

Source: TSG SA WG2
Title: CRs on 23.234 (3GPP WLAN interworking)
Agenda Item: 7.2.3

The following Change Requests (CRs) have been approved by TSG SA WG2 and are requested to be approved by TSG SA plenary #25.

S2 doc #	Title	Spec	CR #	cat	Versi on in	Rel	WI	S2 meeting	Clauses affected
S2-042933	WLAN Manual PLMN Network selection - CR	23.234	033r3	F	6.1.0	6	WLAN	S2 #41	5.4.2.1.3, 5.4.3
S2-042522	Cleanup of figure 7.4 in TS 23.234	23.234	055r1	D	6.1.0	6	WLAN	S2 #41	7.3.1
S2-042523	Correction of mistakes and inaccurate descriptions in 23.234	23.234	058r1	F	6.1.0	6	WLAN	S2 #41	3.3, 6.3.3, 6.3.6, 6.3.12, 6.5, 7.10.3, 7.12.1, D.1.1
S2-042518	Clarification on usage of 3GPP AAA server	23.234	061r1	F	6.1.0	6	WLAN	S2 #41	6.2.3, 6.2.4
S2-042964	Alignment of PLMN selection	23.234	063r4	F	6.1.0	6	WLAN	S2 #41	2, 5.4.2, 5.4.3
S2-042500	Correction of Wa reference point functionality	23.234	064r1	F	6.1.0	6	WLAN	S2 #41	6.3.1.2
S2-042519	Multiple WLAN connections	23.234	065r1	F	6.1.0	6	WLAN	S2 #41	7.2
S2-042503	Introduction of the WLAN registration within tunnel establishment procedure	23.234	066r1	F	6.1.0	6	WLAN	S2 #41	7.9
S2-042482	Editorial update of already agreed change in figure 6.2b	23.234	068	F	6.1.0	6	WLAN	S2 #41	6.1.2
S2-042483	Removal of issue chapter in Annex F.	23.234	069	D	6.1.0	6	WLAN	S2 #41	F.4
S2-042502	Clarification of NSAPI in Annex F.	23.234	070r1	F	6.1.0	6	WLAN	S2 #41	F.3.0, F.3.1
S2-042509	CR on IMS over WLAN	23.234	071r1	F	6.1.0	6	WLAN	S2 #41	5.7, 6.2.6, a new Annex G
S2-042967	Correction to temporary identity usage and reference	23.234	072r3	F	6.1.0	6	WLAN	S2 #41	5.3.1, 5.3.2, 5.3.4
S2-042875	Correction to PDG Selection Mechanism	23.234	073r2	F	6.1.0	6	WLAN	S2 #41	5.6.1, 5.6.2
S2-042932	Correction to W-APN authorisation and PDG redirection Mechanism	23.234	075r3	F	6.1.0	6	WLAN	S2 #41	7.9, 7.9.1
S2-042934	WLAN User Profile revision	23.234	076r3	F	6.1.0	6	WLAN	S2 #41	6.3.2, 6.5
S2-042930	Charging related data for 3GPP PS based services (WLAN 3GPP IP Access)	23.234	077r3	F	6.1.0	6	WLAN	S2 #41	2, 5.11, 6.3.10, 7.9
S2-042931	Static Remote IP address allocation	23.234	078r3	F	6.1.0	6	WLAN	S2 #41	5.10, 6.2.3, 6.3.10, 7.9
S2-042968	Storage of the AAA server IP address in HSS/HLR	23.234	081r2	F	6.1.0	6	WLAN	S2 #41	6.2.4

CR-Form-v7
CHANGE REQUEST
23.234 CR 033 rev 3 Current version: 6.1.0

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

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

Title:	WLAN Manual PLMN Network selection		
Source:	SA2 (RIM, T-Mobile)		
Work item code:	WLAN	Date:	5/08/2004
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:	It is unclear in Stage 2 whether Manual Network selection will occur if the WLAN UE uses an SSID that has a direct relationship with the HPLMN.
Summary of change:	The proposed change reflects the need for the ability of the WLAN UE to retrieve all available PLMNs during manual network selection.
Consequences if not approved:	Manual Network selection will not behave consistently and will lead to poor user experience.

Clauses affected:	5.4.2.1.3, 5.4.3										
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 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.

*****New Text For the TS*****

Proposed changes

****1st Change****

5.4.2.1.3 Network Selection

The WLAN UE shall store a list of and Preferred SSIDs provided by the Home Network operator and shall also maintain a list of the user's Preferred SSIDs.

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 oOnce a list of all available SSIDs has been obtained, it shall be possible for the WLAN UE ~~shall~~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.

****2nd Change****

5.4.3 ~~V~~PLMN Advertisement and Selection

5.4.3.1 General

The following principles shall be used in ~~V~~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. Details on the usage and coding of Network advertisement information are included in 3GPP TS 24.234 [9].

****End of Changes****

CR-Form-v7

CHANGE REQUEST

23.234 CR 055 rev 1 Current version: **6.1.0**

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

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

Title:	Cleanup of figure 7.4 in TS 23.234		
Source:	SA2 (Orange)		
Work item code:	WLAN	Date:	16/08/2004
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: 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:	In TS 23.234, Figure 7.4 does not appear correctly.
Summary of change:	Re-edition of Figure 7.4.
Consequences if not approved:	

Clauses affected:	7.3.1						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> O&M Specifications	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
Other comments:							

How to create CRs using this form:

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

- 1) Fill out the above form. The symbols above marked contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

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

***** Start of Changes *****

7.3.1 Access and service Authorization information update procedure

This procedure is for WLAN 3GPP IP Access.

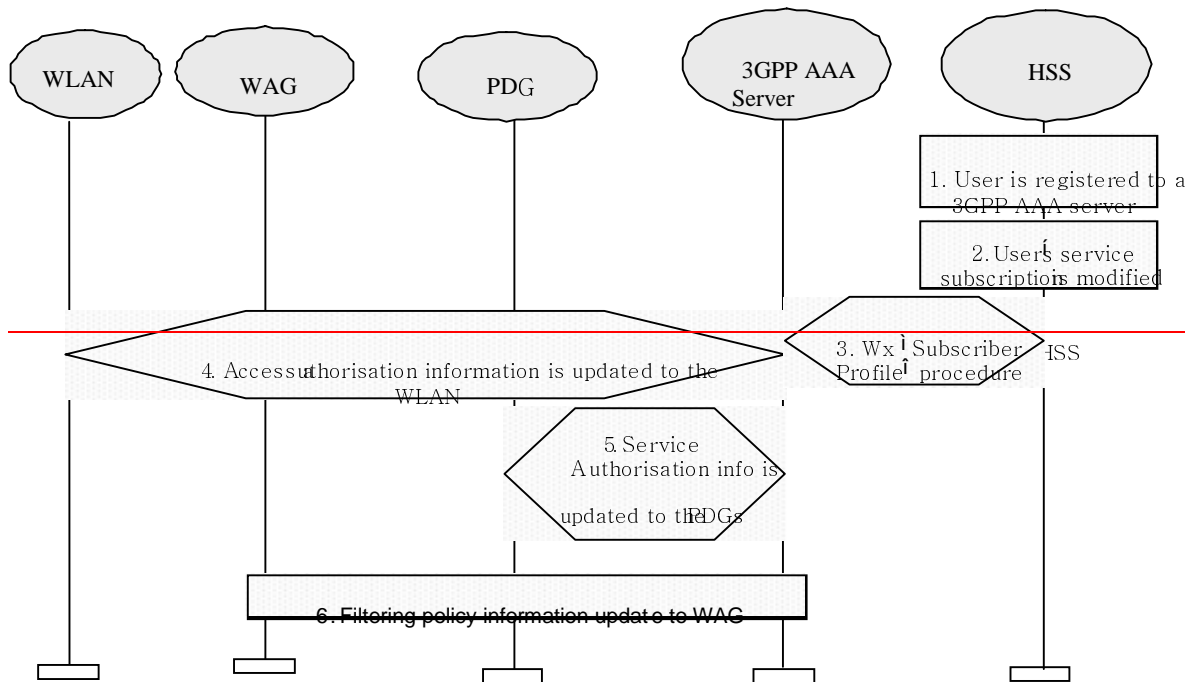
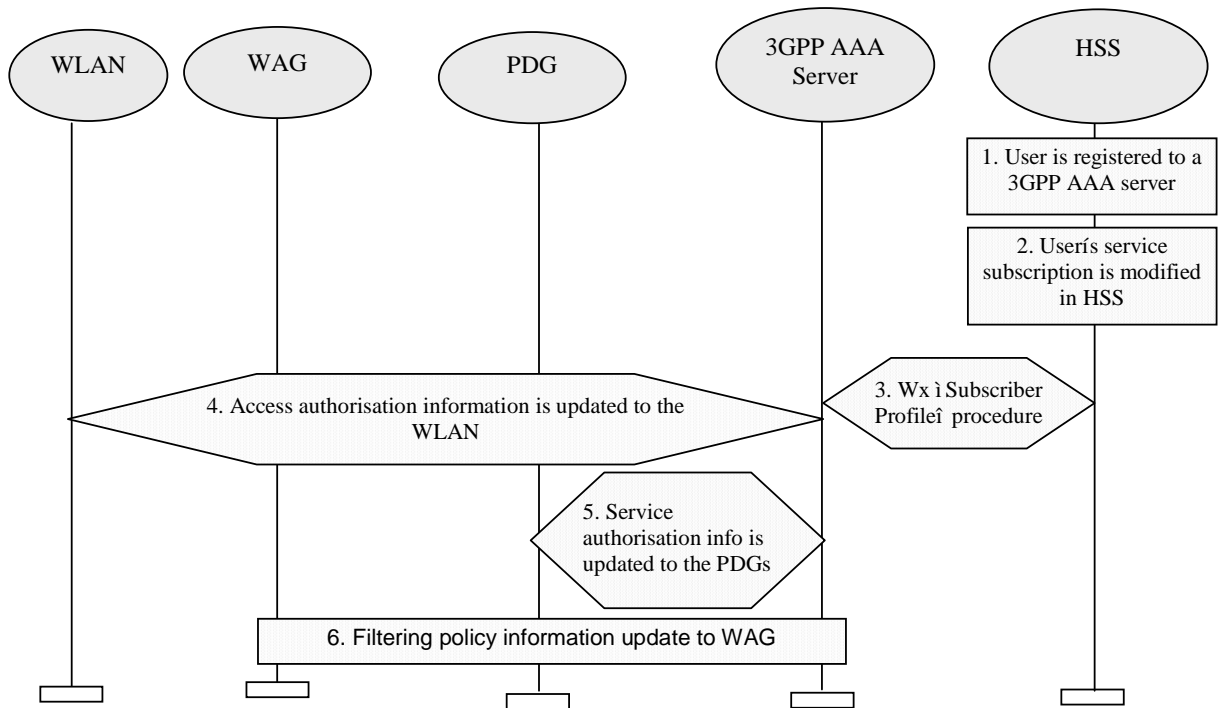


Figure 7.4: Authorization information Update Procedure

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.
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.

