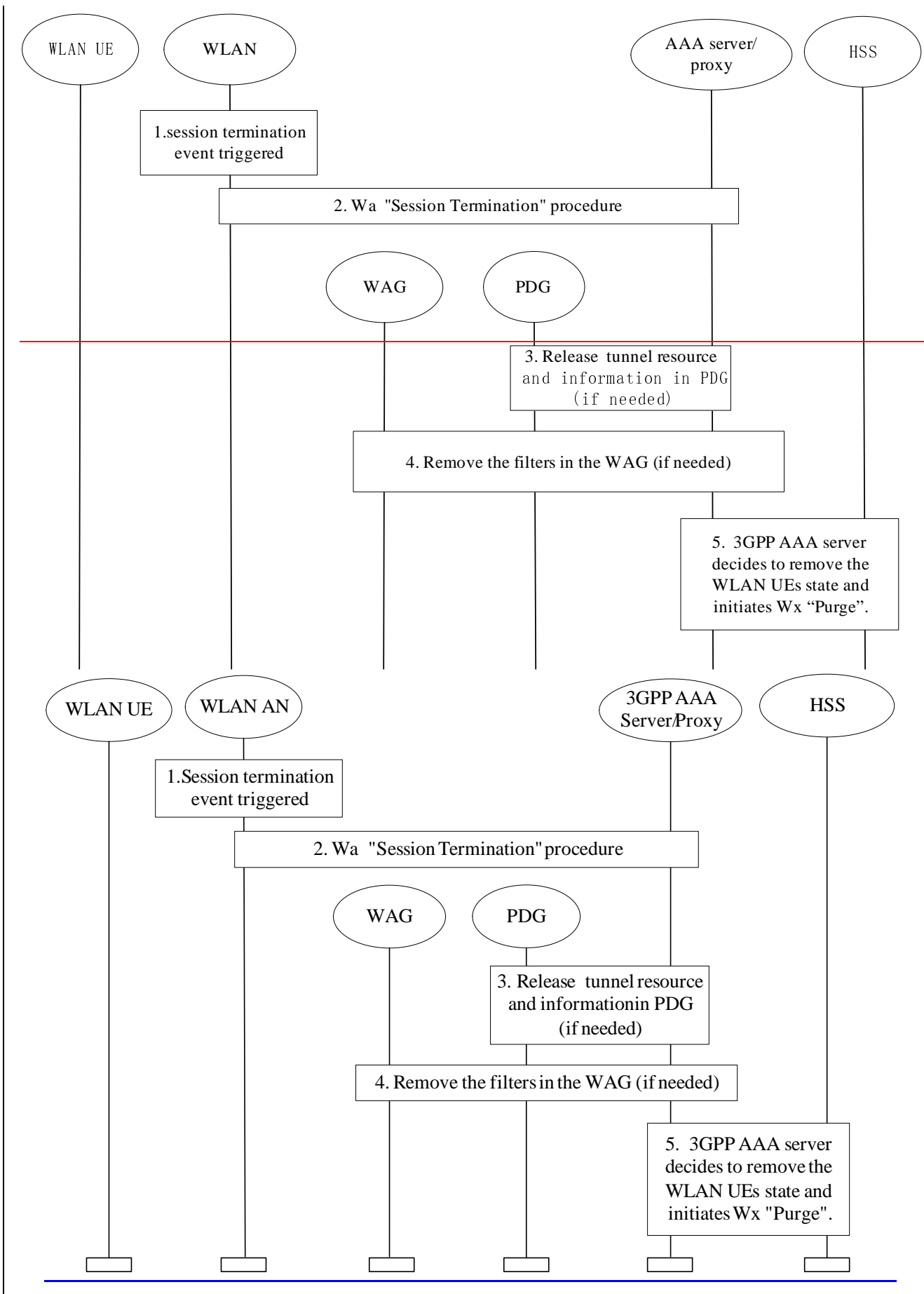


Figure 7.6: WLAN initiated disconnection procedure

1. WLAN detects that a Session related to a WLAN UE should be terminated towards the 3GPP AAA Server, e.g. when the WLAN UE has disappeared from WLAN coverage.
2. WLAN initiates Wa Session Termination procedure towards 3GPP AAA ~~server~~Server.
3. If the subscriber has a tunnel connection with one or more PDGs, and the 3GPP AAA ~~server~~Server/~~proxy~~Proxy needs to remove the connections, it informs the PDG(s) over the Wm reference point to remove the tunnel related information and resource.
4. The filters, which were deployed to WAG for the tunnel(s) during the tunnel establishment, are removed.
5. In case when the 3GPP AAA ~~server~~Server decides to remove the WLAN UEs state from the 3GPP AAA ~~server~~Server, the 3GPP AAA ~~server~~Server notifies HSS using Wx procedure "Purge" that the WLAN registration in the 3GPP AAA Server has been cancelled. HSS removes the state related to that 3GPP AAA ~~server~~Server, e.g., the address of the serving 3GPP AAA ~~server~~Server for the identified subscriber.

****** Next changes ******

7.9 W-APN resolution and Tunnel establishment

This information flow presents the generic message exchange necessary in order to resolve the selected W-APN and establish a WLAN UE-Initiated tunnel for WLAN 3GPP IP Access purposes.

As a prerequisite of these procedures it is necessary to perform the following:

1. WLAN Access Authentication and Authorisation and provisioning of the WLAN UE's local IP address

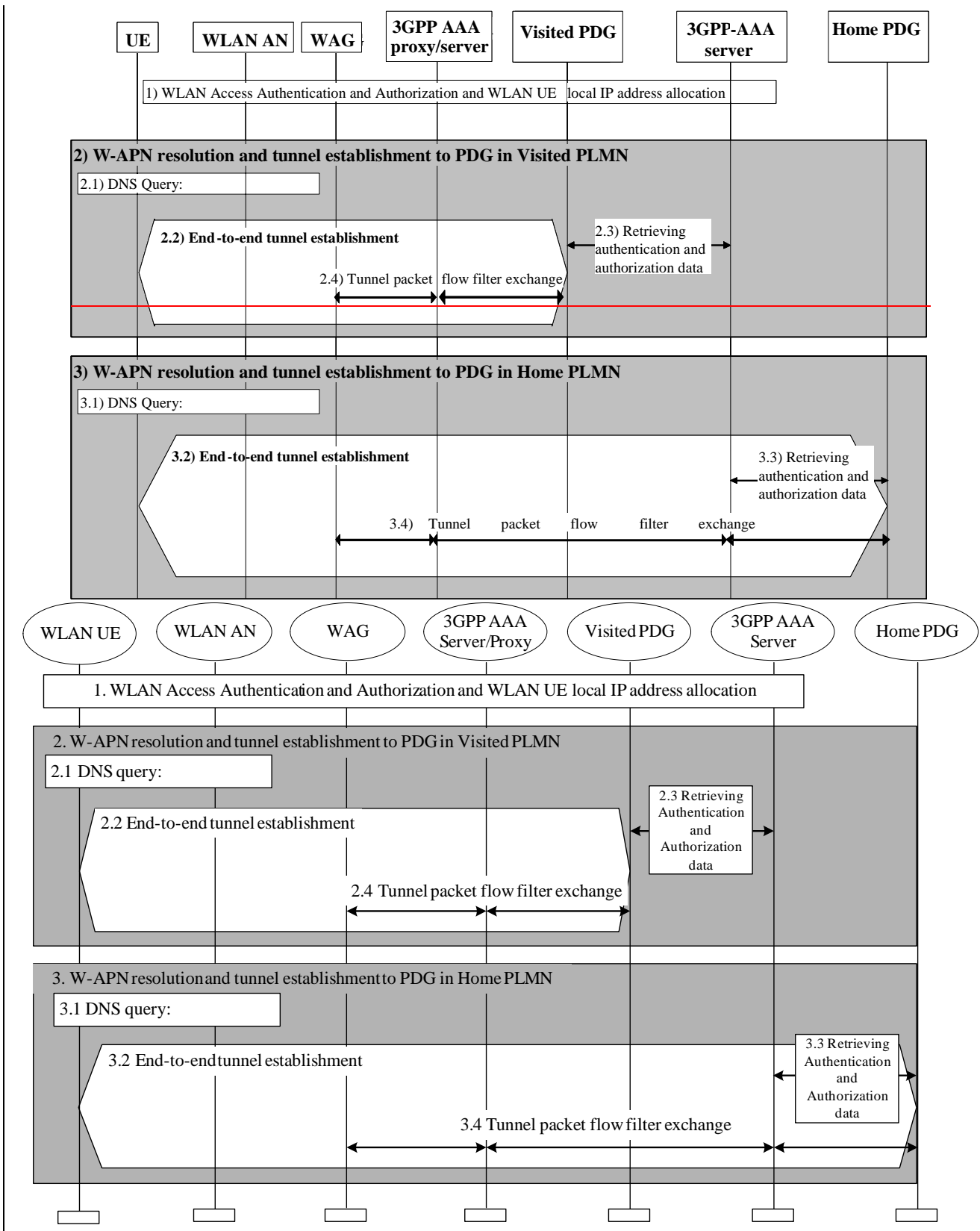


Figure 7.10: Example message flow to WLAN UE-Initiated tunnel establishment

When the user decides that he wants to access a service, the WLAN UE selects the W-APN network ID associated to the service requested by the user.

A detailed description of the W-APN resolution and the WLAN UE-Initiated Tunnel Establishment is given below.

2. Depending on internal configuration, the WLAN UE initiates W-APN resolution and tunnel establishment with a PDG in VPLMN.

Note: The configuration of the WLAN UE regarding W-APNs can be controlled by e.g. USIM Application Toolkit-based mechanisms.

- 2.1 WLAN UE constructs an FQDN using the W-APN Network Identifier and VPLMN ID as the Operator Identifier and performs a DNS query to resolve it. The DNS response will contain one or more IP addresses of equivalent PDGs that support the requested W-APN in the VPLMN according to standard DNS procedures.
If the VPLMN does not support the W-APN, then the DNS query returns a negative response. In this case, the WLAN UE continues with step 3.
- 2.2 The WLAN UE selects a PDG from the list received in step 2.1. If the DNS response contains IPv4 and IPv6 addresses, the WLAN UE has to select an address that has the same format as its own local IP address. If a PDG is finally selected, the establishment of an end-to-end tunnel is performed between the WLAN UE and this PDG. The WLAN UE shall include the W-APN and the user identity in the initial tunnel establishment request.
- 2.3 During the tunnel establishment, the PDG contacts the 3GPP AAA Server in the HPLMN via the 3GPP AAA proxy for authorization of the WLAN UE for the W-APN being requested by the WLAN UE and to retrieve the information required for the mutual authentication part of the tunnel establishment. As a result of successful mutual authentication the 3GPP AAA Server registers the WLAN UE at the HSS. This action may be omitted if the WLAN UE is already registered at this 3GPP AAA Server.
The 3GPP AAA Server shall be able to check that the user requesting the tunnel establishment has been already successfully WLAN Access Authorized. Based on operator policy it shall be possible to turn this check on and off. The check may be based on the user's subscription data, e.g. the user's subscribed services. If the check is not successful, the tunnel establishment request is rejected.
If the WLAN UE is not allowed to use a visited-PDG to access the given W-APN, the 3GPP AAA Server shall send a rejection message to the PDG and then the tunnel establishment shall be rejected by the PDG. The 3GPP AAA server shall provide PDG with the subscribed Charging Characteristics or W-APN Charging Characteristics. If it is not possible to establish the tunnel with any of the PDGs received from step 2.1, or the tunnel establishment failure reason is that the WLAN UE is not allowed to use a visited-PDG to access the given W-APN, then the WLAN UE continues with step 3.
- 2.4 During the tunnel establishment procedure, the PDG and the WAG exchange information via the 3GPP AAA Proxy in order to establish a filtering policy to allow the forwarding of tunnelled packets to the PDG. The 3GPP AAA Proxy requests the WAG to apply filtering policy based on information obtained from the PDG. The 3GPP AAA Proxy decides which filtering policy could be applied by the WAG according to local information (e.g. based on number of users, WAG capabilities, roaming agreement policy, etc).
3. Depending on internal configuration, or due to the failure of step 2.1 or 2.3, the WLAN UE initiates W-APN resolution and tunnel establishment with a PDG in HPLMN.
 - 3.1 WLAN UE constructs an FQDN using W-APN Network Identifier and the HPLMN ID as the Operator Identifier, and performs a DNS query to resolve it. The DNS response will contain one or more IP addresses of equivalent PDGs that support the requested W-APN in the HPLMN according to standard DNS procedures.
 - 3.2 The WLAN UE selects a PDG from the list received in step 3.1. If the DNS response contains IPv4 and IPv6 addresses, the WLAN UE has to select an address that has the same format as its own local IP address. If a PDG is finally selected, establishment of an end-to-end tunnel is performed between the WLAN UE and this PDGs. The WLAN UE shall include the W-APN and the user identity in the initial tunnel establishment request.
 - 3.3 During the tunnel establishment, the PDG contacts the 3GPP AAA Server in the HPLMN for authorization of the WLAN UE for the W-APN being requested by the WLAN UE and to retrieve the information required for the mutual authentication part of tunnel establishment. As a result of successful mutual authentication the 3GPP AAA Server registers the WLAN users at the HSS. This action may be omitted if the WLAN UE is already registered at this 3GPP AAA Server. The 3GPP AAA Server shall be able to check that the user requesting the tunnel establishment has been already WLAN Access Authorized. Based on operator policy it shall be possible to turn this check on and off. The check may be based on the user's subscription data, e.g. the user's subscribed services. If the check is not successful, the tunnel establishment request is rejected. If the WLAN UE is not allowed to use a Home PDG to access the given W-APN according to his

subscription, the 3GPP AAA Server shall send a rejection message to the PDG and then the tunnel establishment shall be rejected by the Home PDG. The 3GPP AAA Server shall 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~~Server shall provide PDG with the subscribed Charging Characteristics or W-APN Charging Characteristics.

3.4 During the tunnel establishment, the PDG and the WAG exchange information via the 3GPP AAA Server and 3GPP AAA Proxy in order to establish a filtering policy to allow the forwarding of tunnelled packets to the PDG. The 3GPP AAA ~~server~~Server requests to the WAG to apply filtering policy based on information obtained from the PDG. The 3GPP AAA ~~server~~Server decides which filtering policy could be applied by the WAG according to local information (e.g. based on number of user, WAG capabilities, roaming agreement policy, etc). The applied filtering policy is communicated to the Home-PDG.

7.9.1 Redirection

In the above procedures, the WLAN UE may not be authorised to access the requested W-APN through the selected PDG. This may occur for the following reasons:

- (i) The requested W-APN is not supported by the network
- (ii) The user is not subscribed to the requested W-APN
- (iii) The PDG is in the VPLMN and the user's subscription indicates that VPLMN access is not allowed for the requested W-APN
- (iv) The operator does not wish to include all PDG addresses in DNS and so (for example) all initial requests are handled by a default PDG which may not be the correct PDG for the requested W-APN
- (v) The user has not supplied an explicit requested W-APN. This is treated as a request for the first appropriate subscribed W-APN, or for a network default W-APN (if a wildcard W-APN is included in the subscription), as per 23.060 Annex A.

