3GPP TSG CT Plenary Meeting #28 **CP-050196**
1st – 3rd June 2005 Quebec, Canada.

Source: TSG CT WG4

Title: Corrections on WLAN

Agenda item: 9.17

Document for: APPROVAL

Doc-2nd-Level	Spec	CR #	Rev	Rel	Tdoc Title	CAT	C_Version
C4-050759	29.234	049	1	Rel-6	Addition of missing functionality to Wa Interface RADIUS profile	F	6.2.0
C4-050760	29.234	050	1	Rel-6	Addition of missing functionality to Wa Interface Diameter profile	F	6.2.0
C4-050866	29.234	051	2	Rel-6	Mandating RFC 3576 in WLAN-IW	F	6.2.0
C4-050876	29.230	051	1	Rel-6	Addition of Maximum-Number-Accesses AVP	F	6.3.0
C4-050578	29.234	052		Rel-6	Removal of reference to User Data AVP on the Wm interface	F	6.2.0
C4-050579	29.234	053		Rel-6	Clean up of 29.234	F	6.2.0
C4-050761	29.234	054	1	Rel-6	Visited Network Identifier on the Wx interface	F	6.2.0
C4-050581	29.234	055		Rel-6	Reference to W-APN definition in 23.003	F	6.2.0
C4-050762	29.234	056	1	Rel-6	Clarifications on Wa and Wd RADIUS profiles	F	6.2.0
C4-050871	29.234	058	2	Rel-6	WAG address resolution on Wg interface	F	6.2.0
C4-050766	29.234	060	2	Rel-6	Missing functionality on Wa, Wm interfaces	B	6.2.0
C4-050864	29.234	061	2	Rel-6	Pr Interface for Presence via I-WLAN	B	6.2.0
C4-050874	29.234	062	2	Rel-6	Limit on the number of sessions in WLAN 3GPP IP Access	F	6.2.0
C4-050873	23.008	145	2	Rel-6	Corrections on Serving WAG	F	6.5.0
C4-050765	23.008	146	1	Rel-6	Corrections on WLAN UE Remote IP Address	F	6.5.0
C4-050875	23.008	151	1	Rel-6	Limit on the number of sessions in WLAN 3GPP IP Access	F	6.5.0

3GPP TSG CN WG4 Meeting #27 **N4-050578**
Cancun, Mexico, 25th – 29th April 2005

CR-Form-v7

CHANGE REQUEST

⌘ **29.234** **CR** **052** ⌘ **rev** **-** ⌘ Current version: **6.2.0** ⌘

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

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

Title:	⌘	Removal of Reference to User Data AVP on the Wm interface
Source:	⌘	Nokia
Work item code:	⌘	WLAN-IW
Date:	⌘	14/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*

Reason for change:	⌘	Section 8.3.2.1 states that 3GPP AAA Server shall download to PDG the APN-User-Data. This is inconsistent with the detailed lists of parameters sent in the AA-Response message in Table 8.3.2.2
Summary of change:	⌘	Removal of the APN-User-Data AVP from section 8.3.2.1 description. Replacement by general text describing the information elements actually sent
Consequences if not approved:	⌘	Incorrect interface description

Clauses affected:	⌘	8.3.2.1

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

Other comments:	⌘	

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

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

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

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

**** Start of change #1 ****

8.3.2.1 3GPP AAA Server Detailed Behaviour

The 3GPP AAA Server shall, in the following order (if there is an error in any of the steps, the 3GPP AAA Server shall stop processing and return the corresponding error code):

1) Check that the user exists in the 3GPP AAA Server. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2) Check the Session-Request-Type AVP:

- If Request type is set to AUTHORIZATION REQUEST, it indicates that the WLAN-UE does not have a tunnel active to the particular W-APN at the PDG and is requesting authorization for such a W-APN.

  - The 3GPP AAA Server shall check that the user has subscription for the W-APN requested. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_NO_APN_SUBSCRIPTON.