CR-Form-v7.1

CHANGE REQUEST

23.234 CR 058 rev 1 Current version: 6.1.0

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

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


Title:	Correction of mistakes and inaccurate descriptions in 23.234		
Source:	SA2 (China Mobile,Huawei)		
Work item code:	WLAN	Date:	18/08/2004
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:	There are some mistakes and inaccurate descriptions in current TS.		
Summary of change:	<ol style="list-style-type: none"> 1. Add definitions on VLAN and ACL in abbreviations table. 2. Correct the difiniton of Wg in clause 6.3.6 3. Confirm that Wu reference point was implemented via Wn,Wp and Ww reference points in clause 6.3.12. 4. Correct the description for SMS-IWMSC in section D.1.1 of Annex D: Replace that GMSC with SMS-IWMSC 5. Correct some editorial mistales 		
Consequences if not approved:	Mistakes and inaccurate descriptions may lead to be misleading in some aspects. And specification will be not complete.		

Clauses affected:	3.3, 6.3.3, 6.3.6, 6.3.12, 6.5, 7.10.3, 7.12.1, D.1.1						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">X</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications	X	<input checked="" type="checkbox"/>				
X							
<input checked="" type="checkbox"/>							
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">X</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> O&M Specifications	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.

***** MODIFIED SECTION *****

3.3 Abbreviations

AAA	Authentication, Authorisation and Accounting
<u>ACL</u>	<u>Access Control List</u>
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
<u>VLAN</u>	<u>Virtual Local Area Network</u>
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 MODIFIED SECTION *****

6.3.3 D'/Gr' reference point

This optional reference point is located between 3GPP AAA Server and pre-R6 HLR/HSS. The prime purpose of the protocol(s) crossing this reference point is communication between WLAN AAA infrastructure and HLR. The protocol crossing this reference point is based upon the D/Gr reference points defined in 3GPP TS 29.002 ~~f7~~[10]. Support of the D'/Gr' reference points requires no modifications to the MAP protocol at the HLR.

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

- Retrieval of authentication vectors, e.g. for USIM authentication, from HLR.

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

The functions provided on the D'/Gr' reference points are a subset of the functions provided on the D/Gr reference points described in 3GPP TS 29.002 [\[10\]](#)~~[7]~~.

If a 3GPP AAA Server supports the D' reference point, it will appear to the HLR/HSS as a VLR and shall behave according to the description of the behaviour of a VLR supporting the D reference point as described in 3GPP TS 29.002 [\[10\]](#)~~[7]~~.

If a 3GPP AAA Server supports the Gr' reference point, it will appear to the HLR/HSS as an SGSN and shall behave according to the description of the behaviour of an SGSN supporting the Gr reference point as described in 3GPP TS 29.002 ~~[7]~~[\[10\]](#).

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

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

6.3.6 Wg reference point

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

This is an AAA interface between the 3GPP AAA Server/Proxy and the WAG. It is used to

- Provide information needed by the WAG to perform policy enforcement functions for authorised users.
- Transport per-tunnel based charging information from the WAG to the AAA Proxy, [only for roaming scenario](#).

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

6.3.12 Wu reference point

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

The Wu reference point is located between the WLAN UE and the Packet Data Gateway. It represents the WLAN UE-initiated tunnel between the WLAN UE and the Packet Data Gateway. Transport for the Wu reference point protocol is provided by the [Ww](#), Wn and Wp reference points, which ensure that the data are routed via the WLAN Access Gateway where routing enforcement is applied.

The functionality of the Wu reference point is to enable:

- WLAN UE-initiated tunnel establishment
- User data packet transmission within the WLAN UE-initiated tunnel
- Tear down of the WLAN UE initiated tunnel

***** NEXT 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 (optional)

User identification, for example used for charging purposes

3. Operator determined barring of 3GPP-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 "access allowed" flag 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. Charging mode (pre-paid, post-paid, both) and accounting server identifier(s) for every charging mode

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. Each W-APN shall have a flag indicating whether access is allowed in visited PLMNs or in the home PLMN.

8. Local access allowed

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 and 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-WLAN Interworking in an WLAN AN that have no direct connection to the home PLMN.

***** NEXT 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 after the disconnection of the tunnel, a disconnection procedure will proceed as described in section 7.6 (step~~2~~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 MODIFIED SECTION *****

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.x.27.12.2~~ 7.12.2 presents an example of the session flow when the 3GPP AAA Server needs to query the SLF.

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

D.1.1 IP Short Message Gateway (IP-SM-GW)

The IP-SM-GW shall provide the protocol interworking for delivery of the short message between the IP client and the GSM/UMTS network. The functions of this network element are:

- To connect to the GMSC using established MAP protocols over SS7, appearing to the GMSC as an MSC or SGSN using the E or Gd reference points
- To connect to the SMS-IW MSC using established MAP protocols over SS7, appearing to the SMS-IW MSC ~~GMSC~~ as an MSC or SGSN using the E or Gd reference points

- To communicate with the IP client using IP based protocols maintaining the format and functionality of the SMS message. It is intended that existing messaging protocols supported by the UE should be reused for this purpose.
- To maintain the association between the MSISDN and the IP address of the terminal
- Support registration and authentication of the UE for SMS services
- Support of security associations between UE and IP-SM-GW

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

CR-Form-v7.1

CHANGE REQUEST

23.234 CR 061 rev 1 Current version: 6.1.0

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

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


Title:	Clarification on usage of 3GPP AAA server		
Source:	SA2 (Huawei)		
Work item code:	WLAN	Date:	18/08/2004
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: <i>Ph2</i> (GSM Phase 2) <i>R96</i> (Release 1996) <i>R97</i> (Release 1997) <i>R98</i> (Release 1998) <i>R99</i> (Release 1999) <i>Rel-4</i> (Release 4) <i>Rel-5</i> (Release 5) <i>Rel-6</i> (Release 6) <i>Rel-7</i> (Release 7)

Reason for change:	It is not clear in the current TS whether multiple AAA servers for a WLAN subscriber are needed. If it is allowed, much complexity will come to the current architecture for handling the different info in different AAA server, extra burden to HSS/HLR will also happen by duplicated retrieving of user information/profile and some judgement can not be done by AAA servers themselves because of multiple servers situation.
Summary of change:	It is clarified in the TS that there shall be only one 3GPP AAA server for a WLAN attached subscriber. Functionality of 3GPP AAA server, HSS are updated to avoid multiple AAA servers for a WLAN subscriber.
Consequences if not approved:	Confusions keep in current stage3 and stage 2 work. Unnecessary complexity will be added to the current architecture.

Clauses affected:	6.2.3, 6.2.4										
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;">X</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> </table>	Y	N	X	X	X	X	X	X	Other core specifications Test specifications O&M Specifications	
Y	N										
X	X										
X	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.

#####

The Changes

#####

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 to the HPLMN CCF/CGw.
- [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 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.

6.2.4 HLR/HSS

The HLR/HSS located within the 3GPP subscriber's home network is the entity containing authentication and subscription data required for the 3GPP subscriber to access the WLAN interworking service.

The HSS also provides access to the WLAN UE's WLAN-attach status for other entities, e.g. answers or relays the WLAN-attach status query from other entities (which are out of the scope of this TS).

[When a 3GPP AAA Server other than the registered 3GPP AAA Server of a subscriber, requests authentication information or the profile of the subscriber, the HSS should request it transfer the authentication to the registered 3GPP AAA Server by providing the registered 3GPP AAA Server address to it.](#)

CHANGE REQUEST

⌘ **23.234 CR 063** ⌘ rev **4** ⌘ Current version: **6.1.0** ⌘

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

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

Title:	⌘ Alignment of PLMN selection		
Source:	⌘ SA2 (Telecom Italia S.p.A.)		
Work item code:	⌘ WLAN	Date:	⌘ 16/08/2004
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:	⌘ To align the Network selection procedure to the I-WLAN interworking requirement defined in TS 22.234 and in proposed SA1 CR 006 rev1, CR 009
Summary of change:	⌘ Revision of Network selection procedure to align the procedure to TS 22.234 requirements.
Consequences if not approved:	⌘ Disalignement between stage 1 and stage 2 requirements

Clauses affected:	⌘ 2, 5.4.2, 5.4.3										
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.

****** 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 networksó 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.
- [21] IEEE Std 802.11-1999, Local and metropolitan area networksó Specific requirementsó 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-11 (October 2003).
- [23] IETF Internet-Draft: "EAP SIM Authentication" draft-haverinen-pppext-eap-sim-12 (October 2003).
- [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"](#)

******2nd 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 shall maintain a list of I-WLAN identities' preferences. One list will contain the preferred SSIDs provided by the Home Network operator and one list shall also maintain a list of contains the SSIDs preferred by the user's Preferred SSIDs.~~

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.

Once a list of all available SSIDs has been obtained, the WLAN UE

shall obtain a list of 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 lists of 'the I-WLAN identities preference lists Preferred SSIDs for WLAN access'~~. 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 Preferred PLMNs for WLAN access'~~ and the lists from step 1b) to ~~s~~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 ~~V~~PLMN. If more than one I-WLAN AN supports the best matched ~~V~~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 Preferred SSID-lists~~ procedures ~~n~~ for example ~~Preferred SSID-I-WLAN identities preference~~-lists could include SSID formats defined by operators for the above purposes.

5.4.2.2 Case of other WLANs

Other WLANs, such as HiperLAN or Bluetooth, are not described in this TS but not excluded.

5.4.3 VPLMN Advertisement and Selection

5.4.3.1 General

The following principles shall be used in VPLMN 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. Details on the usage and coding of Network advertisement information are included in 3GPP TS 24.234 [9].

5.4.3.3 Network Selection

[The automatic and manual mode PLMN selection procedures are defined in TS 22.234 \[25\]. The detailed procedure in case of IEEE 802.11 WLAN is described in 5.4.2.](#)

The WLAN UE shall indicate its home network through the use of an initial NAI. The realm part of this initial NAI shall be derived from the IMSI, as described in section 5.3.3. Optionally, if there is preference for a roaming network, the initial NAI then takes the form of a Roaming NAI, as described in section 5.3.4; e.g., ~~F~~for optimizing user access experience in re-access case, the WLAN UE may include information of preferred roaming network from previous successful authentication while it is associated to the same AP.