In cases (i), (ii) and (iii), the request is simply rejected. In case (iii), the WLAN UE may attempt tunnel establishment to the HPLMN as described in Section 7.8.

In cases (iv) and (v) above, the 3GPP AAA Server may determine that the user is authorised to access the W-APN through a different PDG. The 3GPP AAA Server then sends the IP address of the alternative PDG (i.e the authorized PDG) to the requested PDG. The IP address of the alternative PDG is then returned to the WLAN UE in the rejection message from PDG to WLAN UE. In this case the WLAN UE shall attempt a new tunnel establishment request to the provided PDG address.

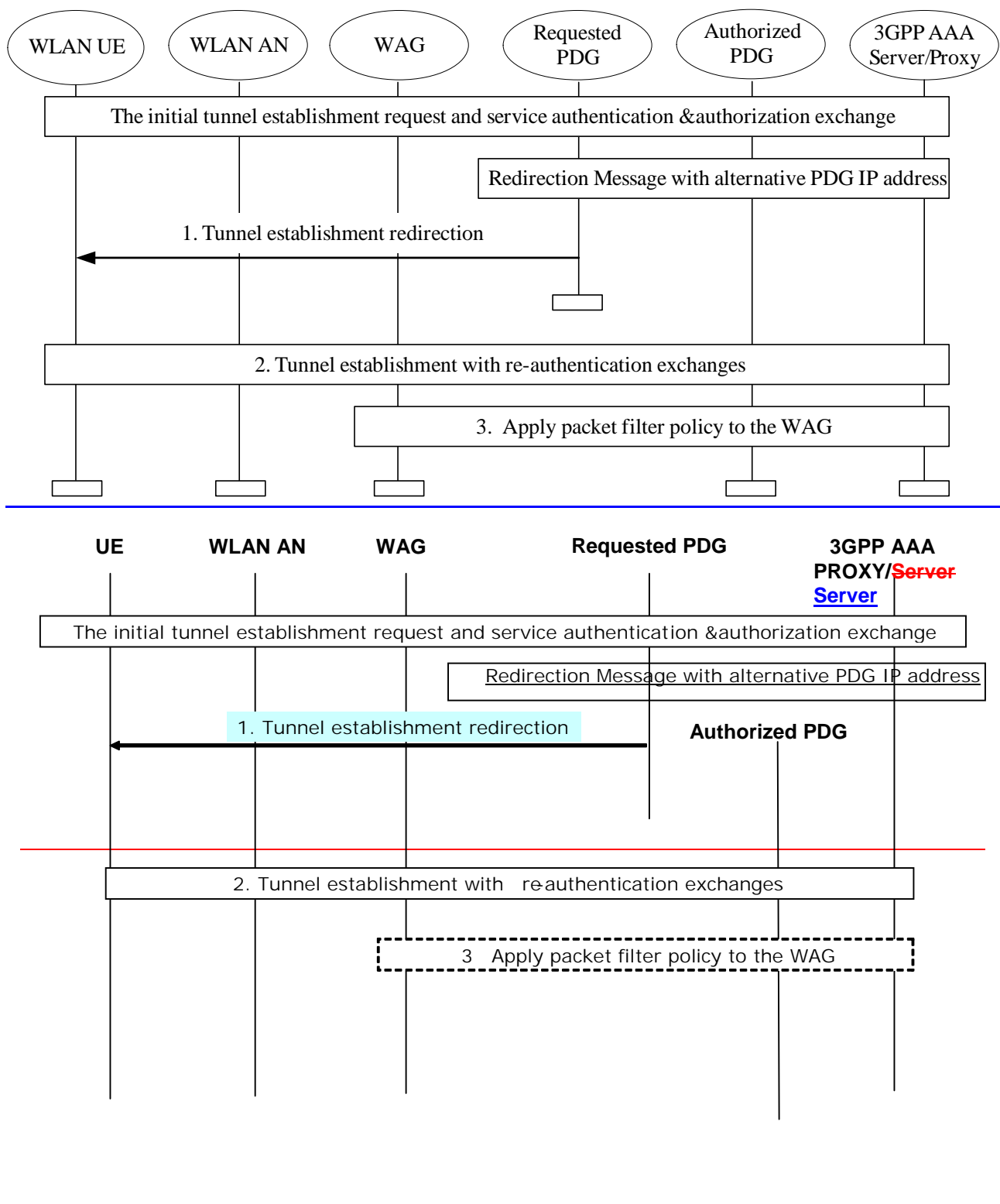


Figure 7.11: Message flow of the tunnel establishment with redirection

During the step 2.3/3.3 in the procedure of clause 7.9, the 3GPP AAA Server authorizes the service to the WLAN UE, and sends the authorization information to the requested PDG. If requested PDG is not authorized to provide the service then the 3GPP AAA ~~server~~Server sends a new PDG (Authorized PDG) address and the authorized W-APN, then the following steps performed:

1. The requested PDG sends tunnel redirection request to the UE with service authorization information (authorized PDG address and authorized W-APN).

2. The WLAN UE sends an end-to-end tunnel establishment request to the Authorized PDG. Then end-to-end tunnel establishment begins between the Authorized PDG and the WLAN UE. A full or fast re-authentication method should be used during this tunnel establishment.
3. The Authorized PDG provides filtering information to the WAG as it is specified in clause 7.9.

7.9.2 Subsequent authentication

In the case that the user attempts a subsequent tunnel establishment to a different PDG, it should be possible to avoid repeating the full authentication process and to perform fast re-authentication. Fast re-authentication is an optional feature and its activation is performed in the home operator's network.

7.9.3 Use of DNS

It shall be possible to restrict the propagation of DNS information used for the above mechanism to DNS servers controlled by the PLMNs and to DNS servers available only to authorised 3GPP WLAN UEs (i.e. those WLAN UEs which have successfully connected to a 3GPP Interworking WLAN.)

It shall be possible to configure multiple PDG addresses against a single FQDN in a manner which allows the load to be shared across these PDGs.

It shall be possible to configure IPv4 and IPv6 addresses against a single FQDN and to return these addresses together to the WLAN UE.

Note: The above shall be achieved by standard DNS mechanisms. The usage of TLD and the DNS query performed by the WLAN UE to resolve the W-APN are left to stage 3. Further details are in [5].

7.9.4 Subsequent tunnel establishment

The subsequent tunnel establishment should follow the same procedure as in the first tunnel establishment.

7.10 Tunnel disconnection procedures

Tunnel disconnection can be either:

- Initiated from the WLAN UE, as a result of an explicit deactivation/de-registration from the service.
- Initiated from the PDG, e.g. due to timeout of the tunnel connection or request from the [3GPP AAA server](#) or other network entities.

Tunnel disconnection is specified for the following situations:

- Normal service termination resulting from an end user requesting termination of the end-to-end tunnel connection using tunnel control signalling or deletion of the IP bearers associated with a service,
- Service termination resulting from network operator intervention,
- Loss of radio connections which are used to transport the tunnel signalling.

The tunnel disconnection message exchanges between the WLAN UE and the PDG are performed basing on the specific tunnel control signalling protocol. The WLAN UE and the PDG release the control information associated with the tunnel during the exchange, and the PDG should send a tunnel release report to the [3GPP AAA server](#) to update the corresponding subscriber's service connection information and status in the [3GPP AAA server](#), e.g. the service/tunnel connection activation info, the allocated IP address, etc. The filtering policy information applied on the WAG should also be removed, if necessary.

7.10.1 WLAN UE initiated tunnel disconnection

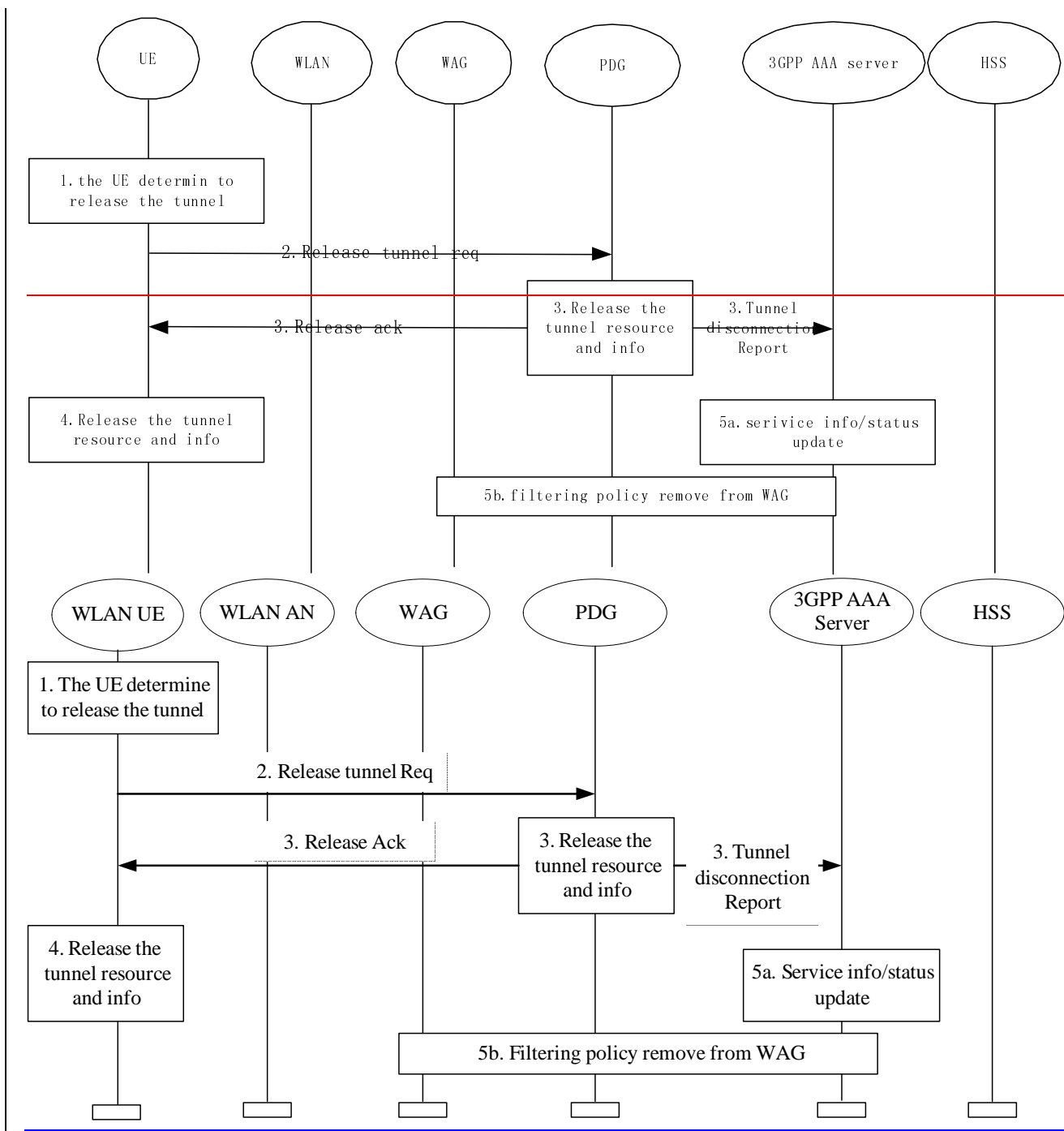


Figure 7.12: WLAN UE initiated tunnel disconnection

1. The WLAN UE determine to release the tunnel, e.g. due to the normal service termination operation.
2. The WLAN UE send a Release tunnel request to the PDG.
3. Upon receiving the Release tunnel request, the PDG sends a Release acknowledgement to the WLAN UE, releases the resources and the associated control information of the tunnel, and sends a Tunnel disconnection report to the 3GPP AAA server.
4. Upon receiving the Release acknowledgement, the WLAN UE releases the resources and the control information of the tunnel.

5. Upon receiving the Tunnel disconnection report, the 3GPP AAA ~~server~~Server updates the related service information and/or status of the subscriber; and removes the filtering policy related to the disconnected tunnel from WAG if necessary.

7.10.2 The network initiated tunnel disconnection

1. The PDG determines to release the tunnel, e.g. due to timeout of the tunnel connection or a request from the 3GPP AAA ~~server~~Server, or due to a network initiated normal service termination or a service termination resulting from network operator intervention.
2. The PDG sends a Release tunnel request to the WLAN UE.
3. Upon receiving the Release tunnel request, the WLAN UE releases the resources and the associated control information of the tunnel, and sends the Release acknowledgement to the PDG.
4. Upon receiving the release acknowledgement, the PDG releases the resources, the associated control information of the tunnel, and the related service authorization information; and sends a Tunnel disconnection report to the 3GPP AAA ~~server~~Server.
5. Upon receiving the Tunnel disconnection report, the 3GPP AAA ~~server~~Server updates the related service information and/or status of the subscriber; and removes the filtering policy related to the disconnected tunnel from WAG if necessary.

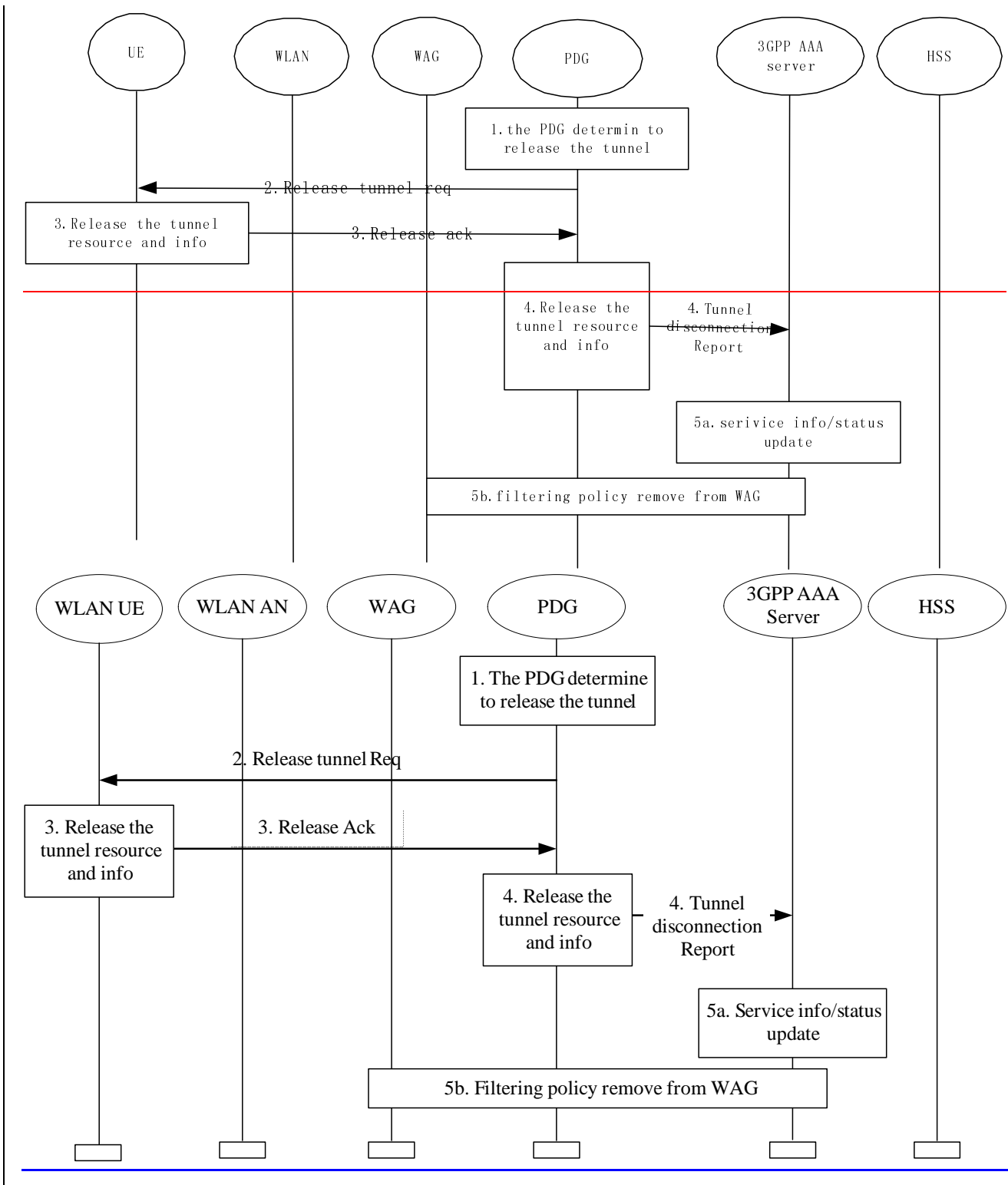


Figure 7.13: The network initiated tunnel disconnection

7.10.3 Disconnection of the last tunnel for a WLAN UE

If the PDG detects that the disconnected tunnel is the last tunnel between the PDG and the WLAN UE, then all the WLAN UE related authorization and profile information could be removed from the PDG during the tunnel disconnection process.