  - The 3GPP AAA Server shall check whether the user has access to that W-APN, otherwise Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED.

  - If the user is roaming (indicated by the presence of the Visited-Network-Identifier AVP), the 3GPP AAA Server shall check if the user is allowed to access the W-APN from a VPLMN. This information is obtained from the HSS within the APN-Authorization AVP. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR _ROAMING_NOT_ALLOWED.

  - The 3GPP AAA Server shall store the PDG IP address.

  - The 3GPP AAA Server shall download user data relevant to the W-APN, ~~APN-User-Data-AVP and the~~ e.g. WLAN UE remote IP address if present and the charging information as received from the HSS. The Result-Code shall be set to DIAMETER_SUCCESS.

- If Request type is set to ROUTING POLICY, it indicates that the WLAN-UE already has an active tunnel to the given PDG and is informing the 3GPP AAA Server of the routing policy for the tunnel. The 3GPP AAA Server shall store the Routing-Policy AVP and use Wg procedures to install this policy at the WAG. If this is successful, 3GPP AAA Server shall set Result-Code AVP to DIAMETER_SUCCESS in the AAA message. If not, Result-Code shall be set to DIAMETER_UNABLE_TO COMPLY.

Exceptions to the cases specified here shall be treated by 3GPP AAA Server as error situations, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY. No authorization information shall be returned.

8.3.2.2 AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy is required to handle roaming cases in which the PDG is in the VPLMN. On this interface, it may act to limit policy enforcement by modifying messages. It shall therefore maintain session state. The 3GPP AAA Proxy shall, in the following order (if there is an error in any of the steps, the 3GPP AAA Proxy shall stop processing and return the corresponding error code).

Check the Request Type AVP:

1) If Request type indicates AUTHORIZATION REQUEST, it indicates that the WLAN-UE does not have a tunnel active to the particular APN at the PDG and is requesting authorization for such an APN.

   a) The 3GPP AAA Proxy shall check locally configured information whether users from the HPLMN are allowed to access to the W-APN requested from this (V)PLMN. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR _ROAMING_NOT_ALLOWED and the AA-A message sent to the PDG. In all other cases, the message shall be forwarded transparently to the 3GPP AAA Server.

2) If Request-Type indicates ROUTING POLICY:

   a) This indicates that the WLAN-UE already has an active tunnel to the given PDG and is informing the 3GPP AAA Server of the routing policy for the tunnel. The 3GPP AAA Proxy shall store the Routing-Policy AVP and use Wg procedures to download the policy to the WAG. If this is successful, 3GPP AAA Server shall set Result Code to "Success" and send the AAR reply. If not, Result Code shall be set to DIAMETER_UNABLE_TO COMPLY.

Exceptions to the cases specified here shall be treated by 3GPP AAA Proxy as error situations, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY and AA-A message sent to the PDG.

**** End of change #1 ****

3GPP TSG CN WG4 Meeting #27 **N4-050579**
Cancun, Mexico, 25th – 29th April 2005

CR-Form-v7

CHANGE REQUEST

⌘ **29.234** **CR** **053** ⌘ **rev** **-** ⌘ Current version: **6.2.0** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Clean up of 29.234
Source:	⌘	Nokia
Work item code:	⌘	WLAN-IW
Date:	⌘	14/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Editorial
Summary of change:	⌘	Editorial modifications to 4.3 and 5.3, 5.3.1. Removal of superfluous editors notes in several sections.
Consequences if not approved:	⌘	Incorrect interface definition

Clauses affected:	⌘	4.3, 5.2 and 5.3, 5.3.1, 6.2, 8.2.

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

Other comments: ⌘

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

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

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

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

****** Start of change #1 ******

4 Wa Description

4.1 Functionality

The Wa reference point is defined between the I-WLAN and the 3GPP AAA Server or 3GPP AAA Proxy. The description of the reference point and its functionality is given in 3GPP TS 23.234 [4].~~-~~ carrying accounting signalling per WLAN user.