For the manual selection case allowed by some operator, initial NAI can include the roaming network decided by the user, e.g. using a preferred PLMN list stored in the UICC.

If the WLAN AN is able to route authentication request based on the initial NAI, then no special processing for network advertisement/selection is needed.

If the WLAN AN is unable to route authentication request from WLAN UE based on the initial NAI, the WLAN AN shall deliver the network advertisement information to the WLAN UE. The WLAN UE processes this information according to its internal roaming preference policies or prompts the user to select a VPLMN preference. It uses the result to determine how to construct a new NAI indicating the selected VPLMN, according to Section 5.4.2.

After the network advertisement information is delivered and VPLMN selection is performed, the WLAN UE attempts to authenticate with the new NAI determined in the prior step.

The WLAN AN shall use the NAI to route the AAA traffic to the appropriate VPLMN AAA Proxy.

CHANGE REQUEST

23.234 CR 064 rev 1 Current version: **6.1.0**

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

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


Title:	Correction of Wa reference point functionality		
Source:	SA2 (Nokia)		
Work item code:	WLAN	Date:	18/08/2004
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: <i>Ph2</i> (GSM Phase 2) <i>R96</i> (Release 1996) <i>R97</i> (Release 1997) <i>R98</i> (Release 1998) <i>R99</i> (Release 1999) <i>Rel-4</i> (Release 4) <i>Rel-5</i> (Release 5) <i>Rel-6</i> (Release 6) <i>Rel-7</i> (Release 7)

Reason for change:	The current version of TS 23.234 is confusing whether procedures for online charging over Wa is mandatory or optional or prohibited. According to clause 6.3.1.2 the online charging shall be "transparent" to the Wa and the WLAN AN. However procedures for online charging in clause 7 define quota based charging procedures within the WLAN AN and hence cannot be transparent to the Wa and the WLAN AN.
Summary of change:	The proposal is to state that the support of online charging over Wa (as it is specified in clause 7) is an optional feature.
Consequences if not approved:	There will be a contradiction in the TS.

Clauses affected:	6.3.1.2										
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 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.

6.3.1 Wa reference point

6.3.1.1 General description

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

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

EAP authentication shall be transported over the Wa reference point.

6.3.1.2 Functionality

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

- Carrying data for authentication signalling between WLAN UE and 3GPP Network.
- Carrying data for authorization signalling between WLAN AN and 3GPP Network. These data may include a well-defined identification of the WLAN AN.
- Carrying charging signalling per WLAN user. ~~The data carried on the Wa interface shall to enable both offline and/or online charging. To minimize the requirements put on the WLAN Access Network, the use of online charging over Wa is optional and depends on the agreement between the operators of the WLAN AN and the 3GPP PLMN. and to protect the confidentiality of the subscriber's charging status the fact whether a user is offline or online charged by his 3GPP subscription provider shall be transparent for the WLAN AN and thus for the Wa reference point.~~ to enable both offline and/or online charging. To minimize the requirements put on the WLAN Access Network, the use of online charging over Wa is optional and depends on the agreement between the operators of the WLAN AN and the 3GPP PLMN.
- Enabling the identification of the operator networks amongst which the roaming occurs.
- Carrying keying data for the purpose of radio interface integrity protection and encryption.
- May carry Routing Enforcement information from the PLMN to ensure that all packets sent to/from the WLAN UE for PS based services are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case) appropriately.
- When such functionality is supported by the WLAN AN, purging a user from the WLAN access for immediate service termination
- Providing access scope limitation information to the WLAN based on the authorised services for each user (for example, IP address filters)

CR-Form-v7.1

CHANGE REQUEST

23.234 CR 065 rev 1 Current version: **6.1.0**

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

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

Title:	Multiple WLAN connections		
Source:	SA2 (Nokia)		
Work item code:	WLAN	Date:	11/08/2004
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:	At SA2#40 meeting it was agreed (based on the LS from SA1: S2-041751) that no multiple WLAN connections to different VPLMNs or WLAN ANs shall be allowed to the WLAN UE. This agreement has not been implemented in the specification.
Summary of change:	During the authentication procedure the AAA server and HSS checks whether there is a previously established authentication session of the WLAN user. If yes then the previously established session is removed.
Consequences if not approved:	The TS will not reflect the requirements received from SA1 (S2-041751) and it will remain ambiguous whether multiple WLAN connections are allowed.

Clauses affected:	7.2						
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;">X</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications	X	<input checked="" type="checkbox"/>				
X							
<input checked="" type="checkbox"/>							
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">X</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> O&M Specifications	X	<input checked="" type="checkbox"/>				
X							
<input checked="" type="checkbox"/>							
Other comments:							

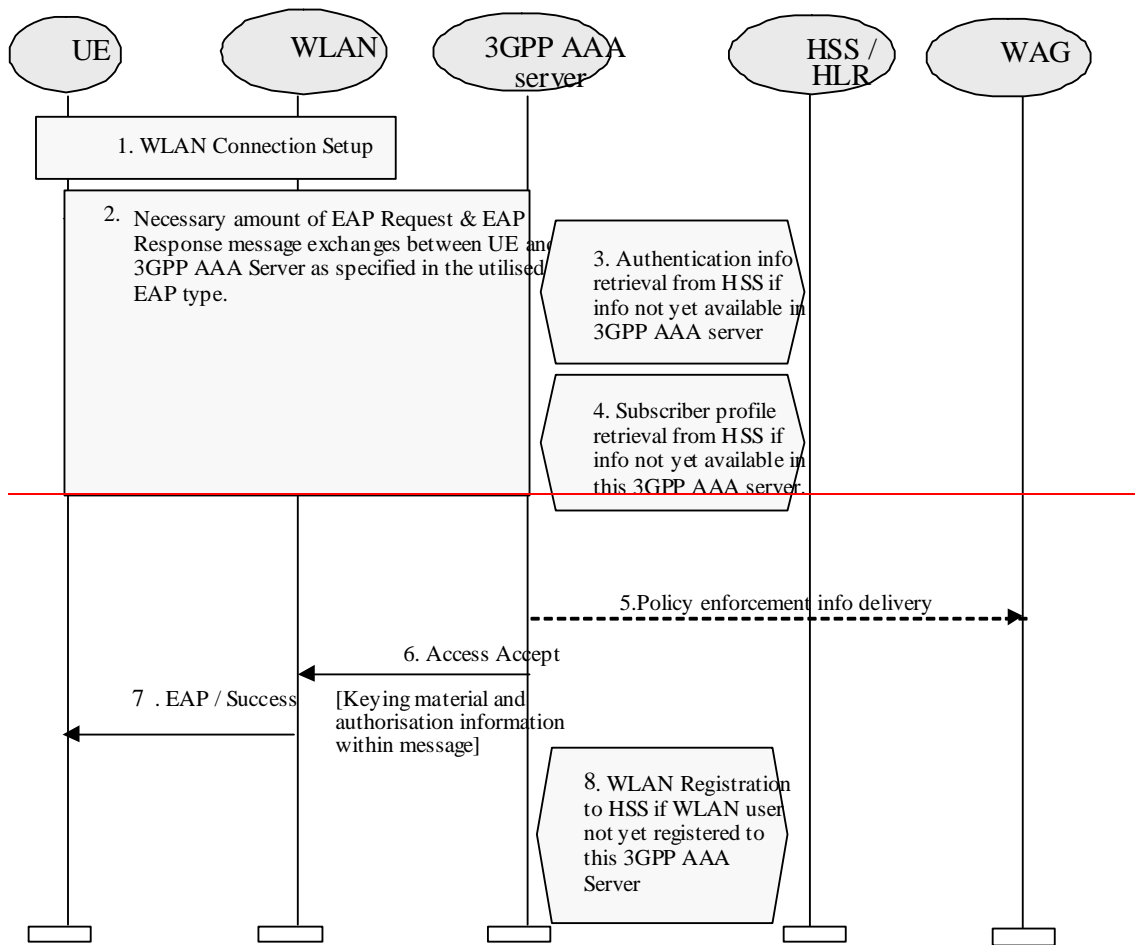
How to create CRs using this form:

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.

7.2 WLAN Access Authentication and Authorisation



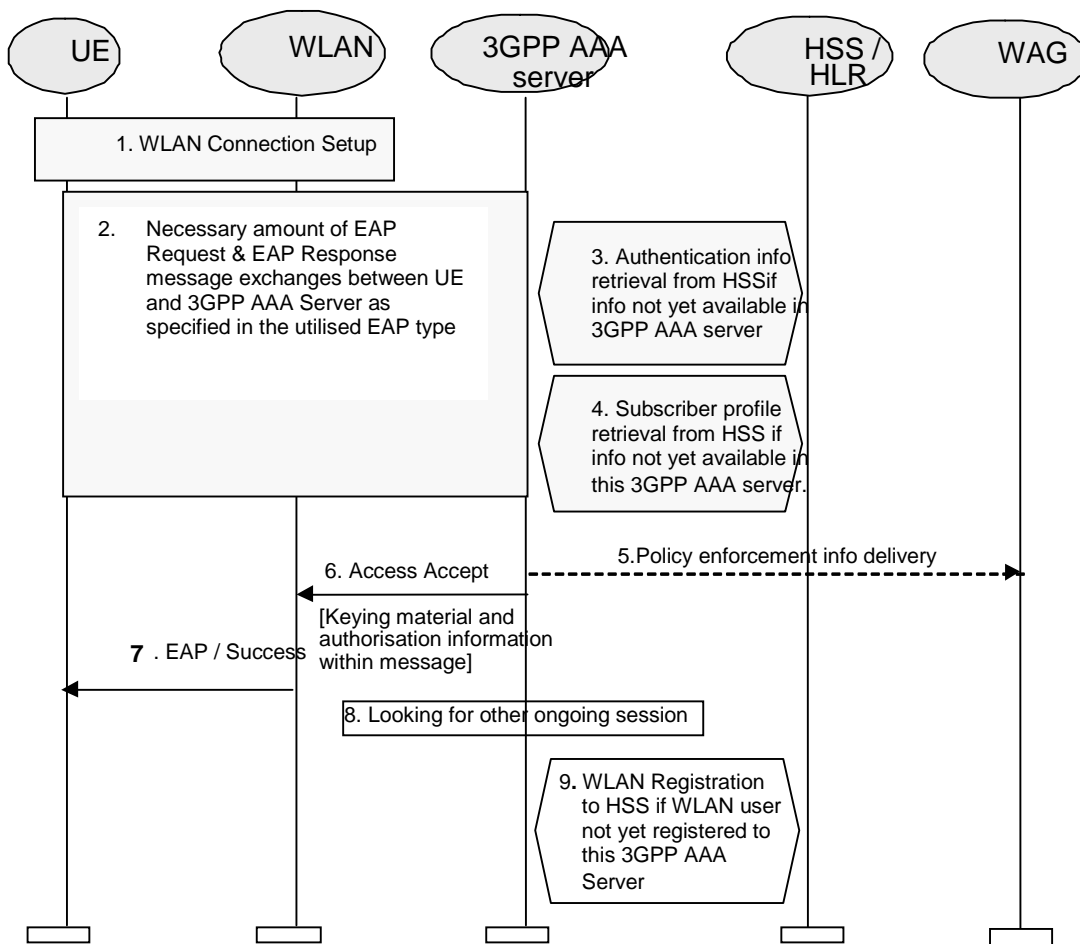


Figure 7.2: Authentication and authorisation procedure

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 already registered to serve for the user. In case the HSS/HLR detects that another 3GPP AAA server has already registered for this user, it shall provide the current 3GPP AAA server with the previously registered AAA server address. The authentication signalling is then routed to the previously registered 3GPP AAA server.
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 (or the 3GPP AAA 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 AAA server shall close the previously established session ("Session abort procedure" over Wa) to avoid multiple WLAN direct IP access sessions.