In case the 3GPP AAA server decides to disconnect the WLAN UE after the disconnection of the tunnel, a disconnection procedure will proceed as described in section 7.6 (step 3-4),

After the WLAN UE disconnected, if the 3GPP AAA Server decides to remove the WLAN UE's information from the 3GPP AAA Server, the 3GPP AAA Server notifies HSS using Wx procedure "Purge" that the WLAN registration in the 3GPP AAA Server has been cancelled. The HSS removes the state related to that 3GPP AAA Server, e.g., the address of the serving 3GPP AAA Server for the identified subscriber.

****** Next changes ******

7.12 User identity to HSS resolution

7.12.1 General

This section describes the resolution mechanism, which enables the 3GPP AAA Server 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. This resolution mechanism is not required in networks that utilise a single HSS. An example for a single HSS solution is a server farm architecture. The NAI will be used as user identifier towards the SLF.

The subscription locator is accessed via the Dw reference point. The Dw reference point is the standard interface between the 3GPP AAA Server and the SLF. The synchronisation between the SLF and the different HSSs is an O&M issue.

The subscription locator is already defined in 3GPP TS 23.228 [24] for Cx and Sh interfaces.

The Dw interface provides:

- an operation to query the subscription locator from 3GPP AAA Server
- a response to provide the HSS name towards 3GPP AAA Server.

By sending the Dw-operation DW_SLF_QUERY the 3GPP AAA Server indicates a user identity of which it is looking for an HSS. By the Dw-operation DW_SLF_RESP, the SLF responds with the HSS address. The 3GPP AAA Server may optionally store the HSS address for a given subscriber so subsequent queries to the SLF are not needed.

Subclause 7.12.2 presents an example of the session flow when the 3GPP AAA Server needs to query the SLF.

7.12.2 SLF query

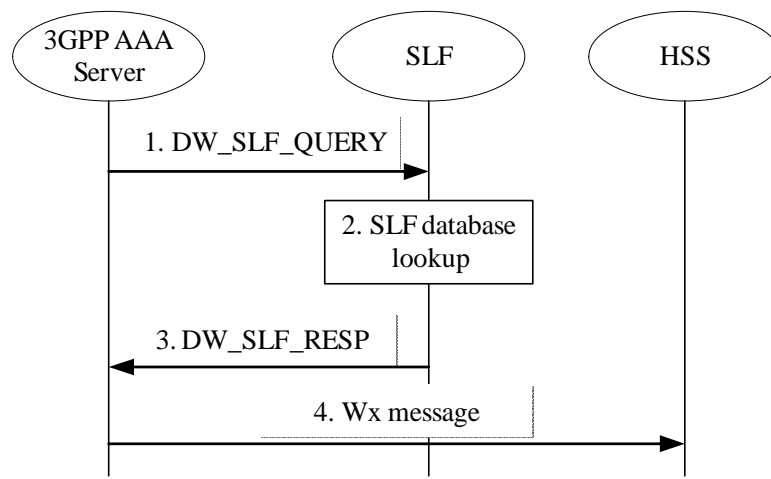
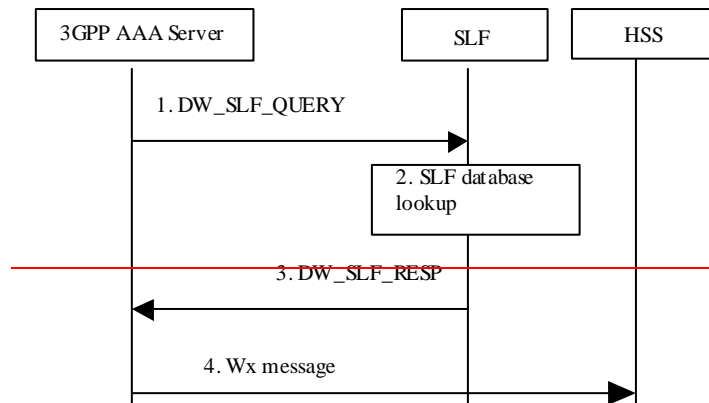


Figure 7.14: Query through SLF

1. 3GPP AAA Server detects that it requires the user profile, the registration or new authentication vectors for a given 3GPP subscriber, so has to query for the location of the user’s subscription data. The 3GPP AAA Server sends a DW_SLF_QUERY to the SLF and includes as parameter the user identity of the subscriber.
2. The SLF looks up its database for the queried user identity.
3. The SLF answers with the HSS address in which the user’s subscription data can be found.
4. The 3GPP AAA Server can proceed by querying the appropriate HSS by Wx protocol.

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

CR-Form-v7.1

CHANGE REQUEST

№ **23.234 CR 113** № rev **1** № Current version: **6.2.0** №

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the № symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	№ Correction on Annex E		
Source:	№ Samsung		
Work item code:	№ WLAN	Date:	№ 19/11/2004
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:	№ Wrong explanation about Wn and Wp reference point in Annex E.
Summary of change:	№ Correct the explanation of Wn and Wp reference point in Annex E.
Consequences if not approved:	№ The Figure E.1.1 and the Figure E.2.1 does not match with the section E.5 and E.6

Clauses affected:	№ E.5, E.6										
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.

******* FIRST MODIFIED SECTION *******

E.5 Wn Reference Point

Reference point Wn is located ~~between the WAG and the PDG in the HPLMN. 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 Wn serves a similar purpose as the connecting network entities of the Gn interface in GPRS; the GTP protocol would be considered as a candidate for the Wn reference point.~~ 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 ~~in the VPLMN~~ and the PDG ~~in the HPLMN~~. 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. This reference point caters for the roaming WLAN traffic by transporting tunnelled WLAN user data between WAG in the VPLMN and the PDG in the HPLMN. 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 112** ⌘ rev **2** ⌘ Current version: **6.2.0** ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Editorial corrections		
Source:	⌘ Samsung		
Work item code:	⌘ WLAN	Date:	⌘ 19/11/2004
Category:	⌘ D	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:	⌘ Correction and addition of references
Summary of change:	⌘ Correct out-dated references in the text and add appropriate ones
Consequences if not approved:	⌘ Wrong and/or insufficient references can reduce readability

Clauses affected:	⌘ 5.2, 5.3.1, 5.5, A.5.1, Annex G						
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="text-align: center; padding: 2px;"><input type="checkbox"/></td> <td style="text-align: center; padding: 2px;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<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"/>	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/](http://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.

***** FIRST MODIFIED SECTION *****

5.2 Access Control Principles

End to End Authentication: WLAN Authentication signaling is executed between WLAN UE and 3GPP AAA Server for the purpose of authenticating the end-user and authorizing the access to the WLAN and 3GPP network.

Transporting Authentication signalling over WLAN Radio Interface: WLAN authentication signalling is carried between WLAN UE and WLAN AN by WLAN Access Technology specific protocols. To ensure multivendor interoperability these WLAN technology specific protocols shall conform to existing standards of the specific WLAN access technology.

Transporting Authentication signalling between WLAN AN and 3GPP network: WLAN Authentication signalling shall be transported **between any WLAN AN and 3GPP network** by a standard protocol, which is independent of the specific WLAN technology utilised within the WLAN Access network.

Details of end to end authentication and transport of authentication signalling over the WLAN radio interface and between the 3GPP network and WLAN is covered in 3GPP TS 33.234 [~~10~~14]

WLAN Access Authorization: This defines the process(es) in 3GPP AAA Server verifying whether WLAN Access should be allowed to a subscriber and deciding what access rules/policy should be applied to a subscriber. It is the stage after access authentication, but before service authorisation and WLAN UE's local IP address allocation.

***** NEXT MODIFIED SECTION *****

5.3.1 General

The network authentication procedure is based on the use of EAP method where user identification is based on Network Access Identifier (NAI), whose format is specified in RFC 2486 [~~12~~17]. A NAI is composed of a username part and a realm part. In the following, the term of 'identity' includes both the NAI username part and the realm part, while the term of 'username' only refers to the NAI username part.

***** NEXT MODIFIED SECTION *****

5.5 Authentication methods

Authentication methods are discussed in TS 33.234 [614].

***** NEXT MODIFIED SECTION *****

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:

....

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.

******* NEXT MODIFIED SECTION *******

Annex G (informative): Consideration on supporting IMS over I-WLAN

In GPRS, interaction between bearer service (i.e. GPRS) and IMS is done by a service-based local policy (SBLP) for bearer QoS authorization, gating and charging correlation.

The followings are a brief analysis of possible methods to provide interactions between I-WLAN and IMS.

1. Applying SBLP with full functionality including QoS authorization

- Pros: It provides full solution for IMS over I-WLAN as the same level as GPRS.
- Cons: It requires a big amount of new work including E2E QoS and enhancement of SBLP.
- It is not standardized in this version of the TS.

2. Applying SBLP partially, e.g. without QoS authorization

- Pros: It provides necessary functions of SBLP for IMS over I-WLAN. Note that current assumption is there is no mechanism of QoS provisioning for I-WLAN in this release.
- Cons: It also requires modification of SBLP.
- It is not standardized in this version of the TS.

3. Applying IP-Flow Based Charging (FBC) instead of SBLP

- Pros: As stated in TS 23.125[15] Annex D, FBC can provide policing functions, which can be used for IMS over I-WLAN. When QoS is not in the picture, FBC can provide enough functionalities required for IMS over I-WLAN such as gating and charging related features.
- Cons: In the current version of TS 23.234, FBC is stated of optional feature of a PDG (not mandatory one). It also requires additional functionality and interface in PDG.
- It is an optional feature in this version of the TS.

******* END OF CHANGES *******

CHANGE REQUEST

⌘ **23.234 CR 086** ⌘ rev **6** ⌘ Current version: **6.2.0** ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Correction of online charging disconnect procedure.		
Source:	⌘ Ericsson, Huawei, Nokia		
Work item code:	⌘ WLAN	Date:	⌘ 5/11/2004
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: 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) Rel-7 (Release 7)

Reason for change:	⌘ The sequence diagram to disconnect a user that is online charged is not inline with a reply LS sent from SA2#41 (S2-042830) to CN4. The reply indicates that the HSS is only informed when the last tunnel is teared down. However, the sequence diagram indicates that the HSS is always updated. Hence, there is a need to clarify that this diagram only applies to when the 'last tunnel' is disconnected. Also, added is a sequence diagram for the case when the tunnels of an online charged user are disconnected due to the lack of credits.
Summary of change:	⌘ It is clarified that a message is only sent to the HSS when the last tunnel is disconnected, and added a sequence diagram for tunnel disconnect.
Consequences if not approved:	⌘ Incorrect sequence diagram, and missing tunnel disconnect.

Clauses affected:	⌘ 7.6, 7.10.3										
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> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><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 Test specifications O&M Specifications	⌘
Y	N										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
Other comments:	⌘										

How to create CRs using this form:

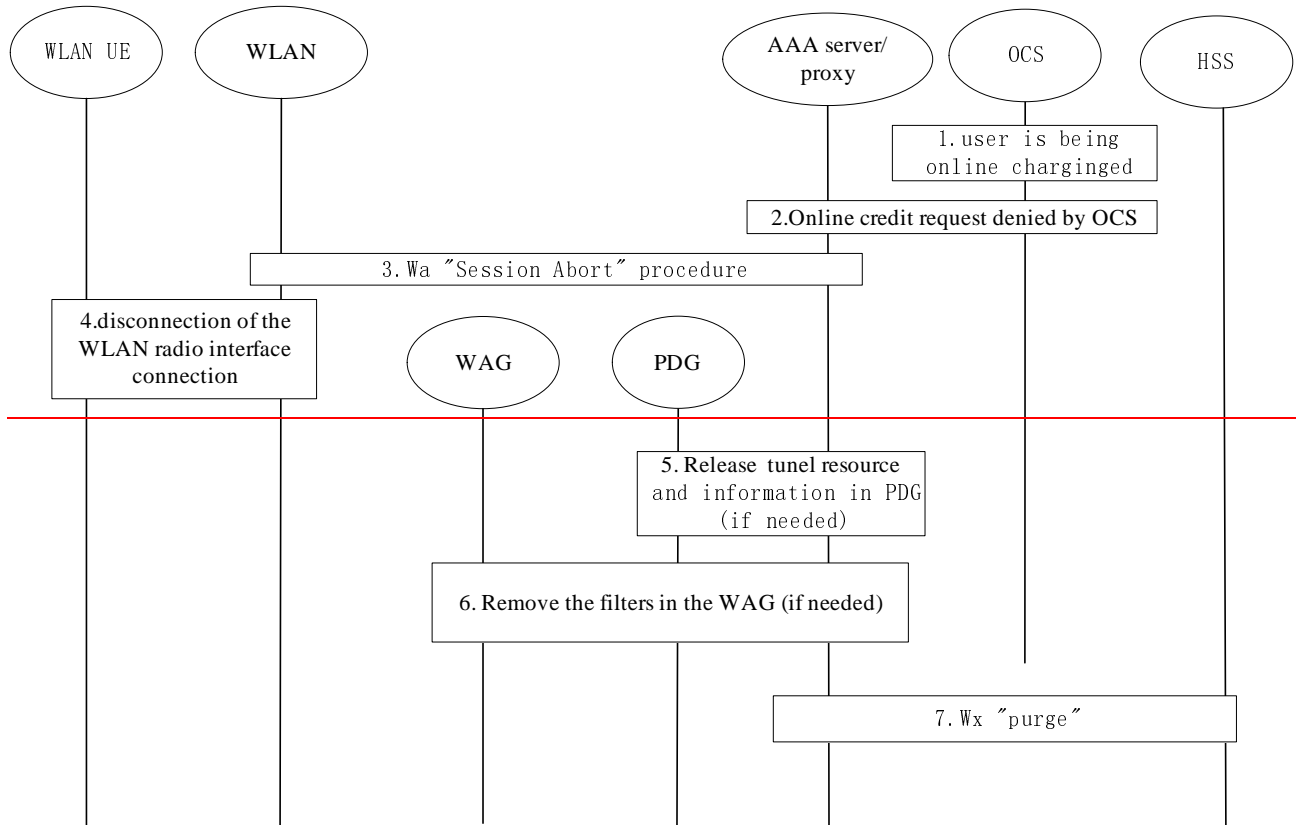
Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 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.