4.2 Protocols

The Wa reference point inter-works between 3GPP networks and WLAN ANs. In early deployments of WLAN-3GPP inter-working, a significant amount of WLAN ANs will provide RADIUS-based interfaces. It is expected that WLAN ANs will migrate gradually towards Diameter-based interfaces.

Therefore, in order to inter-work with the two kinds of WLAN ANs, the 3GPP AAA Proxy in the roaming case and the 3GPP AAA Server in the non-roaming case, both have to support Diameter-based and RADIUS-based protocols at the Wa reference point towards WLAN ANs.

Therefore the Wa reference point shall contain the following protocols:

1) RADIUS, as defined in IETF RFC 2865 [17], including the following extensions:

   - IETF RFC 3579 [14], which provides RADIUS extensions to support the transport of EAP frames over RADIUS.

   - IETF Draft "Carrying Location Objects in RADIUS", draft-ietf-geopriv-radius-lo-01 [16], which provides RADIUS Extensions for Public WLAN are also used in order to identify uniquely the owner and location of the WLAN.

   - IETF RFC 3576 [13], which provides RADIUS extensions to support~~s~~, amongst other capabilities, the capability to immediately disconnect a user from the WLAN AN.

2) Diameter Base, as defined in IETF RFC 3588 [7], as well as IETF Draft " Diameter Extensible Authentication Protocol (EAP) Application" [8], which provides a Diameter application to support the transport of EAP (IETF RFC 3748 [21] frames over Diameter.

The 3GPP AAA Proxy in the roaming case and 3GPP AAA Server in the non-roaming case shall support both 1) and 2) over Wa reference point.

WLAN ANs, depending on their characteristics, shall use either 1) or 2) over Wa reference point.

The Application-Id to be advertised over Wa reference point corresponds to the EAP or Diameter Base Protocol Application-Id, depending on the command sent over Wa.

****** End of change #1 ******

****** Start of change #2 ******

5.2 Protocols

The Wd reference point shall use only a single AAA protocol per WLAN session. RADIUS or Diameter based protocols shall be used, respective of which protocol the WLAN AN is using.

The Wd protocol reference point shall contain the following protocols:

1) RADIUS, as defined in IETF RFC 2865 [17], including the following extensions:

   - IETF RFC 2869 [9], which provides RADIUS extensions to support the transport of EAP frames over RADIUS.

   - IETF Draft "Carrying Location Objects in RADIUS", draft-ietf-geopriv-radius-lo-01 [16], which provides RADIUS Extensions for Public WLAN are to identify uniquely the owner and location of the WLAN.

   - IETF RFC 3576 [13], which provides RADIUS extensions to supports, amongst other capabilities, the capability to immediately disconnect a user from the WLAN AN.

   - GSMA PRD IR.61 [25~~xx~~], which provides a RADIUS Chargeable-User-Id attribute to carry a chargeable user identity (e.g. MSISDN or IMSI) from Home PLMN to Visited PLMN.

2) Diameter Base, as defined in IETF RFC 3588 [7], as well as IETF Draft "Diameter EAP Application" [8], which provides a Diameter application to support the transport of EAP (IETF RFC 2284 [10] and IETF Draft "EAP" [11]) frames over Diameter. In addition, Diameter Base (IETF RFC 3588 [7]) and NASREQ IETF Draft draft-ietf-aaa-diameter-nasreq-12 [12] specify the accounting messaging to be exchanged.

The 3GPP AAA Proxy and the 3GPP AAA Server shall support both 1) and 2) over the Wd reference point. The 3GPP AAA Proxy, depending on the WLAN ANs characteristics, shall use either 1) or 2) over the Wd reference point. See subclause 5.3 for more information of when either 1) or 2) is used.