- 89 3GPP AAA server registers the WLAN users 3GPP AAA 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.

CHANGE REQUEST

23.234 CR 066 rev 1 Current version: 6.1.0

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

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

Title:	Introduction of the WLAN registration within tunnel establishment procedure		
Source:	SA2 (NTT DoCoMo, Siemens, T-Mobile, HP, Samsung, Nokia, Ericsson, Nortel Networks)		
Work item code:	WLAN	Date:	18/08/2004
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: After controversial discussions at SA2#40 an LS was sent to SA1 to clarify

- whether SA1 requires an explicit check for I-WLAN access authorization prior to allowing access to PS services;
- whether there is any requirement to support access authentication methods that are different from those based on the (U)SIM;
- whether there is any requirement to preclude PS service access from other access networks than I-WLAN.

In their reply LS S2-042430 (S1-040716) SA1 answers the following way:

- to the first question: SA1 does require that it shall be possible for an explicit check for I-WLAN access authorization to be performed before accessing 3GPP PS based services;
- to the second question: it is required for the user to be authenticated by the 3GPP system in order to access PS based services;
- to the third question: there is no requirement to preclude access to PS based services from access networks other than I-WLAN.

From answers one and three we understand that the current text in 23.234 chapter 7.9. on the strong correlation between EAP based access authorization and service authorization has to be re-formulated as currently only subscribers authenticated and authorized by the specified 3GPP/WLAN Interworking procedures can access PS services in the PLMN. We propose to change the text in a way that the AAA server shall be able to perform a check for access authorization during service authorization. However, the operator shall have the opportunity to turn this check on and off and to recognize the user's subscription data when performing the check. Thus access to PS services can be permitted based on the user's subscribed services.

And also, if WLAN 3GPP IP Access (scenario 3) is provided independently without WLAN Direct IP Access (scenario 2) authorization, tunnel establishment by the WLAN UE could be the very first time to attach the WLAN-interworking network, which leads the AAA server to register that user to the HSS. In contrast, the cancellation of the WLAN registration is performed when the last tunnel for that UE is disconnected as specified in clause 7.10.3 (extracted for information).

Summary of change: ⓘ It is clarified that the AAA server shall be able to check during tunnel establishment that the WLAN UE is already access authorized and that this check may optionally be based on the user's subscription data. It shall be possible to turn the check on and off based on operator policy. Within the mutual authentication between the WLAN UE and the PDG, it is stated that the 3GPP AAA Server registers the WLAN users to the HSS if the user is not already registered to this 3GPP AAA Server.

Consequences if not approved: ⓘ Inflexible provision of PS based services to users accessing the mobile core network from alternative access systems or access systems using various access authentication and authorization methods, e.g. WLAN hotspots with portal page authentication. No registration is performed if WLAN 3GPP IP Access is provided independently.

Clauses affected: ⓘ 7.9

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

Other comments: ⓘ This is merged with S2-042494

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.

***** 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

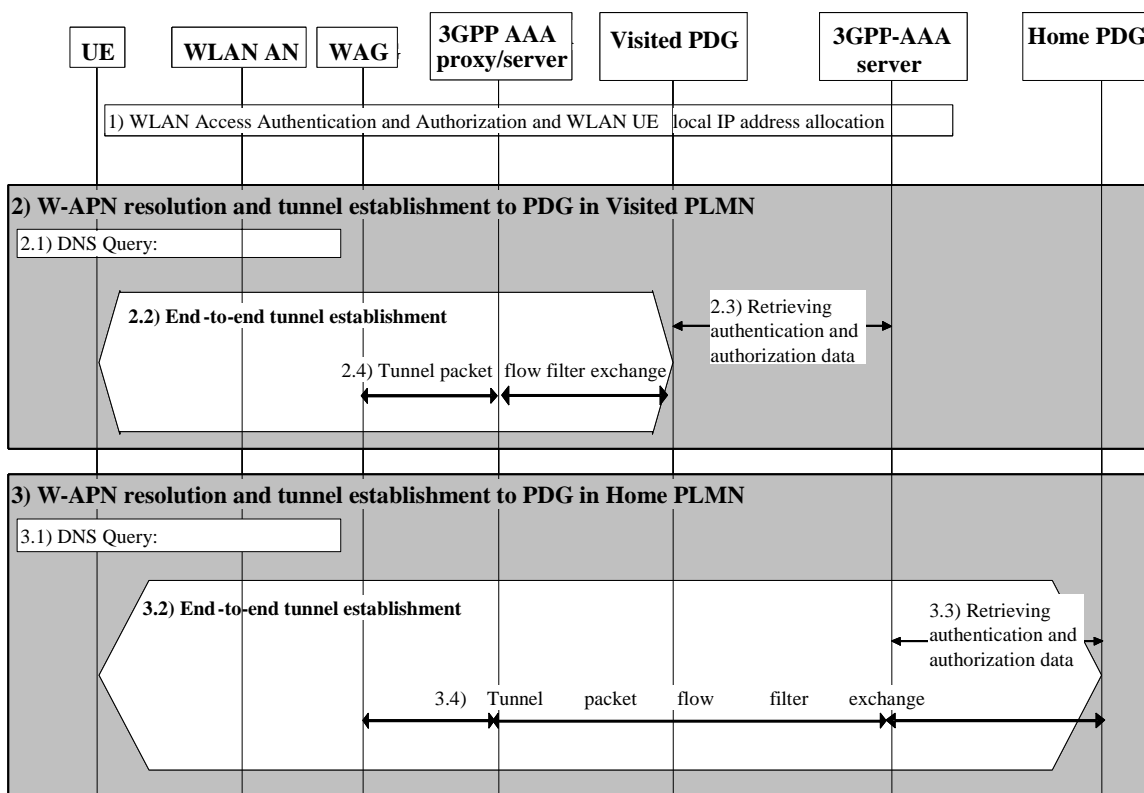


Figure 7.10: Example message flow to WLAN UE-Initiated tunnel establishment

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 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 ~~verifies~~ [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, then the tunnel establishment shall be rejected by the PDG.
- 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 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 ~~verifies~~ [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, then the tunnel establishment shall be rejected by the Home PDG.
- 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.

***** FOR INFORMATION *****

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 (step2-4),

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.

CHANGE REQUEST

⌘ 23.234 CR 068 ⌘ rev - ⌘ Current version: 6.1.0 ⌘

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

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

Title:	⌘ Editorial update of already agreed change in figure 6.2b		
Source:	⌘ SA2 (Ericsson)		
Work item code:	⌘ WLAN	Date:	⌘ 11/08/2004
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:	⌘ Editorial update of already agreed change in figure 6.2b		
Summary of change:	⌘ At SA2#39 CR 30r2 (S2-041645) was approved, which was a merge of CR 2 (S2-041250) and CR 18 (S2-041224). CR 18 clarifies that Wm reference point is between AAA proxy and PDG in the visited network, and updates figure 6.2 b accordingly. However, the same figure was also updated at SA2#40, and the change from CR 18 was lost. Hence, this CR corrects that mistake.		
Consequences if not approved:	⌘ Agreed CR 18 is not implemented correctly.		

Clauses affected:	⌘ 6.1.2										
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> <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:

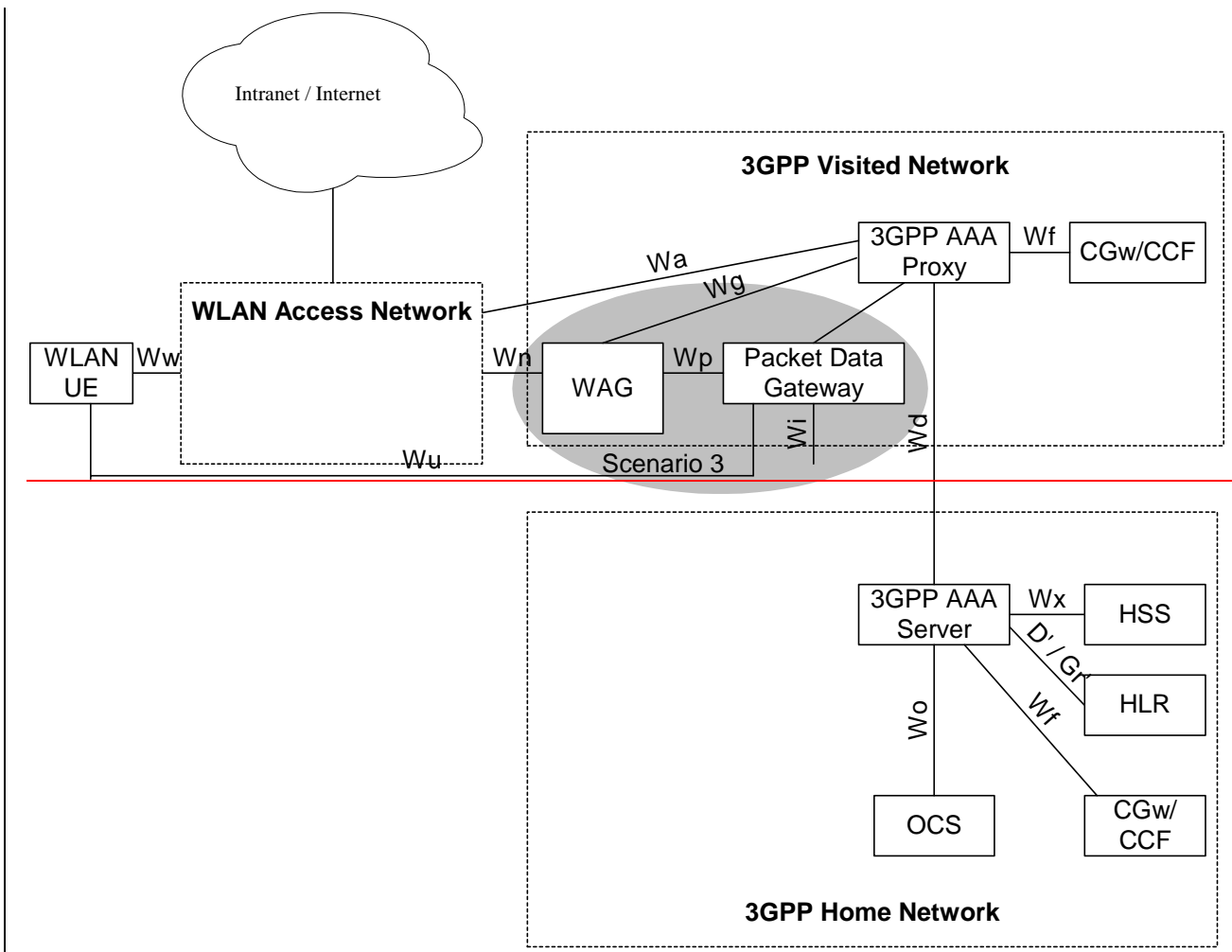
Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