**** Start of 1 set of changes ****

7.6 Disconnecting a Subscriber by Online Charging System

7.6.1 The OCS initiated WLAN AN access disconnection



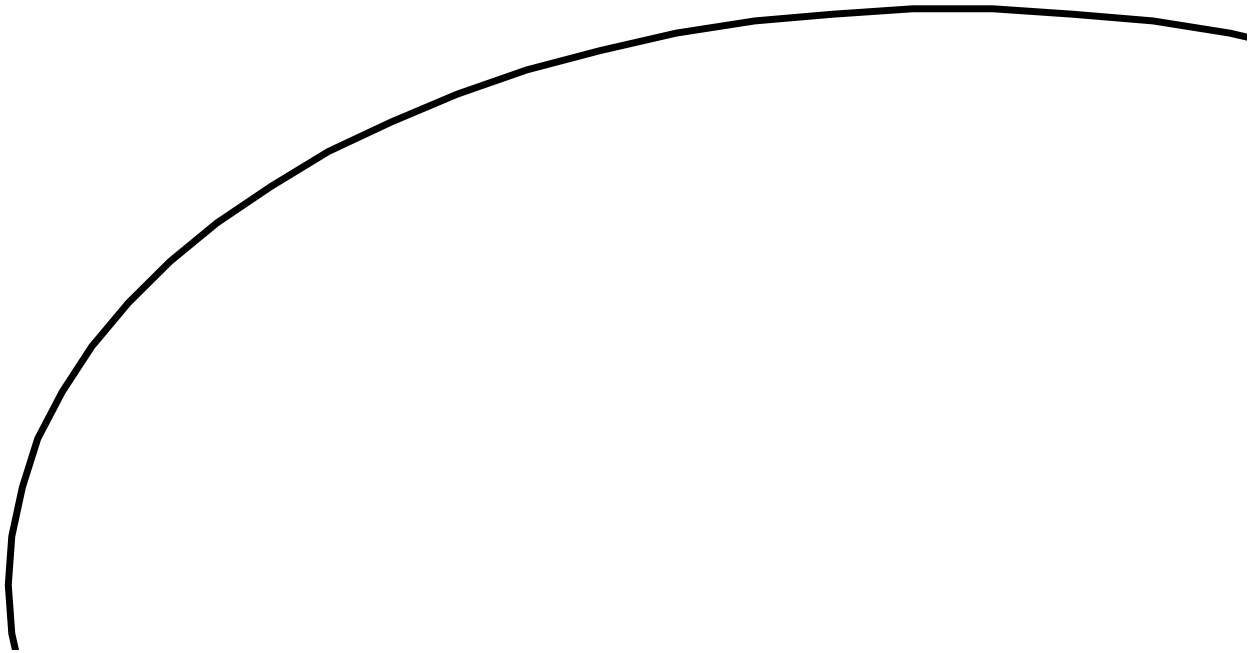


Figure 7.7: The OCS initiated WLAN AN access Disconnection Procedure

This section applies to the case when an online charged user runs out of credit and is totally disconnected from WLAN.

1. A subscriber is ~~being~~ online charged by 3GPP AAA ~~server~~ Server for WLAN access.
2. The OCS (online-Online Charging System) denies credit request from the 3GPP AAA ~~server~~ Server for WLAN access. The possibly already retrieved online credit runs out.
3. To disconnect the subscriber's connection, Wa reference point procedure "Session Abort" procedure is executed towards the WLAN AN.
4. The WLAN AN disconnects the radio interface connection by WLAN technology specific mechanisms.
5. If the subscriber's tunnel connection with one or several PDG(s) exists, the 3GPP AAA ~~server/proxy~~ Server/Proxy informs the PDG(s) over the Wm reference point, to remove the tunnel related information and resource.
6. ~~The If filters, which~~ were deployed to WAG for the tunnel(s) during the tunnel establishment, then they are removed.
7. If no Wx "Purge" procedure was already initiated in step 3, then the 3GPP AAA ~~server~~ Server notifies HSS that WLAN registration in the 3GPP AAA ~~server~~ Server has been cancelled, by means of Wx procedure "Purge"

7.6.2 The OCS initiated tunnel disconnection

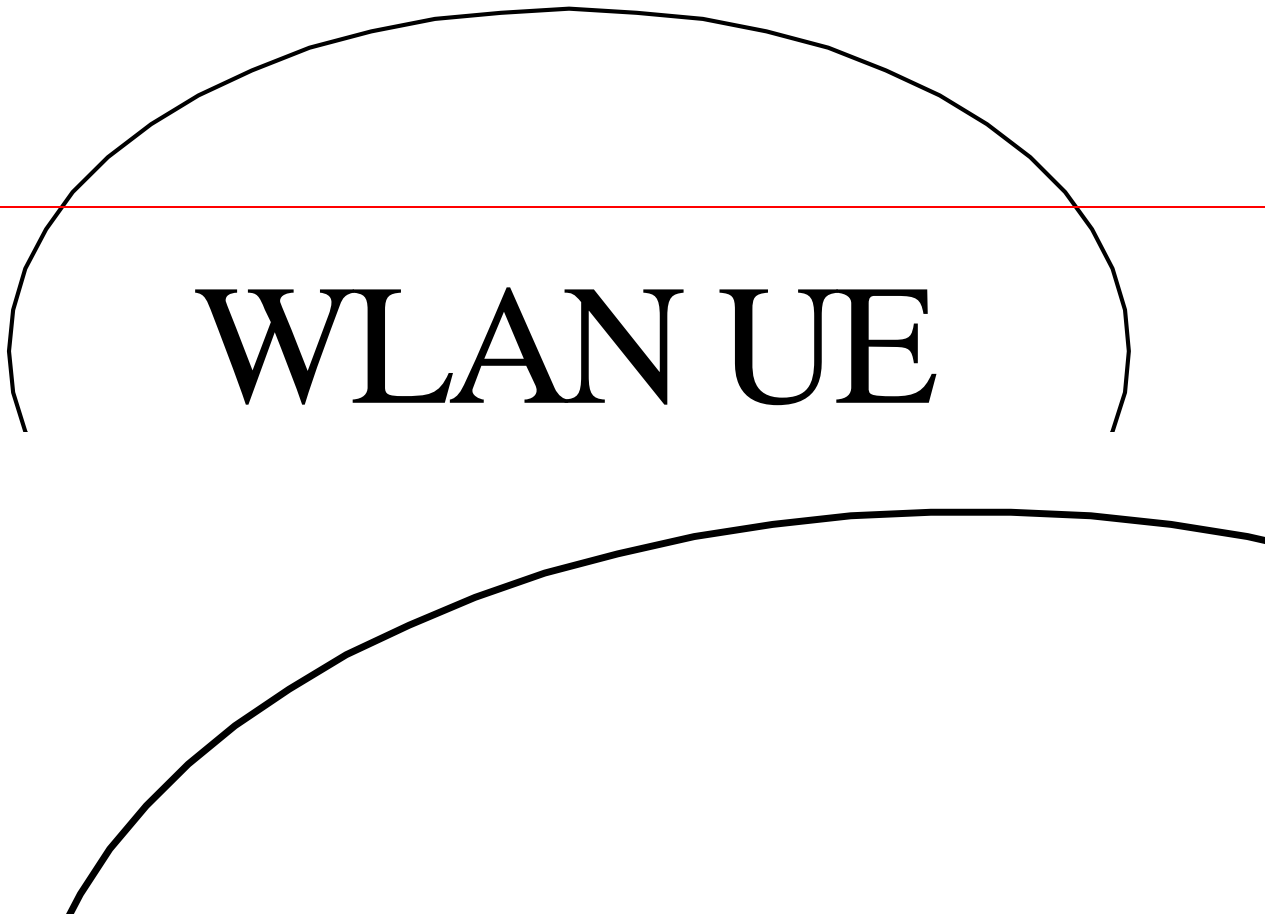


Figure 7.8: The OCS initiated tunnel disconnection procedure

This section applies to the case when the tunnels of an online charged user are disconnected due to the lack of credits.

1. The Online Charging System (OCS) denies the credit request from the PDG. The possibly already retrieved online credit runs out.
2. The PDG disconnects the tunnels that require new credits using the network initiated tunnel disconnection procedure (clause 7.10.2). The tunnels that do not require new credits (e.g., the tunnels using free of charge W-APNs) will not be disconnected.
3. If all tunnels of the subscriber have been disconnected in the previous step then the 3GPP AAA Server may decide to totally disconnect the subscriber by performing "Session Abort" towards the WLAN AN (i.e. step 3 and 4 of clause 7.6.1).
4. If the subscriber is disconnected from the WLAN AN in step 3 and no Wx "Purge" procedure was already initiated, then the 3GPP AAA Server notifies HSS that WLAN registration in the 3GPP AAA Server has been cancelled, by means of Wx procedure "Purge".

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

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

7.10.3 Disconnection of the last tunnel for a WLAN UE

If the PDG detects that the disconnected tunnel is the last tunnel between the PDG and the WLAN UE, then all the WLAN UE related authorization and profile information could be removed from the PDG during the tunnel disconnection process.

In case the 3GPP AAA server decides to disconnect the WLAN UE after the disconnection of the tunnel, a disconnection procedure will proceed as described in section 7.6.1 (step 3-4),

After the WLAN UE disconnected, if the 3GPP AAA Server decides to remove the WLAN UE's information from the 3GPP AAA Server, the 3GPP AAA Server notifies HSS using Wx procedure "Purge" that the WLAN registration in the 3GPP AAA Server has been cancelled. The HSS removes the state related to that 3GPP AAA Server, e.g., the address of the serving 3GPP AAA Server for the identified subscriber.

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

3GPP TSG SA SA2 Meeting #42
 Seoul, Korea, 15-19 Nov 2004

S2-043883

CR-Form-v7	
CHANGE REQUEST	
⌘ 23.234 CR 105 ⌘ rev 3 ⌘	Current version: 6.2.0 ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Rewording Readability Changes Section 3
Source:	⌘ HP, Samsung
Work item code:	⌘ WLAN
	Date: ⌘ 11/15/2004
Category:	⌘ F
	<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p><i>Use <u>one</u> of the following categories:</i></p> <p>F (correction)</p> <p>A (corresponds to a correction in an earlier release)</p> <p>B (addition of feature),</p> <p>C (functional modification of feature)</p> <p>D (editorial modification)</p> <p>Detailed explanations of the above categories can be found in 3GPP TR 21.900.</p> </div> <div style="width: 45%;"> <p><i>Use <u>one</u> of the following releases:</i></p> <p>2 (GSM Phase 2)</p> <p>R96 (Release 1996)</p> <p>R97 (Release 1997)</p> <p>R98 (Release 1998)</p> <p>R99 (Release 1999)</p> <p>Rel-4 (Release 4)</p> <p>Rel-5 (Release 5)</p> <p>Rel-6 (Release 6)</p> </div> </div>

Reason for change:	⌘ Several sections of TS 23.234 are hard to understand, are outdated because conclusions were reached by the group, or can be greatly clarified by the use of examples or more text. The goal it to allow the TS to be easily readable by those not in the drafting group.
Summary of change:	⌘ Edit text for clarity, allowing additional text for explanation and example. Reorganize paragraphs if required.
Consequences if not approved:	⌘ Difficulty in reading and using the specification. Changes at this time allow review by several of the orginal members of the WLAN Drafting group, which will not be possible in the future as they move to new assignments.

Clauses affected:	⌘ Section 3									
Other specs Affected:	<table border="1" style="font-size: x-small;"> <tr> <td style="width: 20px;">Y</td> <td style="width: 20px;">N</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;"> </td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;"> </td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;"> </td> </tr> </table>	Y	N	X		X		X		⌘ Other core specifications ⌘ ⌘ Test specifications ⌘ ⌘ O&M Specifications ⌘
	Y	N								
	X									
	X									
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.

**** Start of changes ****

3 Definitions, symbols and abbreviations

3.1 Definitions

Available SSID: ~~It is a~~ An SSID that the WLAN UE has found after active and/or passive scanning which meets certain conditions as specified in IEEE 802.11 [19].

3GPP - WLAN Interworking: Used generically to refer to interworking between the 3GPP system and the WLAN family of standards. Annex B includes examples of WLAN Radio Network Technologies.

~~**Environment:** The type of area to be covered by the WLAN network of a 3GPP WLAN interworking; e.g. public, corporate and residential.~~

External IP Network/External Packet Data Network: An IP or Packet Data network ~~to which with~~ access ~~may be~~ provided ~~through by~~ the 3GPP ~~WLAN Interworking~~ system, rather than directly from the WLAN AN. ~~For example, the Internet, an operator's IP network or a 3rd party IP network such as a corporate IP network.~~

Home WLAN: ~~A~~ The WLAN which ~~that is~~ interworking ~~ing~~ with the HPLMN without using a VPLMN. ~~of the 3GPP WLAN interworking user.~~

Interworking WLAN (I-WLAN): A WLAN that interworks with a 3GPP system.

I-WLAN selection: Procedure to for select a specific I-WLAN from ~~the selection among~~ the available I-WLANs ~~APs~~

Local Service Identifier: An identifier ~~used~~ within the 3GPP system ~~for a service available directly from the I-WLAN, for example Internet access or access to a specific corporate network.~~

Offline charging: ~~Offline charging m~~ Mechanism ~~is provided~~ for collecting and forwarding charging information ~~about occurred concerning I-WLAN access resource and core network resource usage, etc~~ without affecting the service ~~rendered~~ in real-time.

Online charging: ~~Online charging m~~ Mechanism ~~is provided for collecting and forwarding charging information concerning I-WLAN and core network resource usage~~ where the service ~~may be rendered is~~ affected in real-time ~~and is required for a direct interaction with session/service control. This allows an online charged subscriber to access WLAN.~~

Policy Enforcement: Functionality ~~Policy Enforcement is~~ implemented in a WAG to insure p Packets coming from or going to the WLAN AN are allowed ~~policed~~ based on unencrypted data within the packets. (e.g., source and destination IP address and port number)

PS based services: ~~In WLAN interworking, PS based service is a g~~ General term to refer to the services provided by a PLMN using the IP bearer capability between a WLAN UEs and the PLMN when WLAN 3GPP IP Access is used. Examples include bearer services such as ~~They include all services provided by 3G PS domain that use the IP bearer service, (e.g., IMS, Internet access, and Corporate IP network access), and higher level other services such as IMS, (e.g., SMS and LCS).~~

Requested W-APN: The W-APN requested by the WLAN UE user.