The Application-Id to be advertised over Wd reference point corresponds to the EAP or Diameter Base Protocol Application-Id, depending on the command sent over Wd.

5.3 3GPP AAA Proxy and 3GPP AAA Server behaviour when Interworking with RADIUS/Diameter WLAN Ans

If a WLAN AN attached to the 3GPP AAA Proxy is Diameter based, Diameter messages shall be passed on to the 3GPP AAA Server through the 3GPP AAA Proxy. If a WLAN AN attached to the 3GPP AAA Proxy is RADIUS based, the RADIUS messages sent by the WLAN AN shall be either passed on to the 3GPP AAA Server through the 3GPP AAA Proxy, or translated by the 3GPP AAA Proxy Translation Agent into Diameter messages to be sent on to the 3GPP AAA Server by the 3GPP AAA Proxy. This protocol translation shall be done as follows.

The 3GPP AAA Server needs to be aware of what kind of client it is serving in order to adapt its operation to the capabilities of the WLAN AN.

The 3GPP AAA Proxy is the only network element in direct contact with the WLAN AN and therefore it is the only network element aware of whether the WLAN AN is RADIUS or Diameter based. The following rules shall apply for the 3GPP AAA Server to determine this:

If the Wd reference point uses RADIUS then:

- The 3GPP AAA Server shall assume that the WLAN AN is RADIUS based.

If the Wd reference point uses Diameter then:

- The 3GPP AAA Server shall assume the WLAN AN to be Diameter- based unless the 3GPP AAA Proxy specifically indicates that the WLAN AN is RADIUS based (see subclause 5.3.1.3~~6.3.3~~).

Once the 3GPP AAA Server is aware of which AAA protocol that the WLAN AN is using , it shall adapt its operation over the Wd reference point.

If the WLAN AN is determined to be Diameter based, the operation mode of the 3GPP AAA Server shall be the normal behaviour as described in Diameter (IETF Draft "EAP" [8]) and the Diameter Base (RFC 3588 [7]). for authentication and NASREQ[12] for accounting.

If the WLAN AN is determined to be RADIUS based, the operation mode of the 3GPP AAA Server shall be the following:

If the Wd reference point is using RADIUS then:

- Normal behaviour for RADIUS as specified in the first bullet in subclause 5.2.

If the Wd reference point is using Diameter then:

- The normal behaviour for Diameter as specified in the second bullet in subclause 5.2, but shall be modified as follows to ensure RADIUS compatibility:
  - Diameter AVPs to RADIUS attributes compatibility:
    - 3GPP AAA Server shall restrict itself to use only Diameter AVPs that are compatible with RADIUS attributes. In general, 3GPP AAA Server shall use Diameter AVPs with codes not greater than 255. See section 9.5 in [12] for further detail.
  - Diameter specific procedures when interacting with RADIUS clients:
    - 3GPP AAA Server shall not attempt server-initiated re-authentication.
    - 3GPP AAA Server may attempt server-initiated re-authorization and server-initiated session termination.
      - If the WLAN AN and the 3GPP AAA Proxy support "Dynamic Authorization Extensions to RADIUS" RFC 3576 [13], then the procedures are performed normally.
      - If the WLAN AN and the 3GPP AAA Proxy do no support "Dynamic Authorization Extensions to RADIUS" RFC 3576 [13], then 3GPP AAA Proxy shall notify the 3GPP AAA Server of this by sending a protocol error such as DIAMETER_COMMAND_UNSUPPORTED. In that case, the 3GPP AAA Server shall not continue to attempt server-initiated re-authorization and/or server-initiated session termination.