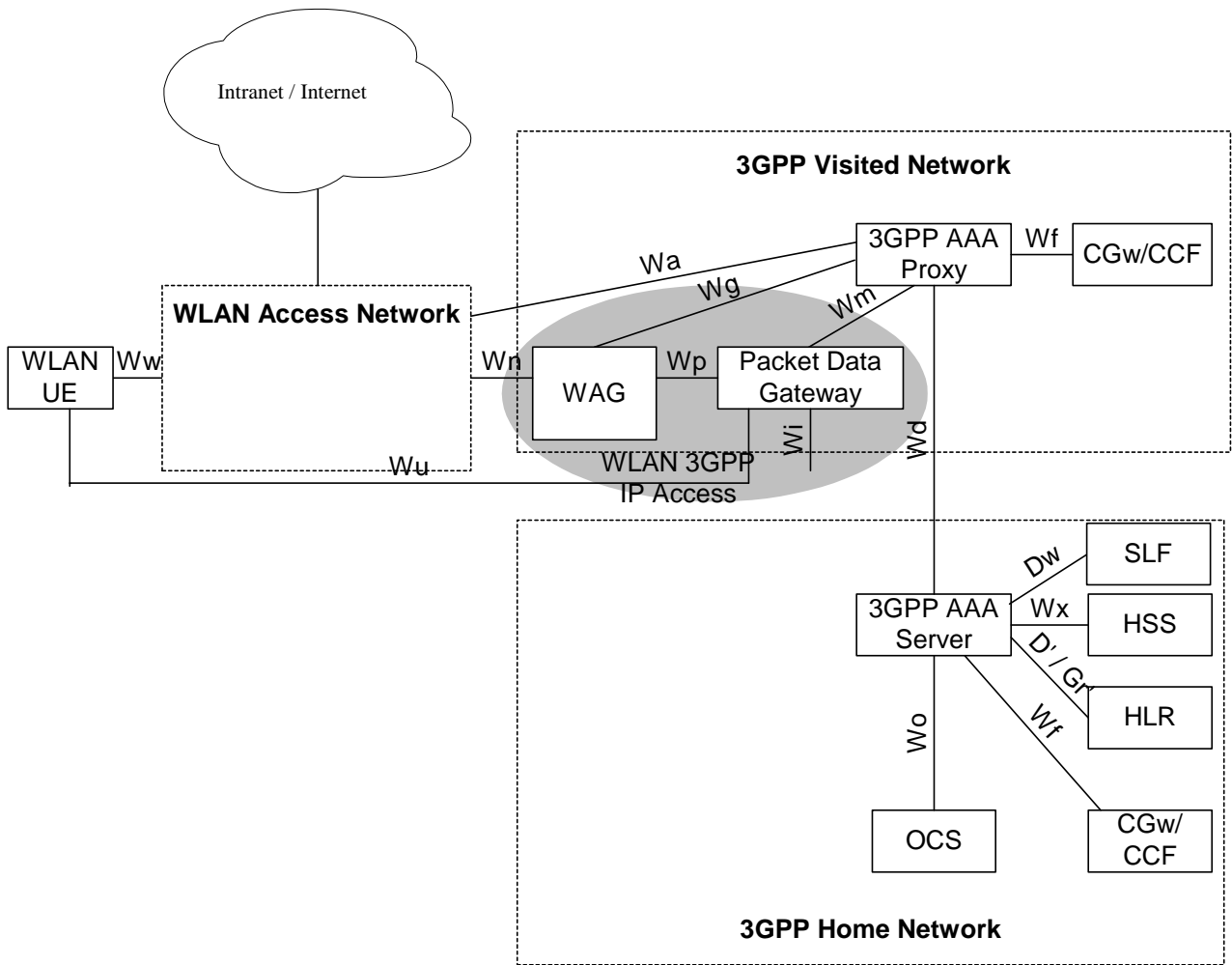
- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") 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.

****** First change ******





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

**** End of first change ****

CHANGE REQUEST

⌘ 23.234 CR 069 ⌘ rev - ⌘ Current version: 6.1.0 ⌘

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

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

Title:	⌘ Removal of issue chapter in Annex F.		
Source:	⌘ SA2 (Ericsson)		
Work item code:	⌘ WLAN	Date:	⌘ 11/08/2004
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: 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:	⌘ Chapter F.4 lists issues to investigate for the GnI reference point. However, the only issue listed in 23.234v6.1.0, i.e. MSISDN for WLAN UE's, is now resolved and MSISDN is included in the User Profile. Also, the editors note in the chapter indicates that the section is expected to be resolved once the issues are resolved.
Summary of change:	⌘ Removal of section F.4.
Consequences if not approved:	⌘ Inconsistent specification.

Clauses affected:	⌘ F.4						
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 change ****

F.4 ~~Issues to investigate for Gn' reference point~~[void](#)

~~Editor's note: This section is expected to be removed once the investigation on the issues listed here has been concluded.~~

~~Some issues that needs to be investigated have been identified:~~

~~—GTP requires MSISDN. MSISDN might be a requirement for WLAN for charging or other reasons, but if it doesn't this is an issue.~~

**** End of first change ****

CHANGE REQUEST

⌘ **23.234** CR **070** ⌘ rev **1** ⌘ Current version: **6.1.0** ⌘

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

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

Title:	⌘ Clarification of NSAPI in Annex F.		
Source:	⌘ SA2 (Ericsson, NTT DoCoMo)		
Work item code:	⌘ WLAN	Date:	⌘ 11/08/2004
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:	⌘ The approved solution for allocation of the NSAPI value in the TTG is described in chapter F.5. However, some text about the NSAPI also remains in chapter F.3.0 that may lead to confusion.
Summary of change:	⌘ In chapter F.3.0 refer to F.5 for allocation of the NSAPI. Further, the editors note in chapter F.3.1 is removed.
Consequences if not approved:	⌘ The current text in the specification is unclear, and may create confusion.

Clauses affected:	⌘ F.3.0, F.3.1										
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.

**** First change ****

F.3.0 General

A minimum set of interworking procedures over the Gn reference point would include the following messages:

- Create PDP Context Request / Response;
- Update PDP Context Request / Response;
- Delete PDP Context Request / Response;
- Error Indication;
- Version Not Supported;
- GTP payload forwarding (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 an 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.

~~To support WLAN UEs, which may use GPRS and WLAN access simultaneously, the NSAPI value to use by TTG need either be a value reserved for TTG or an NSAPI value passed from WLAN UE to TTG. In Existing GPRS, the NSAPI is assigned in the UE and is used to distinguish between a UE's PDP contexts. The NSAPI is an integer value between 5 and 15. The NSAPI value to be provided over the Gn reference point is allocated in the TTG, see subclause F.5.~~