Routing Enforcement: Routing Enforcement ensures ~~that all~~ packets sent to/from the WLAN UE for 3G PS based service are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case). Routing Enforcement is implemented between a WLAN AN and a WAG.

Selected W-APN: ~~The~~ W-APN selected by the network as a result of the ~~WLAN UE user~~ subscriber request

Service Authorization: Authorization allowing a subscriber for a user to access the requested service based on ~~according to the user's~~ subscription.

~~**Supported PLMN:** A PLMN of a roaming partner (i.e. to which the WLAN operator has a direct roaming relationship).~~

Tunnel Identifier: Identifier of an ~~an end-to-end~~ tunnel between a WLAN UE and a PDG. It is contained in the unencrypted part of ~~a~~ the packet.~~s~~

User Identifier: Identifier of a user which may be used, for example, in e-g-charging functionality

~~Visited WLAN: An interworking WLAN that Interworks only with a visited PLMN.~~

W-APN: WLAN Access Point Name. ~~It is used to identify~~ ~~identifies~~ a specific IP network and a point of interconnection to that network (Packet Data Gateway).

WLAN 3GPP IP Access: Access to an IP network via a PLMN via a tunnel. A related term is WLAN 3GPP Direct IP Access~~the 3GPP system.~~

WLAN coverage: ~~an~~ The area where a WLAN UE can connect to a WLAN, ~~wireless local area network access services are provided for interworking by an entity in accordance with WLAN standards.~~

WLAN Direct IP Access: Access to an IP network ~~is directly~~ ~~from~~ a ~~the~~ WLAN AN without passing data to a PLMN via a tunnel. A related term is WLAN 3GPP IP Access.

~~WLAN roaming: The ability for a 3GPP WLAN interworking user (subscriber) to function in a serving WLAN different from the home WLAN~~

WLAN UE's local IP address: ~~The~~ An address ~~that is necessary used~~ to deliver ~~a~~ the packet to a WLAN-UE in a WLAN AN. It identifies the WLAN UE in the WLAN AN. ~~The~~ WLAN UE's local IP address may be translated by a Network Address Translation prior to being received by ~~the interworking function~~, any other IP network, including a PLMN.

WLAN UE's remote IP address: ~~The~~ An address used ~~by~~ in the data packet encapsulated ~~inside~~ by the WLAN UE to PDG-initiated tunnel. It represents the address-identity of the WLAN UE in the network which the WLAN UE is accessing via the PDG, ~~the WLAN UE is accessing.~~

3.2 Symbols

For the purposes of the present document the following symbols apply:

D'	Reference point between a pre-R6 HSS/HLR and a 3GPP AAA Server
Dw	Reference point between a 3GPP AAA Server and an SLF
Gr'	Reference point between a pre-R6 HSS/HLR and a 3GPP AAA Server
Wa	Reference point between a WLAN Access Network and a 3GPP AAA Server/Proxy (charging and control signalling)
Wd	Reference point between a 3GPP AAA Proxy and a 3GPP AAA Server (charging and control signalling)
Wf	Reference point between a CGw/CCF and a 3GPP AAA Server/Proxy
Wg	Reference point between a 3GPP AAA Server/Proxy and WAG
Wi	Reference point between a Packet Data Gateway and an external IP Network
Wm	Reference point between a Packet Data Gateway and a 3GPP AAA Server or 3GPP AAA proxy
Wn	Reference point between a WLAN Access Network and a WLAN Access Gateway
Wp	Reference point between a WLAN Access Gateway and a Packet Data Gateway
Wo	Reference point between a 3GPP AAA Server and an OCS
Wu	Reference point between a WLAN UE and a Packet Data Gateway
Wx	Reference point between an HSS and a 3GPP AAA Server

3.3 Abbreviations

AAA	Authentication, Authorisation and Accounting
ACL	Access Control List
AKA	Authentication and Key Agreement
AP	Access Point
APN	Access Point Name
CCF	Charging Collection Function
CGw	Charging Gateway
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol

FQDN	Fully Qualified Domain Name
GGSN	Gateway GPRS Support Node
GTP	GPRS Tunnelling Protocol
HLR	Home Location Register
HPLMN	Home PLMN
HSS	Home Subscriber Server
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IP-SM-GW	IP Short Message Gateway
ISP	Internet Service Provider
I-WLAN	Interworking WLAN
NAI	Network Access Identifier
NAT	Network Address Translation
OCS	Online Charging System
PDA	Personal Digital Assistant
PDG	Packet Data Gateway
PLMN	Public Land Mobile Network
SIM	Subscriber Identity Module
SSID	Service Set ID
VLAN	Virtual Local Area Network
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
USIM	UMTS SIM
SSID	Service Set Identifier
VPLMN	Visited PLMN
WAG	WLAN Access Gateway
W-APN	WLAN APN
WLAN	Wireless Local Area Network
WLAN AN	WLAN Access Network
WLAN UE	WLAN User Equipment

**** End of changes ****

3GPP TSG SA SA2 Meeting #42
 Seoul, Korea, 15-19 Nov 2004

S2-043884

CR-Form-v7	
CHANGE REQUEST	
⌘ 23.234 CR 103 ⌘ rev 3 ⌘	Current version: 6.2.0 ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Consistant Wording, Spacing, and Grammar Readability Changes		
Source:	⌘ HP		
Work item code:	⌘ WLAN	Date:	⌘ 11/15/2004
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: 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:	⌘ Make sure terms are used consistantly in Sections 1 through 6. Correct spacing, and make simple grammatical corrections
Summary of change:	⌘ Modified capitization and use of terms for consistency. Removed or insert spaces as needed. Removed duplicated words, and made other simple grammar changes.
Consequences if not approved:	⌘ Confusion from using slightly different terms for the same concept. Decreased readability due to simple errors.

Clauses affected:	⌘ Sections 1, 3, 4, 5, and 6										
Other specs Affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><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 ⌘ Test specifications O&M Specifications	
Y	N										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<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.

**** Start of changes ****

1 Scope

This document specifies system description for interworking between 3GPP systems and ~~WLAN~~-Wireless Local Area Networks (WLANs). The intent of 3GPP-WLAN Interworking is to extend 3GPP services and functionality to the WLAN access environment: the 3GPP-WLAN Interworking ~~s~~System. The 3GPP-WLAN Interworking ~~S~~system is assumed to provide bearer services for connecting a 3GPP subscriber via WLAN to IP based services compatible with those offered via PS domain.

This specification defines a 3GPP system and procedures for the following functionalities:

- Provide the ~~I~~nterworking WLAN (~~I~~-WLAN) with a means of Access, Authentication and Authorisation (AAA) through the 3GPP System, which allows WLAN UEs to access ~~the~~ WLAN and the locally connected IP network (e.g. Internet)
- Provide WLAN UEs with IP bearer capability to access PS based services which are provided by PLMN.

**** Second change ****

3 Definitions, symbols and abbreviations

3.1 Definitions

Available SSID: It is an SSID that the WLAN UE has found after active and/or passive scanning which meets certain conditions as specified in IEEE 802.11 [19].

3GPP - WLAN Interworking: Used generically to refer to interworking between the 3GPP system and the WLAN family of standards. Annex B includes examples of WLAN Radio Network Technologies.

Environment: The type of area to be covered by the WLAN network of a 3GPP - WLAN interworking; e.g. public, corporate and residential.

External IP Network/External Packet Data Network: An IP network to which access may be provided through the 3GPP system, rather than directly from the WLAN AN. For example, the Internet, an operator's IP network or a 3rd party IP network such as a corporate IP network.

Home WLAN: The WLAN that is interworking with the HPLMN of the 3GPP - WLAN interworking user.

Interworking WLAN (~~I~~-WLAN): ~~—~~WLAN that interworks with a 3GPP system.

I-WLAN selection: Procedure for the selection among the available I-WLAN APs

Local Service Identifier: An identifier, used within the 3GPP system, for a service available directly from the I-WLAN, for example Internet access or access to a specific corporate network

Offline charging: Offline charging mechanism is provided for collecting and forwarding charging information about occurred WLAN access resource and core network resource usage, etc without affecting the service rendered in real-time.

Online charging: Online charging mechanism is provided where the service rendered is affected in real-time and is required for a direct interaction with session/service control. This allows an online charged subscriber to access WLAN.

Policy Enforcement: Policy Enforcement is implemented in a WAG Packets coming from or going to the WLAN AN are policed based on unencrypted data within the packets. (e.g., source and destination IP address and port number)

PS based services: In WLAN interworking, PS based service is a general term to refer to the services provided by a PLMN using IP bearer capability between WLAN UEs and the PLMN when WLAN 3GPP IP Access is used. They include all services provided by 3G PS domain that use the IP bearer service, (e.g., IMS, Internet access, Corporate IP network access), and other services (e.g., SMS and LCS).

Requested W-APN: The W-APN requested by the user

Routing Enforcement: Routing Enforcement ensures that all packets sent to/from the WLAN UE for 3G PS based service are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case). Routing Enforcement is implemented between a WLAN AN and a WAG.

Selected W-APN: The W-APN selected by the network as a result of the user request

Service Authorization: Authorization for a user to access the requested service according to the user's subscription.

Supported PLMN: A PLMN of a roaming partner (i.e. to which the WLAN operator has a direct roaming relationship).

Tunnel Identifier: Identifier of an end to end tunnel between a UE and a PDG. It is contained in the unencrypted part of the packets

User Identifier: Identifier of a user used for e.g. charging functionality

Visited WLAN: An interworking WLAN that Interworks only with a visited PLMN.

WLAN Access Point Name (W-APN): ~~WLAN Access Point Name~~ identifies an IP network and a point of interconnection to that network (Packet Data Gateway)

WLAN 3GPP IP Access: Access to an IP network via the 3GPP system

WLAN coverage: an area where wireless local area network access services are provided for interworking by an entity in accordance with WLAN standards.

WLAN Direct IP Access: Access to an IP network is direct from the WLAN AN.

WLAN roaming: The ability for a ~~3GPP-WLAN interworking user~~ (subscriber) to function in a serving WLAN different from the home WLAN.

WLAN UE's local IP address: An address that is necessary to deliver the packet to a WLAN UE in a WLAN AN. It identifies the WLAN UE in the WLAN AN. WLAN UE's local IP address may be translated by Network Address Translation prior to being received by the interworking function.

WLAN UE's remote IP address: An address used in the data packet encapsulated by the WLAN UE-initiated tunnel. It represents the identity of the WLAN UE in the network which the WLAN UE is accessing.

****** Third Change ******

4 WLAN Radio networks interworking with 3GPP

This specification defines two new procedures in the 3GPP System:

- WLAN Access, Authentication and Authorisation, which provides for access to the WLAN and the locally connected IP network (e.g. Internet) to be authenticated and authorised through the 3GPP System. Access to a locally connected IP network from the WLAN, is referred to as WLAN Direct IP Access.

- WLAN 3GPP IP Access, which allows WLAN UEs to establish connectivity with External IP networks, such as 3G operator networks, corporate Intranets or the Internet via the 3GPP system.

WLAN 3GPP IP Access should, as far as possible, be technically independent of WLAN Access Authentication and Authorisation. However, WLAN 3GPP IP Access to External IP Networks from 3GPP-WLAN Interworking Systems shall be possible only if WLAN Access Authentication/Authorisation has been completed first.

Note: The independence requirement does not preclude the possibility that the procedure WLAN GPP IP Access may rely on information derived in the procedure for WLAN Access Authorization.

Figure 4.1 illustrates WLAN networks from the point of view of 3GPP interworking.

The Packet Data Gateway supports WLAN 3GPP IP Access to External IP networks. The WLAN includes WLAN access points and intermediate AAA elements. It may additionally include other devices such as routers. The WLAN User Equipment (WLAN UE) includes all equipment that is in possession of the end user, such as a computer, WLAN radio interface adapter etc.

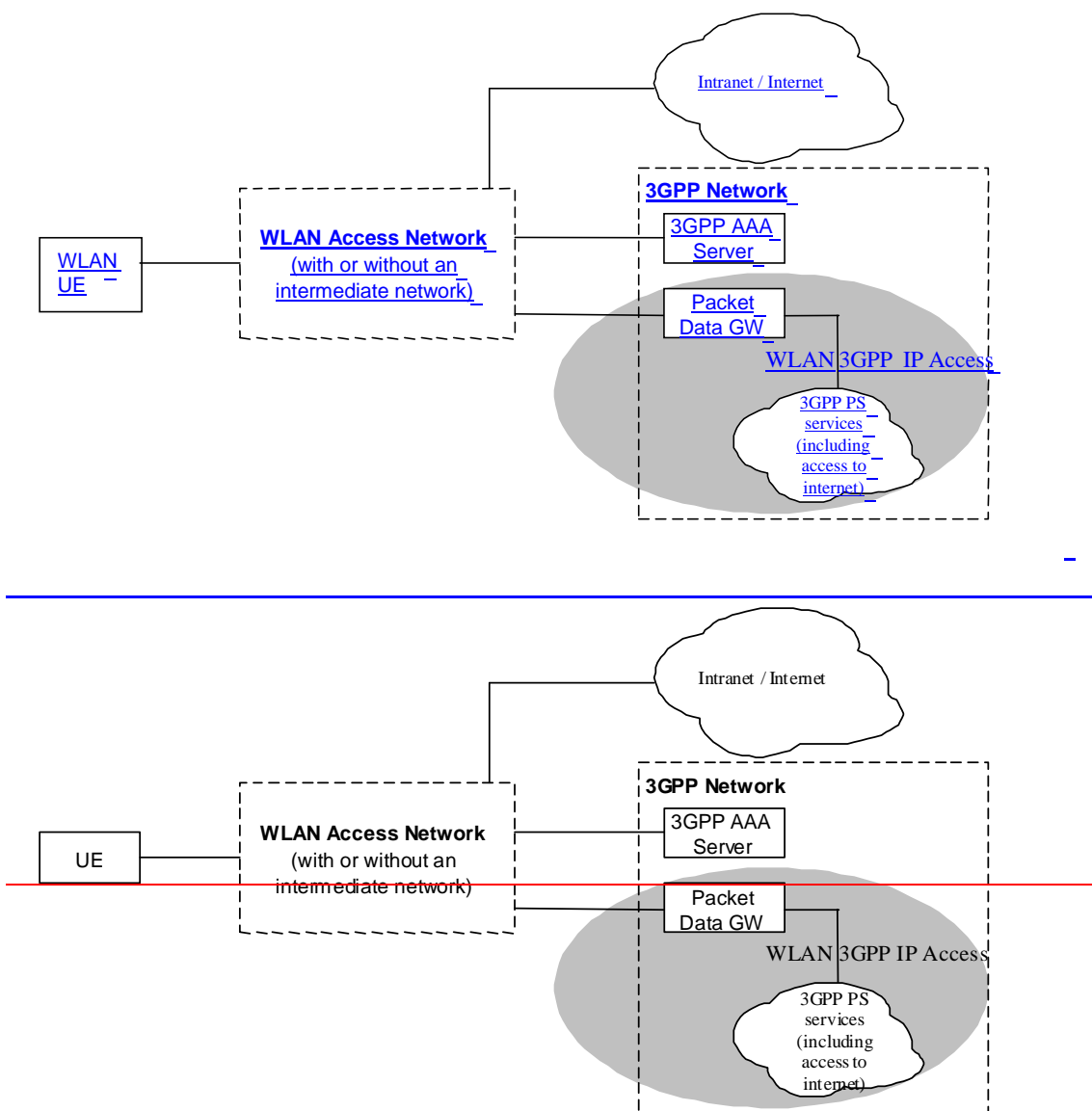


Figure 4.1: Simplified WLAN Network Model. The shaded area refers to WLAN 3GPP IP Access functionality

As 3GPP-WLAN interworking concentrates on the interfaces between 3GPP elements and the interface between the 3GPP system and the WLAN, the internal operation of the WLAN is only considered in order to assess the impact of architecture options/requirements on the WLAN.