5.3.1 Requirements in 3GPP AAA Proxy for RADIUS/Diameter "Translation Agent"

~~Editor's note: This subclause contains all the requirements for the 3GPP AAA Proxy Translation Agent and details about the conversion processes~~

A RADIUS/Diameter Translation Agent has the following requirements:

- Receive RADIUS requests (sent to UDP port 1812);
- Diameter proxy functionality (communicate over TCP/SCTP port TBD, mandatory support for IPSec, optional support for TLS, etc.);
- Convert RADIUS requests to Diameter requests;
- Convert Diameter responses to RADIUS responses;
- Advertise to the 3GPP AAA Server whether the client located in WLAN AN is RADIUS or Diameter based;

- Managing the transaction state information of the RADIUS requests.

The Diameter protocol defines a common space for many RADIUS information elements (AVPs), so that no conversion is necessary when transporting them. However, there are certain AVPs that do need translation and differences of the message formats and transport protocols need to be handled.

**** End of change #2 ****

**** Beginning of change #3 ****

6.2 Protocols

The Wx reference point shall be Diameter based and shall have an application ID defined for it. It is defined as an IETF vendor specific Diameter application, where the vendor is 3GPP. The application identifier is to TBA. It is to be assigned by IANA (http://www.iana.org/assignments/enterprise-numbers).

~~Editors note: Wx has been specified to reuse Cx as much as possible. However, changes to the mandatory AVPs in the procedure definitions require that a new Diameter application ID is needed for Wx interface.~~

**** End of change #3 ****

**** Beginning of change #4 ****

8.3.2 Authorization Procedures

According to the requirements stated in subclause 10.1, Wm reference point shall enable:

- Carrying messages for service authorization between PDG and 3GPP AAA Server/Proxy.
- Allow the 3GPP AAA Server/Proxy to retrieve tunnelling attributes and WLAN UE's IP configuration parameters from/via Packet Data Gateway.

This procedure is used between the PDG and 3GPP AAA Server and Proxy. It is invoked by the PDG, on receipt from the WLAN-UE of a "tunnel establishment request" message and subsequent to the success of tunnel authentication i.e. on receipt of a DEA message from the 3GPP AAA Server with Result Code set to "Success".

The Wm reference point performs authorization download based on the reuse of the NASREQ [12] AAR-AAA command set.

Table 8.3.2.1 Wm Authorization Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.
Request-Type	Session-Request-Type	M	Type of Wm specific Diameter application request. The following values are to be used: AUTHORIZATION REQUEST (0) This value shall indicate the initial request for authorization of the user to the APN. ROUTING POLICY (1) This value shall indicate that routing policy AVP is present.
Visited Network Identifier	Visited-Network-Identifier	C	Identifier that allows the home network to identify the Visited Network. This AVP shall be present if the PDG is not in the WLAN-UE's home network, i.e. the WLAN-UE is roaming.
W-APN-ID	APN-Id	C	This information element contains the W-APN which the UE is requesting authorization. This AVP is present when Session-Request-Type AVP is set to AUTHORIZATION REQUEST.
Routing Policy	Routing-Policy	C	This AVP includes the routing policy of the tunnel set-up. This AVP shall be present when Session-Request-Type AVP is set to ROUTING POLICY. The exact format of this AVP is specified in section 10.1.24. ~~Editor's Note: Its exact format is ffs.~~
Routing Information	Destination-Host	M	The 3GPP AAA Server name is obtained from the Origin-Host AVP of a previously received message.