**** End of first change ****

**** Second change ****

F.3.1 Interworking procedure over GnI - Tunnel establishment procedure

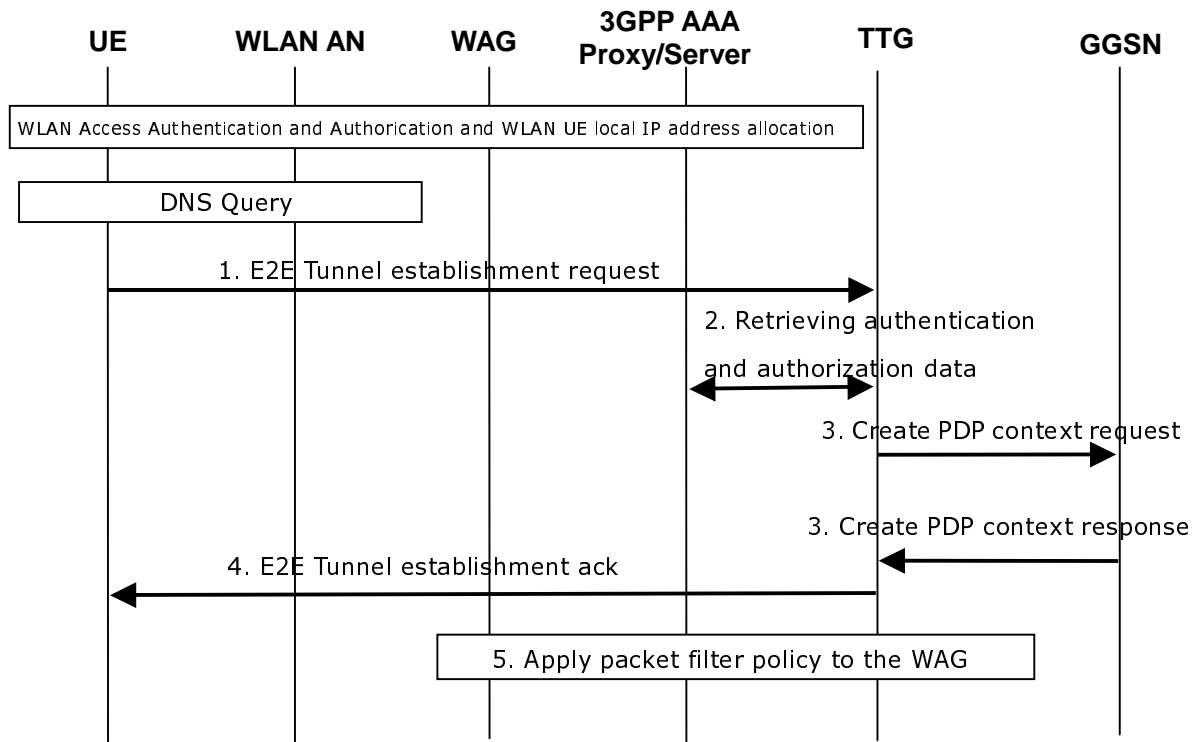


Figure F.3.1: Tunnel establishment procedure

- 1) The UE performs a DNS query to resolve the W-APN and sends E2E tunnel establishment request (W-APN, user identity) to the TTG (see subclause 7.9).
- 2) The TTG contacts the 3GPP AAA Server in the HPLMN possibly via the AAA proxy for authorization and authentication of the WLAN UE (see subclause 7.9). Additionally, the TTG retrieves the IMSI, MSISDN, and serving network identity from the AAA server.
- 3) The TTG performs PDP Context Activation procedure towards the GGSN by using Create PDP Context Request message and Create PDP Context Response message (see TS 23.060 [7]).
- 4) The TTG returns E2E tunnel establishment acknowledgement (remote IP address) to the WLAN UE.
- 5) The TTG provides filtering information to the WAG (see subclause 7.9).

~~Editor's Note : it is ffs how the NSAPI value is allocated when the tunnel establishment procedure over GnI is performed.~~

****** End of second change ******

CR-Form-v7

CHANGE REQUEST

23.234 CR **071** rev **1** Current version: **6.1.0**

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

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

Title:	CR on IMS over WLAN		
Source:	SA2 (Samsung)		
Work item code:	WLAN	Date:	18/08/04
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:	The current text about SBLP functions in the PDG is not in line with the conclusion made in the SA2 #38.
Summary of change:	Remove the text about SBLP features in the PDG. Add an informative annex about possible methods of supporting IMS over WLAN.
Consequences if not approved:	Mainly due to lack of time remained for Release 6, completing standardization of PS services over I-WLAN (including IMS) will be highly risked.

Clauses affected:	5.7, 6.2.6, a new Annex G										
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;">X</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> </table>	Y	N	X	X	X	X	X	X	Other core specifications	
Y	N										
X	X										
X	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.

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

5.7 IP Connectivity for WLAN 3GPP IP Access

Ö.

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.

***** **NEXT 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.

~~— Performs the functions of Service-based Local Policy Enforcement Point (controls the quality of service that is provided to a set of IP flow as defined by a packet classifier, control admission based on policy that is applied to the IP bearers associated with the flow, and configuration of the packet handling and "gating" functionality in the user plane.)~~

~~— Communicates with Policy Decision Function (PDF) to allow service-based local policy and QoS inter-working information to be "pushed" by the PDF or to be requested by the PDG. This communication also provides information to support the following functions in the PDG:~~

- ~~— Control of Diffserv inter-working;~~
- ~~— Control of RSVP admission control and inter-working;~~
- ~~— Control of "gating" function in PDG;~~
- ~~— WLAN bearer authorization;~~
- ~~— QoS charging related function.~~

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

***** 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 TS23.125 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 is an optional feature in this version of the TS.

4. Using GGSN's SBLP/FBC functions

- Pros: When GN1 interface is used, the SBLP/FBC functions and related interfaces can be used.
- Cons: It can be used only in the tunnel extension architecture.
- It is is an optional feature in this version of the TS.

5. Not using any policing mechanism

- Pros: No more work is required.
- Cons: IMS over I-WLAN is not able to support policy control and bearer level charging.
- It is a main working assumption in this version of TS.

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

CR-Form-v7

CHANGE REQUEST

23.234 CR **072** rev **3** Current version: **6.1.0**

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

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

Title:	Correction to temporary identity usage and reference		
Source:	SA2 (Samsung)		
Work item code:	WLAN	Date:	18/08/04
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:	The subclause 5.3.2 about NAI refers to only one kind of temporary identity. It has to be clarified the difference between the Pseudonym and the Fast re-authentication identity. Also in 5.3.4 which describes roaming NAI there is a redundant sentence referring to a wrong subclause.
Summary of change:	Clarification of temporary identities and their usages. Removing redundant reference.
Consequences if not approved:	Misinterpretation that only type of temporary identity is being referred to for NAI usage. Wrong reference may lead to confusion.

Clauses affected:	5.3.1, 5.3.2, 5.3.4										
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> 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"/>		
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.

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

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~~ User Identity, 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. ~~a temporary identity in the username part of the NAI can be used.~~ The use of the Pseudonym username ~~a temporary identifier~~ is necessary to replace the ~~the Permanent username derived from~~ IMSI in radio transmissions, ~~as so that~~ it protects the user against tracing from unauthorized access networks. ~~As a working assumption, it is considered in this version of the TS that temporary identifiers are allocated in the 3GPP AAA Server. The format and the procedure for deriving the temporary identity are defined in TS 33.234 [14].~~

The Fast re-authentication username is used in ~~For~~ 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 EAP-AKA [22] Internet-Drafts ~~as its NAI user identity. The format and the procedure for deriving the re-authentication identity are defined in TS 33.234 [14].~~

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].

***** SECOND MODIFIED SECTION *****

5.3.4 ~~Roaming~~ NAI decoration for roaming

A roaming NAI is constructed when the WLAN UE authenticates through a VPLMN. The WLAN UE shall indicate in the NAI both the user's HPLMN and the chosen VPLMN, based on their MCC and MNC.

~~The realm portion of the roaming NAI shall be constructed according to Section 5.3.2 based on the chosen Visited Network MCC and MNC.~~

The details on Roaming NAI construction are specified in 3GPP TS 23.003 [5].

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

CR-Form-v7			
CHANGE REQUEST			
23.234	CR	073	rev 2 Current version: 6.1.0

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

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

Title:	Correction to PDG Selection Mechanism		
Source:	SA2 (Samsung)		
Work item code:	WLAN	Date:	18/08/04
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:	Clarification of PDG selection requirement based on the agreed PDG selection mechanism
Summary of change:	Clarification of PDG selection requirement.
Consequences if not approved:	Vague requirement can cause confusion.

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;">X</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> </table>	Y	N	X	X	X	X	X	X	Other core specifications	
Y	N										
X	X										
X	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.

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

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 ~~is~~ 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.

******* SECOND MODIFIED SECTION *******

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.

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

CR-Form-v7

CHANGE REQUEST

23.234 CR **075** rev **3** Current version: **6.1.0**

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

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

Title:	Correction to W-APN authorization and PDG redirection Mechanism		
Source:	SA2 (Samsung)		
Work item code:	WLAN	Date:	21/08/04
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:	The PDG after receiving the Tunnel Establishment Request has to forward the W-APN to the AAA Server for service authorisation. This is true for VPLMN or HPLMN case. If AAA Server cannot allow the WLAN UE to take the service for that W-APN it shall send a Reject message to the PDG, which carries it to the WLAN UE. If AAA Server wants to redirect the message, it shall provide the alternate PDG IP address to the requesting PDG which shall then be carried to the WLAN UE through redirect message from PDG.
Summary of change:	AAA Server behaviour incase of W-APN authorisation and redirection.
Consequences if not approved:	The current text doesn't exactly specify how the PDG comes to know about the alternate PDG IP address to be redirected. Also it does not specify how the W-APN is being used for service authorisation.

Clauses affected:	7.9, 7.9.1						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="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 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

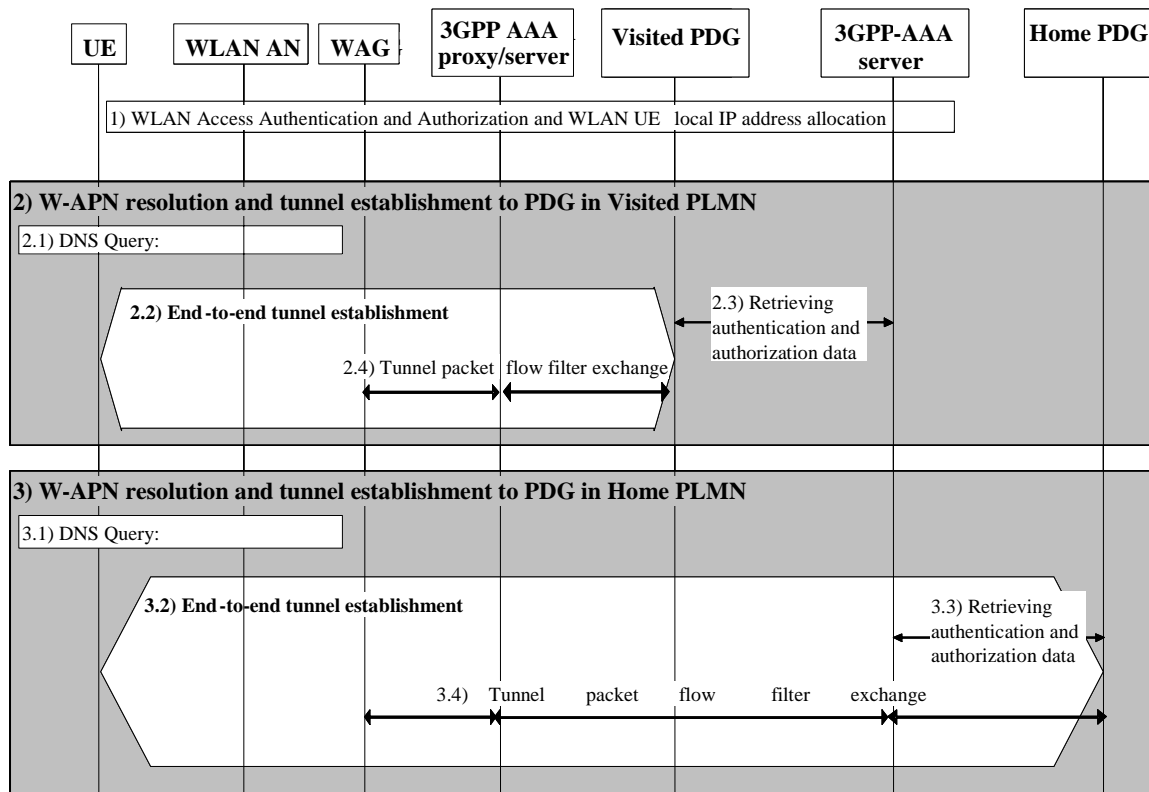


Figure 7.10: Example message flow to WLAN UE-Initiated tunnel establishment

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.