3GPP-WLAN interworking shall be independent of the underlying WLAN Radio Technology.

****** Fourth Change ******

5 High-level Requirements and Principles

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 be able to support all 3GPP PS based services.
- 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 ~~WLAN3GPP-WLAN Interworking System~~~~-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 ~~WLAN3GPP-WLAN I~~~~inter-working S~~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 ~~WLAN3GPP-WLAN I~~~~inter-working S~~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.

5.2 Access Control Principles

End to End Authentication: WLAN Authentication signaling is executed between WLAN UE and 3GPP AAA Server for the purpose of authenticating the end-user and authorizing the access to the WLAN and 3GPP network.

Transporting Authentication signalling over WLAN Radio Interface: WLAN authentication signalling is carried between WLAN UE and WLAN AN by WLAN Access Technology specific protocols. To ensure multivendor interoperability these WLAN technology specific protocols shall conform to existing standards of the specific WLAN access technology.

Transporting Authentication signalling between WLAN AN and 3GPP network: WLAN Authentication signalling shall be transported **between any WLAN AN and 3GPP network** by a standard protocol, which is independent of the specific WLAN technology utilised within the WLAN Access network.

Details of end to end authentication and transport of authentication signalling over the WLAN radio interface and between the 3GPP network and WLAN is covered in 3GPP TS 33.234 [10]

WLAN Access Authorization: This defines the process(es) in 3GPP AAA Server verifying whether WLAN Access should be allowed to a subscriber and deciding what access rules/policy should be applied to a subscriber. It is the stage after access authentication, but before service authorisation and WLAN UE's local IP address allocation.

After the authentication process succeeds, there could be additional conditions for the 3GPP AAA Server to decide whether the access is allowed and what access rules/policy should be applied. These conditions may be based on the subscriber's profile, the account status, O&M rules, local agreements or information about the WLAN AN.

The procedure for WLAN Access Authorization between the WLAN UE and the 3GPP AAA Server is combined with the WLAN Access Authentication.

Access rules/policy decided by the 3GPP AAA Server may be deployed in the 3GPP AAA Server, or/and in other entities such as the WAG or the WLAN AN.

Access rules/policy may include access scope limitation, time limitation, bandwidth control values, and/or user priority.

WLAN Access rules/policy should be specified by the home and/or visited operator based on the subscriber's profile, the account status, O&M rules (e.g. blacklist, access limitation list), and local agreements. Factors such as access time and access location could also be considered in these rules.

The access scope limitation could be, for example, only/not/may "access through WAG"; only/not/may "access intranet X".

Access scope limitation can be achieved using IP allocation scheme, VLAN allocation, Filtering, ACLs in the routers and switchers, etc.

Different access priority or the range of priorities may be authorized for different subscribers, and/or for one subscriber based on different access time or location, etc.

3GPP WLAN attach: The WLAN-attach status indicates whether the WLAN UE is now being served by the [3GPP-3GPP-WLAN](#) [WLAN-IW](#) [Interworking System](#) network.

A WLAN UE is "WLAN-attached" after successful authentication and WLAN Access Authorization.

A WLAN UE is "WLAN-detached" in 3GPP network after its disconnection, or its authentication or WLAN Access Authorization being cancelled.

The WLAN-attach status is maintained by the 3GPP AAA server.

The WLAN UE's WLAN attach status should be obtained from the AAA Server directly or through the HSS, by other entities in the 3GPP or 3GPP connected network. Other entities in the 3GPP network obtain the WLAN UE's WLAN-attach status directly from the AAA Server or through the HSS. These entities and the corresponding reference points are not in the scope of this TS.

The description of the corresponding status in the WLAN UE is out of the scope of this TS.

Additional access control principles for WLAN 3GPP IP Access:

Service Selection and Authorisation: The solution shall include means for securely delivering service selection information from the WLAN UE to the 3GPP AAA server in the Home Network. If a user chooses to access the internet directly using the local IP network, no service selection information is passed to the PLMN. In all other cases, where [WLAN](#) 3GPP IP Access is desired, the service selection information shall contain the name of the W-APN to which access is requested. The 3GPP AAA Server in the Home network shall verify the user's subscription to the indicated W-APN against the subscriber profile retrieved from HSS. The 3GPP AAA Server selects a W-APN based on the requested W-APN and on the user's subscription/local policy.

The service request shall be indicated by a tunnel establishment request from the WLAN UE to the PDG. The PDG shall then seek authentication/authorisation from the 3GPP AAA Proxy or Server in the same network.

The results of the authorisation decision shall be communicated to the Visited Network. All subscription-based authorisation decisions are made in the Home network.

In the case of a request for access to services provided in the Visited Network, the 3GPP AAA Proxy shall also authorise access based on local policy.

5.3 User Identity

5.3.1 General

The network authentication procedure is based on the use of EAP method where user identification is based on Network Access Identifier (NAI), whose format is specified in RFC 2486 [12]. A NAI is composed of a username part and a realm part. In the following, the term of 'identity' includes both the NAI username part and the realm part, while the term of 'username' only refers to the NAI username part.

5.3.2 NAI Username

The NAI username part format shall comply with IETF EAP-SIM [23] and EAP-AKA [22]. Three types of usernames are,

1. a Permanent username,
2. a Pseudonym username
3. a Fast re-authentication username.

Both of the Pseudonym and the Fast re-authentication usernames are used in temporary identities, but the purpose and usage of them are different. The first two types of usernames are only used on full authentication and the last one only on fast re-authentication.

The Permanent username, which is specified in IETF EAP-SIM [23] and EAP-AKA [22], shall be derived from IMSI, which resides in the UICC. Details of these are covered in 3GPP TS 33.234 [14], 3GPP TS 24.234 [9] and TS 23.003 [5].

The Pseudonym username is used for user identity protection. The use of the Pseudonym username is necessary to replace the ~~the~~ Permanent username derived from IMSI in radio transmissions, so that it protects the user against tracing from unauthorized access networks.

The Fast re-authentication username is used in fast re-authentication. It also provides user identity protection. For the fast re-authentication, a WLAN UE shall use the previously allocated Fast re-authentication identity as specified in the IETF EAP-SIM [23] ~~and~~ and EAP-AKA [22] Internet-Drafts

Temporary identities (pseudonyms and fast re-authentication identities) are allocated by the 3GPP AAA Server. The format and the procedure for deriving the temporary identities are defined in TS 33.234 [14].

****** Fifth Change ******

5.4 Network Advertisement and Selection

5.4.1 Description of the issue

If the WLAN radio technology allows for features enabling radio access network sharing or provider selection these shall be reused for WLAN Access Network (WLAN AN) selection in 3GPP-WLAN interworking.

In addition to WLAN Access Network selection, the WLAN UE may need to select a VPLMN through which to authenticate, if more than one is available through the chosen radio network.

WLAN Access Network advertisement and selection depends on the particular WLAN technology.

VPLMN advertisement and selection should be independent of WLAN technology.

The generic Network Advertising and Selection scenario is illustrated in Figures 5.1 and 5.2.

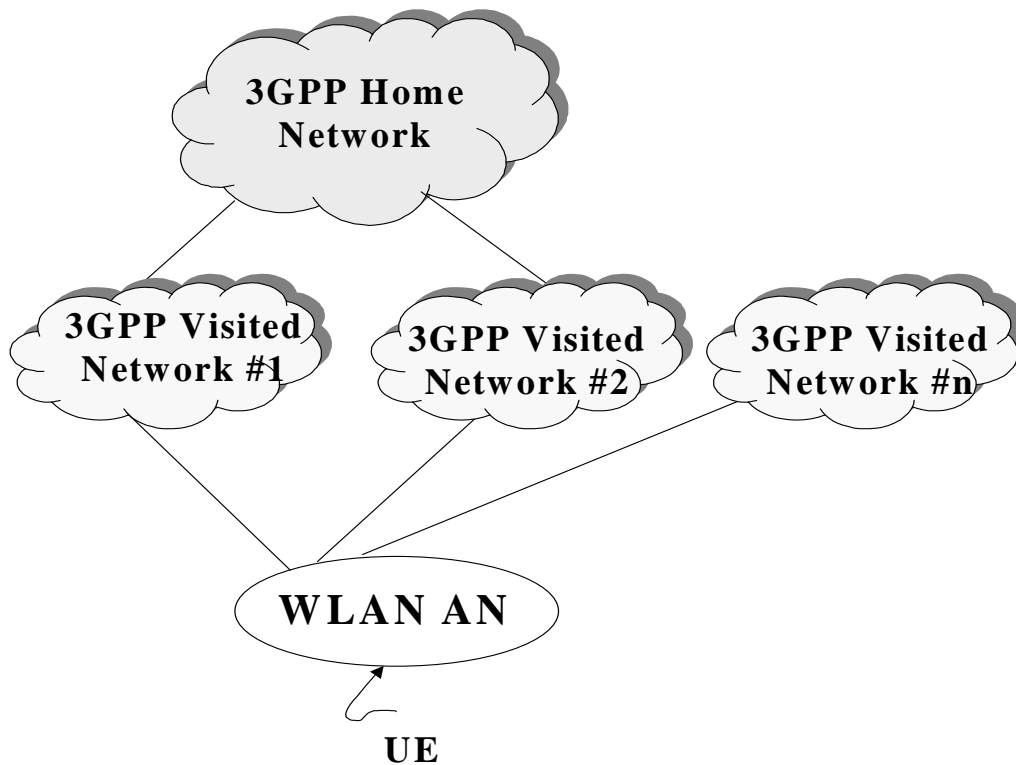


Figure 5.1: Network Advertising and Selection Scenario

An area is shown covered by a WLAN Access Networks having a set of roaming agreements with different 3G networks (3GPP Visited Network #1, #2, ..., #n). A WLAN UE entering the WLAN AN wants to connect to his own 3GPP Home Network to which he is a subscriber (as shown in Figure 5.1).

Referring to the figure the user subscribing to the services provided to the 3GPP Home Network can reach the associated home network in two different ways, e.g. via either of 3GPP Visited Network #1 or 3GPP Visited Network #2.

****** Sixth Change ******

5.4.2.1.3 I-WLAN Access Network Selection

For purpose of selecting the preferred I-WLAN AN the WLAN UE may contain lists of I-WLAN identities' preferences. One list will contain the –SSIDs preferred by the Home Network operator and one list contains the SSID's preferred by the user.

The Operator's preferred SSID list would be populated, for example, with the SSIDs commonly used by major hotspot operators with whom the Home Operator has a direct relationship.

In Manual mode the WLAN UE shall scan (passive scanning) for all available SSIDs in beacon channels it can discover. The WLAN UE may also probe (active scanning) for additional available SSIDs from each of the WLAN networks that it has discovered.

In Manual mode once a list of all available SSIDs has been obtained, it shall be possible for the WLAN UE

to obtain a list of all available PLMNs from each SSID. When a list of PLMNs has been obtained from all SSIDs it shall present them to the user –to select one. The WLAN UE shall then associate with the SSID that supports the PLMN that is selected by the user.

In the automatic mode the procedure is as follows:

0. The WLAN UE scans for all available SSIDs. If the WLAN UE contains the I-WLAN identities' preference lists, the scan should be done in the order of these lists. It is not required to continue the scanning after the highest priority SSID is found.

1. Start association and perform Network Discovery

1a) If authentication to HPLMN succeeds (i.e. EAP-Success is received), then stop this procedure.

1b) If Network Advertisement information is received (i.e. EAP-Identity/Request is received), then store the list and start again step 1.

Repeat step 1 for all available SSIDs following the order specified in the I-WLAN identities preference ~~lists~~ lists. If the scanning in step 0 was stopped due to the discovery of the highest priority SSID, but the HPLMN has not been found (e.g. because the SSID list is not updated or the selected SSID was a fake one), then the user should go back to step 0 and scan for all available SSIDs.

Note that if an AP supporting HPLMN is found in the middle of the procedure, step 1a, then step 1 is stopped and association with the remaining available APs will not take place.

2. Use the lists of 'User Controlled PLMN Selector list for I-WLAN' and 'Operator Controlled PLMN Selector list for I-WLAN' and the lists from step 1b) to select the best matching PLMN. Note that the 'User Controlled PLMN Selector list for I-WLAN' has higher priority than the 'Operator Controlled PLMN Selector list for I-WLAN'. Then select the I-WLAN AN that supports the best match PLMN. If more than one I-WLAN AN supports the best matched PLMN, the I-WLAN AN having the highest priority SSID is selected, if 'I-WLAN identities' preference lists are available.

3. Associate with the AP selected in step 2 and attempt authentication with the best match PLMN. An I-WLAN AN may indicate that it provides 3G interworking without the involvement of any other network than the WLAN AN.

If such an indication is provided by the WLAN AN and if the WLAN UE supports the indication, then the WLAN UE shall use it at SSID selection as defined in 3GPP TS 24.234 [9].

The above requirement may be met through explicit EAP-based procedures or through the generic 'I-WLAN identities' preference lists procedures – for example I-WLAN identities preference lists could include SSID formats defined by operators for the above purposes.

**** Seventh Change ****

5.7.2 Tunnelling Requirements

The requirements that a WLAN UE-Initiated tunnelling protocol should meet are:

- Minimal requirements to the underlying IP connectivity network, i.e. WLAN UE initiated tunnelling and tunnel establishment signalling can be deployed on top of generic IP connectivity networks
- Minimal impacts to the WLAN Access Network
- Establishment of trusted relationships (e.g. mutual authentication for both tunnel end-points) shall be possible
- Tunnel IP configuration of the WLAN UE may be obtained from/through the remote tunnel endpoint
- Set up secure tunnels between WLAN UE and remote tunnel endpoint. Especially support encryption and integrity protection during tunnel establishment and while transporting user data packets, if enabled.
- Remote IP address (inner IP):
 - The transport of IPv4 packets shall be supported
 - The transport of IPv6 packets shall be supported (e.g. in order to support IPv6 services like IMS)
- Local IP address (outer IP):

- The tunnel protocol shall be able to support IPv4 and IPv6 transport addresses
- The tunnel protocol shall support private WLAN UE's local IP addresses, which are non-routable in the public Internet.
- The protocol should be fully specified and 3GPP should define its usage to enable multi-vendor inter-operability.