Table 8.3.2.2: AA-Response

Information element name	Mapping to Diameter AVP	Cat.	Description
Registration Result	Result Code/ Experimental Result Code	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. **Experimental-Result AVP shall be used for Wm errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP**
Subscription-ID AVP	Subscription-ID AVP	C	This AVP shall contain the MSISDN of the user. This AVP shall be present is the Diameter Result Code is set to DIAMETER_SUCCESS
Max-Subscribed-Bandwidth	Max-Requested-Bandwidth	O	The Max requested bandwidth AVP. Can be sent by the 3GPP AAA Server to the PDG if it is present in the user subscription info held at the 3GPP AAA Server.
Charging Data	Charging-Data	C	Charging information for the W-APN for that user. It shall be present when Result-Code is equal to DIAMETER_SUCCESS and when the received Session-Request–Type was set to AUTHORIZATION REQUEST.
Framed-IP-Address	Framed-IP-Address	O	This AVP contains the remote IPv4 address of the WLAN UE that the 3GPP AAA Server downloaded from the HSS. This AVP shall not be present when the 3GPP AAA Server received an authorisation request with Session-Request–Type AVP set to ROUTING POLICY.
Framed-IP-Prefix	Framed-IP-Prefix	O	This AVP contains the remote IPv6 prefix of the WLAN UE that the 3GPP AAA Server downloaded from the HSS. This AVP shall not be present when the 3GPP AAA Server received an authorisation request with Session-Request–Type AVP set to ROUTING POLICY.

****** End of change #4 ******

3GPP TSG CN WG4 Meeting #27 **N4-050581**
Cancun, Mexico, 25th – 29th April 2005

CR-Form-v7

CHANGE REQUEST

⌘ **29.234** **CR** **055** ⌘ **rev** ⌘ Current version: **6.2.0** ⌘

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

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

Title:	⌘	Reference to W-APN definition in 23.003
Source:	⌘	Nokia
Work item code:	⌘	WLAN-IW
Date:	⌘	14/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	W-APN is defined in 23.003. 29.234 descritption of W-APN should therefore reference that
Summary of change:	⌘	Added reference to 23.003 in section 10.1.15.
Consequences if not approved:	⌘	Unclear spec

Clauses affected:	⌘	14			
Other specs affected:	⌘	**Y**	**N**		
		X		Other core specifications	⌘ 23.003-099, 24.234-023
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

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

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

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

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

**** Start of change #1 ****

10.1.15 APN-Id

The APN-Id AVP is of type OctetString, and contains the W-APN for which the user will have services available. These W-APNs may be mapped to services in the home network or in the visited network. W-APN is defined in 3GPP TS 23.003 [22].

**** End of change #1 ****

3GPP TSG CN WG4 Meeting #27
Cancun, MEXICO, 25th – 29th April 2005

C4-050759

CR-Form-v7

CHANGE REQUEST

⌘ **29.234** **CR** **049** ⌘ **rev** **1** ⌘ Current version: **6.2.0** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Addition of missing functionality to Wa Interface RADIUS profile
Source:	⌘	TeliaSonera
Work item code:	⌘	WLAN-IW
Date:	⌘	07/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Stage 2 (23.234) says for the Wa interface that it 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. Also Stage 2 requires support for providing access scope limitation information to the WLAN based on the authorised services for each user (for example, IP address filters). Currently Stage 3 Wa RADIUS profile does not have any support for the Stage 2 requirement.
Summary of change:	⌘	This contribution adds the following: • A reference to an IETF draft describing attributes that can be used to implement needed functionality (draft-congdon-radext-ieee802) • Eight new RADIUS attributes to Wa profile that can be used to implement routing enforcement and tunnelling.
Consequences if not approved:	⌘	The 29.234 is not compliant with the 23.234 requirements for RADIUS Wa.

Clauses affected:	⌘	2, 4.2, 4.4.1

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

⌘

Other comments:	⌘	

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

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

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

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

**** Start of change #1 ****

2 References

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

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

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 22.934: "Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking".

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

[4] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; System description".

[5] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents".

[6] 3GPP TS 29.229: "Cx and Dx interfaces based on the Diameter protocol; Protocol details".

[7] IETF RFC 3588: "Diameter Base Protocol".

[8] IETF Draft: "Diameter Extensible Authentication Protocol (EAP) Application", draft-ietf-aaa-eap-09.txt, work in progress.

[9] IETF RFC 2869: "RADIUS Extensions".

[10] IETF RFC 2284: "Extensible Authentication Protocol (EAP)".

[11] IETF Draft: "Extensible Authentication Protocol (EAP) ", draft-ietf-eap-rfc2284bis-02.txt, work in progress.