The 3GPP AAA Server verifies that the user requesting the tunnel establishment has been already successfully WLAN Access Authorized. If not, 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.

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. The 3GPP AAA Server verifies that the user requesting the tunnel establishment has been already WLAN Access Authorized. If not, 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.

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.

***** SECOND MODIFIED SECTION *****

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 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.

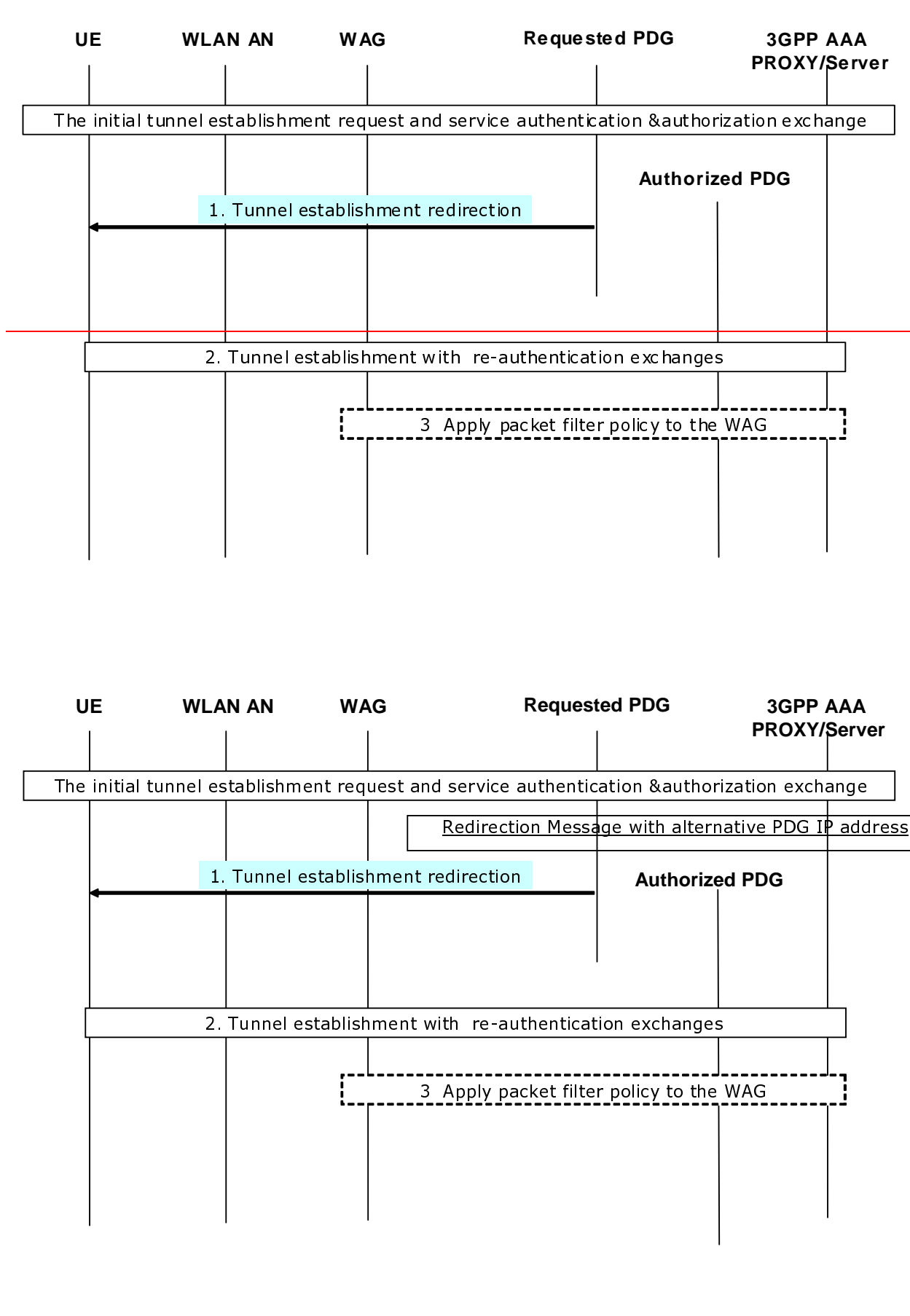


Figure 7.11: Message flow of the tunnel establishment with redirection

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

3GPP TSG-SA2 Meeting #41
 Montreal, Canada 16th ñ 20th August 2004

Tdoc **S2-042934**

CR-Form-v7			
CHANGE REQUEST			
23.234	CR	76	rev 3 Current version: 6.1.0

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

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

Title:	WLAN User Profile revision		
Source:	SA2 (Telef�nica M�viles Espa�a, T-Mobile)		
Work item code:	WLAN	Date:	20/08/2004
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:	The purpose of the CR is to add new subscriber data to the WLAN user profile.		
Summary of change:	The CR proposes to complete the WLAN user profile including some relevant data similar to the ones used in GPRS/UMTS. Other parameters have been modified in order to add more functionality. The changes proposed are mainly oriented to the WLAN 3GPP IP Access described in the TS.		
Consequences if not approved:	The user profile defined in the current TS will not cover all the functionalities currently offered by the operators.		

Clauses affected:	6.3.2, 6.5										
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;">X</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> </table>	Y	N	X	X	X	X	X	X	Other core specifications Test specifications O&M Specifications	
Y	N										
X	X										
X	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.

First modified section

6.3.2 Wx reference point

This reference point is located between 3GPP AAA Server and HSS. The prime purpose of the protocol(s) crossing this reference point is communication between WLAN AAA infrastructure and HSS.

The functionality of the reference point is to enable:

- Retrieval of authentication vectors, e.g. for USIM authentication, from HSS.
- Retrieval of WLAN access-related subscriber information (profile) from HSS
- Registration of the 3GPP AAA Server of an authorised (for WLAN Access) WLAN user in the HSS.
- Indication of change of subscriber profile within HSS (e.g. indication for the purpose of service termination).
- Purge procedure between the 3GPP AAA server and the HSS.
- Retrieval of online charging / offline charging function addresses from HSS.
- Fault recovery procedure between the HSS and the 3GPP AAA Server.
- Retrieval of service related information (e.g. W-APNs that may be selected by the WLAN UE [and the data defined for the W-APNs in the WLAN UE's profile](#)) including an indication of whether the VPLMN is allowed to provide this service.

Second 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 AAA 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 (*optional*)

User identification, for example used for charging purposes

3. Operator determined barring of 3GPP-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](#)~~access allowed~~" flag 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 mode (pre-paid, post-paid, both)~~ [Charging Characteristics](#) and accounting server identifier(s) ~~for every charging mode~~

The [Subscribed Charging Characteristics](#) will implicitly define the ~~C~~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. ~~Each W-APN shall have a flag indicating whether access is allowed in visited PLMNs or in the home PLMN.~~

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.

- o 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., 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 ñ 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-WLAN Interworking in an WLAN AN that have no direct connection to the home PLMN.

3GPP TSG-SA2 Meeting #41
 Montreal, Canada 16th ñ 20th August 2004

Tdoc **S2-042930**

CR-Form-v7			
CHANGE REQUEST			
23.234	CR	077	rev 3
			Current version: 6.1.0

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

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

Title:	Charging related data for 3GPP PS based services (WLAN 3GPP IP Access)		
Source:	SA2 (TelefÙnica MÙviles EspaÒa,T-Mobile)		
Work item code:	WLAN	Date:	20/08/2004
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:	The subscribed/W-APN Charging Characteristics parameters are defined in the WLAN UE's profile. However the TS does not describe how these parameters are sent to the PDG for the WLAN 3GPP IP Access.
Summary of change:	The CR describes the procedures in the 3GPP AAA server to send the charging parameters to the PDG for 3GPP PS based services (WLAN 3GPP IP Access).
Consequences if not approved:	The TS will not cover the provision of charging parameters to the PDG for 3GPP PS based services (WLAN 3GPP IP Access).

Clauses affected:	2, 5.11, 6.3.10, 7.9										
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;">X</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> </table>	Y	N	X	X	X	X	X	X	Other core specifications	
	Y	N									
	X	X									
	X	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.

First 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 networksó 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.
- [21] IEEE Std 802.11-1999, Local and metropolitan area networksó Specific requirementsó 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-11 (October 2003).
- [23] IETF Internet-Draft: "EAP SIM Authentication" draft-haverinen-pppext-eap-sim-12 (October 2003).
- [24] 3GPP TS 23.228: " IP Multimedia Subsystem (IMS); Stage 2".
- [25] [3GPP TS 32.252: "Telecommunication management; Charging management; Wireless Local Area Network \(WLAN\) charging"](#).

Second 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 \[25\].](#)

Third 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 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.
- 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.