5.7.3 IMS support over I-WLAN

IMS over I-WLAN in this release is supported without charging correlation and QoS support, i.e. SBLP for I-WLAN is not supported.

See Annex G about alternatives of implementing these functions for IMS over I-WLAN.

5.8 Roaming requirements for WLAN 3GPP IP Access

For the delivery of 3GPP PS based services in a roaming scenario:

- The roaming architecture shall ensure that CDRs can be generated e.g. volume and time based by the visited network.
- The roaming architecture shall ensure that tunnels established are between entities that have a roaming agreement.
- The roaming architecture shall ensure that the bearer path from the WLAN to Home/Visited 3GPP network conforms to QoS and roaming agreement(s).
- The roaming architecture shall provide the ability to allow the user to access services provided by the visited network, e.g. local PS services.
- The roaming architecture shall allow the home network to limit the set of 3GPP services available for a given roaming user.
- All packets of PS based services sent to/from a WLAN UE are routed via a VPLMN in a 3GPP network; however basic Internet access may be routed directly from the WLAN.

5.9 Routing Enforcement and Policy Enforcement for WLAN 3GPP IP Access

5.9.1 Purpose for routing enforcement and policy enforcement

In order to ensure operator policies, e.g. QoS, Charging can be applied to user traffic, WLAN 3GPP IP Access requires routing enforcement and policy enforcement to be implemented in the ~~3GPP~~ 3GPP-3GPP-WLAN-WLAN-~~I~~ interworking Ssystem.

5.9.2 Routing Enforcement in the WLAN AN

Routing enforcement shall be used to ensure that all packets sent to/from the WLAN UE for 3G PS based service are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case). However, this routing enforcement shall not prevent a WLAN AN from routing non 3G PS based service traffic to another network (e.g. the Internet) other than a PLMN, when provision of such services (e.g. direct Internet access from the WLAN) is agreed between the WLAN and the PLMN.

When subscription limits a WLAN UE to exclusively access only 3GPP PS based service, the PLMN can indicate to the WLAN AN routing enforcement to ensure that all packets sent to/from the WLAN UE are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case).

If a WLAN UE user subscription allows a WLAN Direct IP Access the WLAN AN should be capable of routing packets directly to the external packet data network.

Routing enforcement in the WLAN AN shall ensure that packets sent between a PDG and a WLAN UE are routed to the right entity in the interworking VPLMN (roaming case) or HPLMN (no roaming case).

Routing enforcement should not prevent the WLAN AN from supporting a WLAN Direct IP Access only capable WLAN UE or a WLAN 3GPP IP Access capable WLAN UE opting for a WLAN Direct IP Access, and non 3G interworking WLAN ~~terminals.Routing~~[terminals.Routing](#) enforcement should have minimal impact on the WLAN AN.

**** Eighth Change ****

5.12 AAA Protocol Requirements

- A common AAA protocol shall be used for Authentication, Authorization and Accounting purposes in the WLAN Interworking Architecture within the 3GPP network.
- The protocol used for Accounting purpose in the WLAN Interworking Architecture in the 3GPP network shall be the same as used by the 3GPP Charging Architecture ~~eg:e.g.~~ the AAA protocol used by the 3GPP IMS charging architecture,
- If interworking with a legacy AAA protocol is needed, then it shall be performed at the entry and exit point of the 3GPP network. In the case of roaming, such interworking shall be performed in the visited network. The legacy AAA protocol may not support all features of 3GPP AAA protocol. Therefore, this interworking might limit the usage of features existent in 3GPP AAA protocol but not existent in legacy AAA ~~protoco~~[\(protocol](#) (e.g. filtering rules).

**** Ninth Change ****

6.2.6 Packet Data Gateway

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

3GPP PS based services are accessed via a Packet Data Gateway. 3GPP PS based services may be accessed via a Packet Data Gateway in the user's Home Network or a PDG in the selected VPLMN. The process of authorisation and service selection (e.g. W-APN selection) and subscription checking determines whether a service shall be provided by the home network or by the visited network. The resolution of the IP address of the Packet Data Gateway providing access to the selected service will be performed in the PLMN functioning as the home network (in the VPLMN or HPLMN). If the PDG is intended to support connections from WLAN UEs using IPv4 and IPv6 local addresses, it shall be equipped with a dual IP stack.

Successful activation of a selected service results in:

- Determination of the Packet Data Gateway IP address used by the WLAN UE;
- Allocation of a WLAN UE's remote IP address to the WLAN UE (if one is not already allocated);
- Registration of the WLAN UE's local IP address with the Packet Data Gateway and binding of this address with the WLAN UE's remote IP address.

The Packet Data Gateway:

- Contains routing information for WLAN-3G connected users;
- Routes the packet data received from/sent to the PDN to/from the WLAN-3G connected user;
- Performs address translation and mapping;
- Performs de-capsulation and encapsulation;

- accepts or rejects the requested W-APN according to the decision made by the 3GPP AAA Server;
- redirects the tunnel establishment request towards another PDG if this is indicated to be done by the 3GPP AAA Server

Allows allocation of the WLAN UE's remote IP address;

- Relays the WLAN UE's remote IP address allocated by an external IP network to the WLAN UE, when external IP network address allocation is used.
- Performs registration of the WLAN UE's local IP address and binding of this address with the WLAN UE's remote IP address;
- Provides procedures for unbinding a WLAN UE's local IP address with the WLAN UE's remote IP address;
- Provides procedures for authentication and prevention of hijacking (i.e. ensuring the validity of the WLAN UE initiating any binding of the WLAN UE's local IP address with the WLAN UE's remote IP address, unbinding etc.)
- May filter out unauthorised or unsolicited traffic with packet filtering functions. All types of message screening are left to the operators' control, e.g. by use of Internet firewalls.
- Generates per user charging information.
- Delivers the mapping of a user identifier and a tunnel identifier to the AAA Proxy.
- Generates charging information related to user data traffic for offline and online charging purposes.
- May apply IP flow based bearer level charging [13], [15], e.g. in order to differentiate or suppress WLAN bearer charging for 3GPP PS based services.

Annex F describes how PDG functionality can be provided by re-using existing unmodified GGSN functionality.

6.2.7 Subscription Locator Function (SLF)

The SLF is located within the 3GPP subscriber's home network and enables the 3GPP AAA Server to find the address of the HSS which holds the subscriber data for a given user identity in a configuration with multiple separately addressable HSS'es. The SLF should be used in the same way for WLAN as for IMS, which is specified in 3GPP TS 23.228 [24].

****** Tenth Change ******

6.3.9 Wi reference point

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

This is the reference point between the Packet Data Gateway and a packet data network. The packet data network may be an operator external public or private packet data network or an intra operator packet data network, e.g. the entry point of IMS, RADIUS Accounting or Authentication, DHCP.

Wi reference point is similar to the *Gi* reference point provided by the PS domain. Interworking with packet data networks is provided via the Wi reference point based on IP. Mobile terminals offered services via the Wi reference point may be globally addressable through the ~~operators~~operator's public addressing scheme or through the use of a private addressing scheme.

****** Eleventh Change ******

6.4.2 TunnelingTunnelling layer

The ~~tunnelingtunnelling~~ layer consists of a ~~tunnelingtunnelling~~ header, which allows end-to-end ~~tunnelingtunnelling~~ between a WLAN UE and a PDG. It is used to encapsulate IP packets with the remote IP layer.

When encapsulated IP packets are encrypted, the ~~tunnelingtunnelling~~ header contains a field which is used to identify the peer and decrypt the packets.

****** Twelfth Change ******

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 3GPP AAA server via Wx reference point. The profile shall contain the following data items: Detailed work on these parameters is expected in stage 3 work.

1. IMSI

User identification.

2. MSISDN

User identification, for example used for charging purposes

3. Operator determined barring of ~~3GPP3GPP-WLAN-WLAN~~ Interworking subscription

4. Operator determined barring of 3GPP WLAN tunneling

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 charging node 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)

Indicates 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.

- W-APN Subscribed remote IP address

- Operator determined barring for W-APN. As the service requirements defined in TS 22.234

NOTE: Those W-APNs which have a complete barring, shall not be sent to the 3GPP AAA Server

8. Local access allowed

Indicates the local services that the user is allowed to have direct access to from the WLAN Access Network, Network, e.g. Internet, corporate Internet, corporate Intranets. This is indicated in the form of a list of Local Service Identifiers

NOTE: Local Service Identifiers are not passed outside the 3GPP system – access to services within the WLAN is restricted by means of access scope limitations applied on the Wa reference point.

NOTE: In the roaming case, Local Service Identifiers must be agreed between Home and Visited operators. A Local Service Identifier for Internet access should be specified at Stage 3. A Local Service Identifier for each corporate network should be specified at Stage 3.

9. Roaming allowed

Indicates if the user is allowed to use ~~3GPP~~3GPP-WLAN-WLAN Interworking System in an WLAN AN that have no direct connection to the home PLMN.

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

CHANGE REQUEST

23.234 CR 097 # rev **3** # Current version: **6.2.0**

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

Proposed change affects: UICC apps# ME Radio Access Network Core Network

Title:	# Supplement to the subscriber profile procedure		
Source:	# ZTE Corporation		
Work item code:	# WLAN	Date:	# 5/11/2004
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 section 7.3, there are 2 figures on the subscriber update, the first is more like a description on WLAN direct IP access. So there is an additional subtitle on this section. In the procedure, there are some necessary suppliments on the subsequent process after the profile has been updated.
Summary of change:	# To add a subtitle and some necessary suppliments to this procedure.
Consequences if not approved:	# The related description is not completed.

Clauses affected:	# 7.3				
Other specs Affected:	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr> <td style="width: 20px;">Y</td> <td style="width: 20px;">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 # <input type="checkbox"/>	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; vertical-align: middle;"> <tr> <td style="width: 20px;">X</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications # <input type="checkbox"/>	X	<input checked="" type="checkbox"/>		
X					
<input checked="" type="checkbox"/>					
	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr> <td style="width: 20px;">X</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> O&M Specifications # <input type="checkbox"/>	X	<input checked="" type="checkbox"/>		
X					
<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.

***** BEGIN OF 1st MODIFIED SECTION *****

7.3 Subscriber Profile Update

7.3.0 WLAN Direct Access Authorization information update procedure

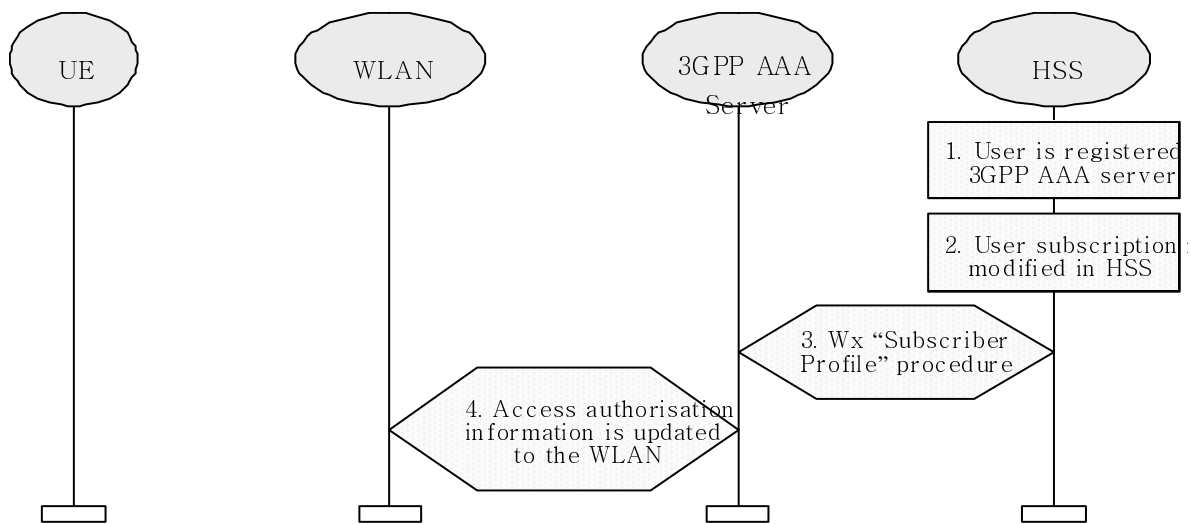


Figure 7.3: Subscriber Profile and access authorization info Update Procedure

1. User is registered to a 3GPP AAA server
2. Subscribers subscription is modified in the HSS e.g. via O&M.
3. HSS updates the profile information stored in the registered 3GPP AAA server by Wx reference point procedure "Subscriber Profile".
4. The WLAN access authorisation information of the associated connection is updated to WLAN as necessary. [If the subscriber loses the authorization of the WLAN access, WLAN shall disconnect the radio interface connection by WLAN technology specific mechanisms.](#)

7.3.1 Access and service Authorization information update procedure

This procedure is for WLAN 3GPP IP Access.

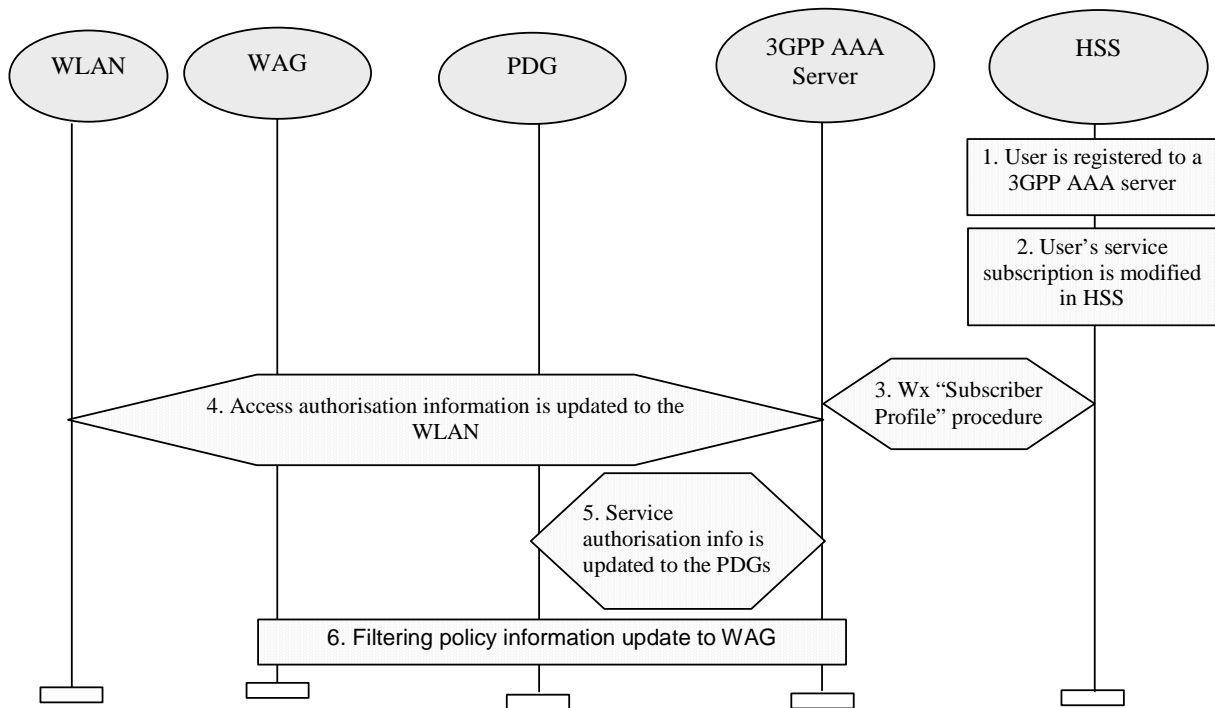


Figure 7.4: Authorization information Update Procedure

1. User is registered to a 3GPP AAA server
2. User's service subscription is modified in the HSS e.g. via O&M,
3. HSS updates the profile information stored in the registered 3GPP AAA server by Wx reference point procedure "Subscriber Profile".
4. The WLAN access authorisation information of the associated connection is updated to WLAN if necessary. [If the subscriber loses the authorization of the WLAN access, WLAN shall disconnect the radio interface connection by WLAN technology specific mechanisms.](#)
5. The service authorisation information of the activated services is updated to PDGs if necessary. A deactivation of service may be initiated if the subscriber lost the authorization of the activated service.
6. The filtering policy information of the activated services is updated to WAG if necessary.

Note: The de-registration may be initiated by the AAA server to the HSS as necessary, i.e., the AAA server determines that the WLAN UE is unable to access any service upon the updated authorization.

***** END OF 1st MODIFIED SECTION *****

3GPP TSG SA SA2 Meeting #42
 Seoul, Korea, 15-19 Nov 2004

S2-043886

CR-Form-v7	
CHANGE REQUEST	
⌘ 23.234 CR 104 ⌘ rev 3 ⌘	Current version: 6.2.0 ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Rewording Readability Changes Section 1	
Source:	⌘ HP, T-Mobile	
Work item code:	⌘ WLAN	Date: ⌘ 11/15/2004
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: 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:	⌘ Several sections of TS 23.234 are hard to understand, are outdated because conclusions were reached by the group, or can be greatly clarified by the use of examples or more text. The goal it to allow the TS to be easily readable by those not in the drafting group.
Summary of change:	⌘ Edit text for clarity, allowing additional text for explanation and example. Reorganize paragraphs if required.
Consequences if not approved:	⌘ Difficulty in reading and using the specification. Changes at this time allow review by several of the orginal members of the WLAN Drafting group, which will not be possible in the future as they move to new assignments.

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

**** Start of changes ****

1 Scope

This document specifies system description for interworking between 3GPP systems and WLAN Local Area Networks (WLANs). The intent of 3GPP-WLAN Interworking is to extend 3GPP services and functionality to the WLAN access environment: ~~the 3GPP-WLAN Interworking system.~~ The 3GPP-WLAN Interworking System ~~is assumed to provide~~ bearer services allowing ~~for connecting~~ a 3GPP subscriber to use a ~~via~~ WLAN to access 3GPP PS ~~IP~~ based services. ~~compatible with those offered via PS domain.~~

This specification defines a 3GPP system architecture and procedures to do ~~for~~ the following ~~functionalities~~:

- ~~Provide the i~~Provide~~interworking WLAN with a means of~~ Access, Authentication and Authorisation (AAA) services to the 3GPP-WLAN Interworking System based on subscription.
- Provide access to the locally connected IP network (e.g. the Internet) if allowed by subscription. ~~through the 3GPP System, which allows WLAN UEs to access WLAN and the locally connected IP network (e.g. Internet)~~
- Provide WLAN UEs with IP bearer capability to the operator's network and PS Services, if allowed by subscription. ~~access PS based services which are provided by PLMN.~~

**** End of changes ****

3GPP TSG SA SA2 Meeting #42
 Seoul, Korea, 15-19 Nov 2004

S2-043909

CR-Form-v7	
CHANGE REQUEST	
⌘ 23.234 CR 107 ⌘ rev 3 ⌘	Current version: 6.2.0 ⌘

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

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Section 5 Reordering	
Source:	⌘ HP	
Work item code:	⌘ WLAN	Date: ⌘ 11/15/2004
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: 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:	⌘ Many ideas were “dumped” into a couple of very high level paragraphs of 5.1 and 5.2. This results in difficult sections to understand since a variety of requirements are co-mingled.
Summary of change:	⌘ Reorganized into new paragraphs based on topic related to the network element they affect (e.g. the WLAN AN, etc). Changed Section 5.1 to include requirements and principles by affected network element. Voided Section 5.2.
Consequences if not approved:	⌘ Difficulty in reading and using the specification. Changes at this time allow review by several of the original members of the WLAN Drafting group, which will not be possible in the future as they move to new assignments.

Clauses affected:	⌘ Section 5					
Other specs Affected:	<table border="1" style="font-size: x-small;"> <tr> <td style="padding: 2px;">Y</td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> </table>	Y	N	⌘	X	Other core specifications ⌘
	Y	N				
	⌘	X				
	<table border="1" style="font-size: x-small;"> <tr> <td style="padding: 2px;">⌘</td> <td style="padding: 2px;">X</td> </tr> </table>	⌘	X	Test specifications		
⌘	X					
<table border="1" style="font-size: x-small;"> <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.

**** Start of changes ****

5 High-level Requirements and Principles

5.1 Access Control ~~Requirements~~

Access Control is the capability to permit or deny a subscriber the use of a resource, in this case the WLAN and/or the interworking to the 3GPP system. The following functional requirements and principles have guided the development of this standard with regard to Access Control~~been identified.~~

5.1.1 WLAN Impacts

The following requirements should be satisfied by the WLAN 3GPP Interworking function with regard to the WLAN itself: ↯

- Legacy WLAN terminals should be supported. However software upgrades may be required for e.g. ~~security reasons to access a (U)SIM.~~
- Existing client hardware and software should be used where ever possible.~~Minimal impact on the user equipment, i.e. client software.~~
- Minimal impact on existing WLAN networks-
- The need for operators to administer and maintain WLAN UE~~end-user~~ software shall be minimized.
- Methods for key distribution to the WLAN access network to allow secure tunnels to be established shall be supported. Note: This does not mean Wireless Equivalent Privacy (WEP) keys in the case of a 802.11 network.
- WLAN Access Authorization shall occur upon the success of the authentication procedure. It may 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).
- Results of WLAN Access Authorization requests shall be indicated to the WLAN, so that the WLAN can take appropriate action.
- It shall be possible to indicate to the user of the results of authorization requests.
- The WLAN Access Authorization mechanism shall be able change service provisioning dynamically, and inform the user and WLAN of any change.
- Transporting Authentication signalling over WLAN Radio Interface: WLAN authentication signalling is carried between WLAN UE and WLAN AN by WLAN Access Technology specific protocols. To ensure multivendor interoperability these WLAN technology specific protocols shall conform to existing standards of the specific WLAN access technology.
- Transporting Authentication signalling between WLAN AN and 3GPP network: WLAN Authentication signalling shall be transported **between any WLAN AN and 3GPP network** by a standard protocol, which is independent of the specific WLAN technology utilised within the WLAN Access network. ~~Details transport of authentication signalling over the WLAN radio interface and between the 3GPP network and WLAN is covered in 3GPP TS 33.234 [10]~~

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.](#) ~~—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. [\(e.g. the HLRSS shall not deregister a PS subscriber when the UE registers on a WLAN\).](#)
- ~~—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. [Please refer to Annex A.](#)

5.1.3 Requirements for WLAN Direct IP Access

The following requirements should be satisfied by the ~~WLAN~~ 3GPP-WLAN Interworking function with regard to allowing direct access to the IP network to which the WLAN is connected (e.g. the Internet):

- A WLAN supporting both WLAN Direct IP Access and WLAN 3GPP IP Access shall be able to support a WLAN UE operating in the WLAN Direct IP Access mode only, e.g. according to subscription.

5.1.4 Requirements for WLAN 3GPP IP Access

The following requirements should be satisfied by the ~~WLAN~~ 3GPP-WLAN Interworking function with regard to allowing access to a WLAN 3GPP IP network (e.g. the operator's intranet which allows IMS access):

~~Additional access control requirements for WLAN 3GPP IP Access:~~

- Service Authorization [for 3GPP services](#) shall occur after the WLAN Access Authentication/Authorization procedure.
- [It shall be possible to use Service B based P policy C 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 be able to support all 3GPP PS based services.

- ~~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 with the subscription for both services should be able to choose between a “WLAN Direct IP Access only” or “a—WLAN 3GPP IP Access”, ~~when the network allows it.~~
- The WLAN UE shall be able to detect ~~When this a WLAN inter working system~~ does not support access to 3GPP PS based services, ~~the WLAN UE shall be able to detect it.~~
- Data flows must be able to ~~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. The enforcement of this ~~is~~ routing ~~enforcement~~ shall not rely on the WLAN UE client.

Note: This routing enforcement may require ~~mandate~~ additional functionality ~~existing~~ in the WLAN AN

- **End to End Authentication:** WLAN Authentication signaling is executed between WLAN UE and 3GPP AAA Server for the purpose of authenticating the end-user and authorizing the access to the WLAN and 3GPP network. Details of End-to-End Authentication is covered in 3GPP TS 33.234 [10].
- **Service Selection and Authorisation:** The solution shall include means for securely delivering service selection information from the WLAN UE to the 3GPP AAA sServer in the Home Network. If a user chooses to access the Internet directly using the local IP network, no service selection information is passed to the PLMN. In all other cases, where WLAN 3GPP IP Access is desired, the service selection information shall contain the name of the W-APN to which access is requested. The 3GPP AAA Server in the Home network shall verify the users subscription to the indicated W-APN against the subscriber profile retrieved from HSS. The 3GPP AAA Server selects a W-APN based on the requested W-APN and on the user's subscription/local policy.
- The service request shall be indicated by a tunnel establishment request from the WLAN UE to the PDG. The PDG shall then seek authentication/authorisation from the 3GPP AAA Proxy or Server in the same network.
- The results of the authorisation decision shall be communicated to the Visited Network. All subscription-based authorisation decisions are made in the Home network.
- In the case of a request for access to services provided in the Visited Network, the 3GPP AAA Proxy shall also authorise access based on local policy.

5.1.5 WLAN Access Authorization

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

5.2 Access Control Principles

~~**End to End Authentication:** WLAN Authentication signaling is executed between WLAN UE and 3GPP AAA Server for the purpose of authenticating the end user and authorizing the access to the WLAN and 3GPP network.~~

~~**Transporting Authentication signalling over WLAN Radio Interface:** WLAN authentication signalling is carried between WLAN UE and WLAN AN by WLAN Access Technology specific protocols. To ensure multivendor interoperability these WLAN technology specific protocols shall conform to existing standards of the specific WLAN access technology.~~

~~**Transporting Authentication signalling between WLAN AN and 3GPP network:** WLAN Authentication signalling shall be transported **between any WLAN AN and 3GPP network** by a standard protocol, which is independent of the specific WLAN technology utilised within the WLAN Access network.~~

~~Details of end to end authentication and transport of authentication signalling over the WLAN radio interface and between the 3GPP network and WLAN is covered in 3GPP TS 33.234 [10]~~

WLAN Access Authorization: This [WLAN Access Authorization](#) defines the process(es) in 3GPP AAA Server verifying whether WLAN Access should be allowed to a subscriber and deciding what access rules/policy should be applied to a subscriber. It is the stage after access authentication, but before service authorisation and WLAN UE's local IP address allocation.

After the authentication process succeeds, there could be additional conditions for the 3GPP AAA Server to decide whether the access is allowed and what access rules/policy should be applied. These conditions may be based on the subscriber's profile, the account status, O&M rules, local agreements or information about the WLAN AN.

The procedure for WLAN Access Authorization between the WLAN UE and the 3GPP AAA Server is combined with the WLAN Access Authentication.

Access rules/policy decided by the 3GPP AAA Server may be deployed in the 3GPP AAA Server, or/and in other entities such as the WAG or the WLAN AN.

Access rules/policy may include access scope limitation, time limitation, bandwidth control values, and/or user priority.

WLAN Access rules/policy should be specified by the home and/or visited operator based on the subscriber's profile, the account status, O&M rules (e.g. blacklist, access limitation list), and local agreements. Factors such as access time and access location could also be considered in these rules.

The access scope limitation could be, for example, only/not/may "access through WAG"; only/not/may "access intranet X".

Access scope limitation can be achieved using IP allocation scheme, VLAN allocation, Filtering, ACLs in the routers and switchers, ~~etc.~~[or other methods](#).

Different access priority or the range of priorities may be authorized for different subscribers, and/or for one subscriber based on different access time or location, etc.

5.1.5 3GPP WLAN Attach

3GPP WLAN attach: ~~The WLAN attach~~ status indicates whether the WLAN UE is now being served by the 3GPP-[WLAN Interworking System W-network](#).

A WLAN UE is "WLAN-attached" after successful authentication and WLAN Access Authorization.

A WLAN UE is "WLAN-detached" in 3GPP network after its disconnection, or its authentication or WLAN Access Authorization being cancelled.

The WLAN-attach status is maintained by the 3GPP AAA ~~s~~[S](#)Server.

The WLAN UE's WLAN attach status should be obtained from the [3GPP](#) AAA Server directly or through the HSS, by other entities in the 3GPP or 3GPP connected network. Other entities in the 3GPP network obtain the WLAN UE's WLAN-attach status directly from the [3GPP](#) AAA Server or through the HSS. These entities and the corresponding reference points are not in the scope of this TS.

The description of the corresponding status in the WLAN UE is out of the scope of this TS.

~~Additional access control principles for WLAN 3GPP IP Access:~~

~~**Service Selection and Authorisation:** The solution shall include means for securely delivering service selection information from the WLAN UE to the 3GPP AAA server in the Home Network. If a user chooses to access the internet directly using the local IP network, no service selection information is passed to the PLMN. In all other cases, where [WLAN 3GPP IP Access](#) is desired, the service selection information shall contain — the name of the W-APN to which access is requested. The 3GPP AAA Server in the Home network shall verify the users subscription to the indicated W-APN against the subscriber profile retrieved from HSS. The 3GPP AAA Server selects a W-APN based on the requested W-APN and on the user's subscription/local policy.~~

~~The service request shall be indicated by a tunnel establishment request from the WLAN UE to the PDG. The PDG shall then seek authentication/authorisation from the 3GPP AAA Proxy or Server in the same network.~~

~~The results of the authorisation decision shall be communicated to the Visited Network. All subscription based authorisation decisions are made in the Home network.~~

~~In the case of a request for access to services provided in the Visited Network, the 3GPP AAA Proxy shall also authorise access based on local policy.~~

5.2 Void

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