Fourth 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

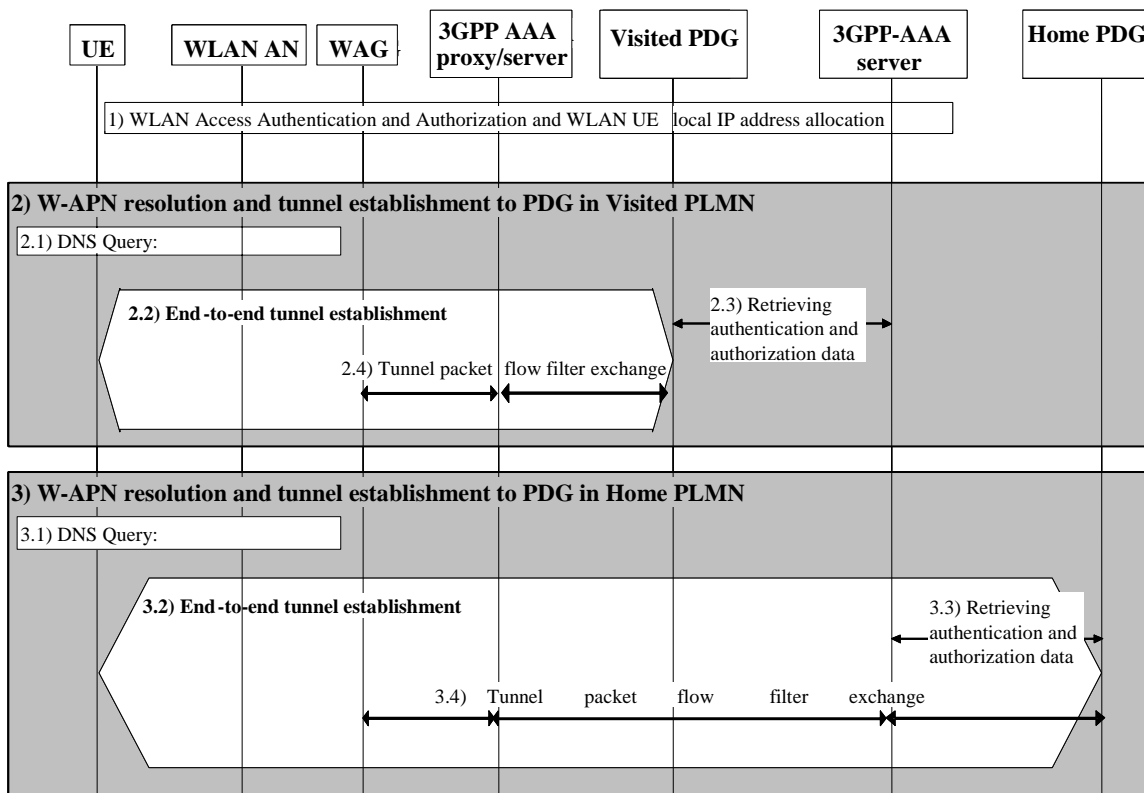


Figure 7.10: Example message flow to WLAN UE-Initiated tunnel establishment

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 and to retrieve the information required for the mutual authentication part of the tunnel establishment.

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, 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 and to retrieve the information required for the mutual authentication part of tunnel establishment. 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, then the tunnel establishment shall be rejected by the Home PDG. [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.

3GPP TSG-SA2 Meeting #41
Montreal, Canada 16th - 20st August 2004

Tdoc **S2-042931**

CR-Form-v7

CHANGE REQUEST

23.234 CR **78** rev **3** Current version: **6.1.0**

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

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

Title:	Static Remote IP address allocation	
Source:	SA2 (Telefónica MÓviles España)	
Work item code:	WLAN	Date: 20/08/2004
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: The changes in the WLAN UE's profile allow the Home operator to assign a WLAN UE a Static Remote IP address. The static remote IP address allocation method is not defined in the TS.

Summary of change: The CR defines the Static Remote IP address allocation method.

Consequences if not approved: The TS will not cover the static IP remote address allocation defined in the WLAN-UE profile.

Clauses affected: 5.10, 6.2.3, 6.3.10, 7.9

Other specs affected:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications
	<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

5.10 IP address allocation for the WLAN UE

5.10.1 General

When using WLAN Direct IP Access, a WLAN UE needs to use its local IP address only. When using WLAN 3GPP IP Access, a WLAN UE shall use two IP addresses; its local IP address and remote IP address.

A WLAN UE's local IP address identifies the WLAN UE in the WLAN AN. In systems supporting only WLAN Direct IP Access, the WLAN UE's local IP address is assigned by the WLAN AN; in a WLAN 3GPP IP Access enabled system, it can be assigned by a WLAN or by a PLMN (a VPLMN in roaming case and a HPLMN in non-roaming case). For the WLAN-assigned local IP address, which belongs to the address space of WLAN AN, there is no additional requirement on the WLAN. WLAN UE's local IP address allocation by the PLMN is for further study.

When using WLAN 3GPP IP Access, a WLAN UE's remote IP address identifies the WLAN UE in the network that the WLAN UE is accessing for the 3G PS service. It shall be used for the inner packet of the WLAN UE-initiated tunnel. It can be assigned by HPLMN, VPLMN or an external IP network. [The remote IP address can be statically or dynamically assigned.](#) The only case where VPLMN assigns the remote IP address for the WLAN UE is when the WLAN UE-initiated tunnel terminates at the VPLMN's PDG. When the WLAN UE's remote IP address is allocated by the external IP network, the PDG is required to have an interface with an address allocation server, such as AAA or DHCP, belonging to the external IP network. For the WLAN UE's remote IP address, IPv4 addresses shall be supported. When the WLAN UE accesses 3G PS based services using an IPv6 network such as IMS services, IPv6 addresses shall be supported for the WLAN UE's remote IP address. To avoid any clashes between addresses used in WLAN AN and PLMN and to enable correct routing of packets sent out by the WLAN UE the PLMN operator should allocate public addresses to network nodes, which are addressed by WLAN UEs.

When a WLAN UE accesses several 3G PS based services with different W-APNs simultaneously, the WLAN UE can get several remote IP addresses. There may be several WLAN UE-initiated tunnels for the services.

5.10.2 Static and Dynamic Remote IP Address

Remote IP address can be allocated to a WLAN UE in four different ways:

- The HPLMN operator assigns a Remote IP address permanently to the WLAN UE (static remote IP address).
- The HPLMN operator assigns a Remote IP address to the WLAN UE when the tunnel is established to the PDG in the home network (dynamic HPLMN remote IP address).
- The VPLMN operator assigns a Remote IP address to the WLAN UE when the tunnel is established to the PDG in the visited network (dynamic VPLMN remote IP address).
- The external IP network operator assigns a permanent or dynamic Remote IP address to the WLAN UE (external Remote IP address allocation).

It is the HPLMN operator that defines in the subscription whether static IP address allocation is used. When static IP address allocation is used, a WLAN UE either can include its static IP address in the tunnel setup request message, or indicate in the tunnel setup request message that the network should configure the static IP address of the WLAN UE or the network simply provides the static address to the WLAN UE.

Second modified section

6.2.3 3GPP AAA Server

The 3GPP AAA server is located within the 3GPP network. 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 to the HPLMN CCF/CGw.

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.

Third 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.](#)
- 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.
- 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.

Fifth 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

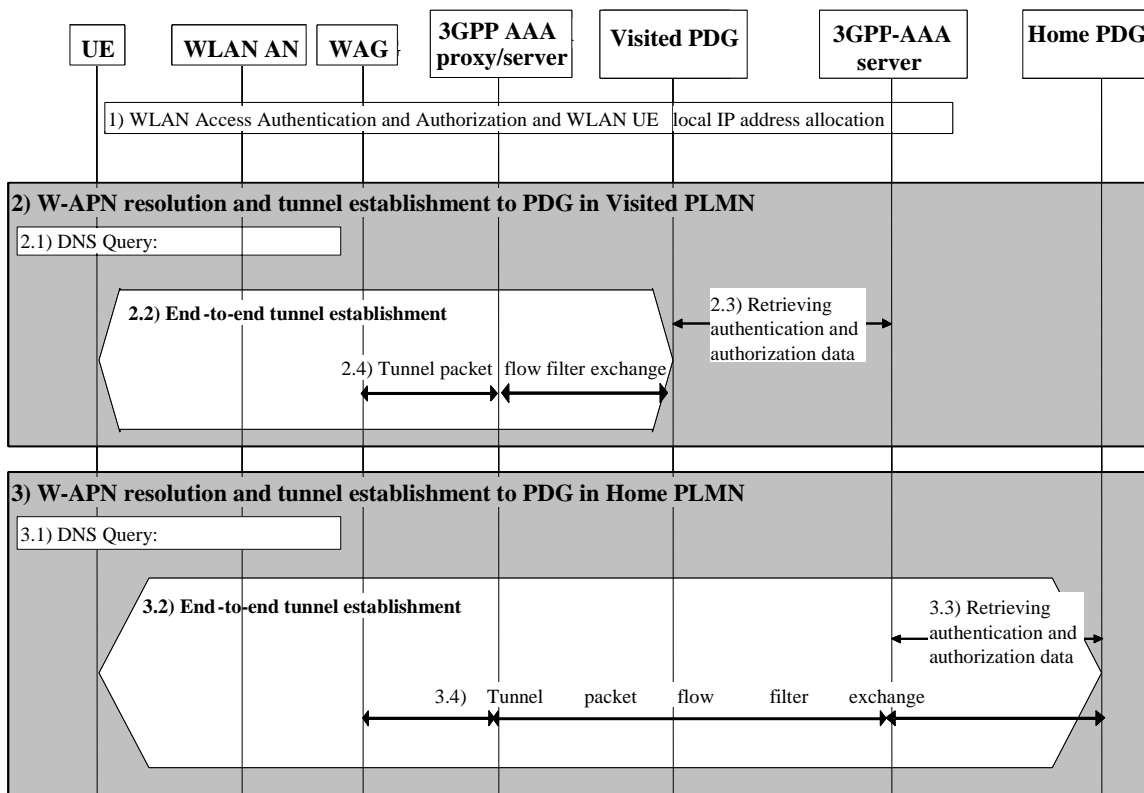


Figure 7.10: Example message flow to WLAN UE-Initiated tunnel establishment

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 and to retrieve the information required for the mutual authentication part of the tunnel establishment.
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, then the tunnel establishment shall be rejected by the PDG.

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 and to retrieve the information required for the mutual authentication part of tunnel establishment. 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, 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.](#)
 - 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.

CR-Form-v7

CHANGE REQUEST

23.234 CR **081** rev **2** Current version: **6.1.0**

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

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

Title:	Storage of the AAA server IP address in HSS/HLR		
Source:	SA2 (Samsung)		
Work item code:	WLAN	Date:	19/08/04
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:	The 3GPP AAA Server address to which the WLAN UE is currently attached must be stored in HSS. This is necessary to know where the WLAN UE is currently located and also to check for any authorized sessions that are going on when a new authentication request reaches the HSS for the same WLAN UE via another 3GPP AAA Server.
Summary of change:	Add sentence of the 3GPP AAA server IP address storage in HSS.
Consequences if not approved:	This would make any other network node quereing HSS with no information about which 3GPP AAA Server the UE is currently attached.

Clauses affected:	6.2.4				
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 checked="" type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications <input checked="" type="checkbox"/> Test specifications <input checked="" type="checkbox"/> O&M Specifications <input checked="" type="checkbox"/>	Y	N	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Y	N				
<input checked="" 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 MODIFIED SECTION *********6.2.4 HLR/HSS**

The HLR/HSS located within the 3GPP subscriber's home network is the entity containing authentication and subscription data required for the 3GPP subscriber to access the WLAN interworking service.

The HSS also provides access to the WLAN UE's WLAN-attach status for other entities, e.g. answers or relays the WLAN-attach status query from other entities ~~(which are out of the scope of this TS)~~. To this end, the HSS shall store the IP address of the 3GPP AAA server to which the WLAN UE is registered.

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