[12] IETF Draft: "Diameter Network Access Server Application", draft-ietf-aaa-diameter-nasreq-12.txt, work in progress.

[13] IETF RFC 3576: "Dynamic Extensions to Remote Authentication Dial In User Service (RADIUS)".

[14] IETF RFC 3579: "RADIUS (Remote Authentication Dial-In User Service) Support For Extensible Authentication Protocol (EAP) ".

[15] IETF RFC 3580: "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines".

[16] IETF Draft, " Carrying Location Objects in RADIUS ", draft-ietf-geopriv-radius-lo-01.txt, work in progress .

[17] IETF RFC 2865: "Remote Authentication Dial In User Service (RADIUS)".

[18] 3GPP TS 33.234: "3G security; Wireless Local Area Network (WLAN) interworking security".

[19] IETF Draft, "Diameter Credit-control Application", draft-ietf-aaa-diameter-cc-04.txt, work in progress.

[20] IETF RFC 2866: "RADIUS Accounting".

[21] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[22] 3GPP TS 23.003: "Numbering, addressing and identification".

[23] 3GPP TS 32.240: " Charging architecture and principles".

[24] 3GPP TS 32.215: "Charging data description for the Packet Switched (PS) domain".

[25] GSMA PRD IR.61, "WLAN Roaming Guidelines".

[26] IETF Draft, "Chargeable User Identity", draft-adrangi-radius-chargeable-user-identity-02.txt, work in progress.

[27] IETF Draft "EAP lower layer attributes for AAA protocols", <draft-mariblanca-aaa-eap-lla-01.txt>, work in progress

[28] IETF Draft "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)", draft-haverinen-pppext-eap-sim-16.txt, work in progress

[29] IETF Draft "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", draft-arkko-pppext-eap-aka-15.txt, work in progress

[xx] IETF Draft “RADIUS Extensions for IEEE 802”, draft-congdon-radext-ieee802-03.txt, work in progress

****** End of change #1 ******

**** Start of change #2 ****

4.2 Protocols

The Wa reference point inter-works between 3GPP networks and WLAN ANs. In early deployments of WLAN-3GPP inter-working, a significant amount of WLAN ANs will provide RADIUS-based interfaces. It is expected that WLAN ANs will migrate gradually towards Diameter-based interfaces.

Therefore, in order to inter-work with the two kinds of WLAN ANs, the 3GPP AAA Proxy in the roaming case and the 3GPP AAA Server in the non-roaming case, both have to support Diameter-based and RADIUS-based protocols at the Wa reference point towards WLAN ANs.

Therefore the Wa reference point shall contain the following protocols:

1) RADIUS, as defined in IETF RFC 2865 [17], including the following extensions:

   - IETF RFC 3579 [14], which provides RADIUS extensions to support the transport of EAP frames over RADIUS.

   - IETF Draft "Carrying Location Objects in RADIUS", draft-ietf-geopriv-radius-lo-01 [16], which provides RADIUS Extensions for Public WLAN are also used in order to identify uniquely the owner and location of the WLAN.

   - IETF RFC 3576 [13], which provides RADIUS extensions to supports, amongst other capabilities, the capability to immediately disconnect a user from the WLAN AN.

   - IETF Draft “RADIUS Extensions for IEEE 802”, draft-congdon-radext-ieee802-03.txt, which provides RADIUS Extensions for Public WLAN including attributes to provide filtering and routing enforcement.

2) Diameter Base, as defined in IETF RFC 3588 [7], as well as IETF Draft " Diameter Extensible Authentication Protocol (EAP) Application" [8], which provides a Diameter application to support the transport of EAP (IETF RFC 3748 [21] frames over Diameter.

The 3GPP AAA Proxy in the roaming case and 3GPP AAA Server in the non-roaming case shall support both 1) and 2) over Wa reference point.

WLAN ANs, depending on their characteristics, shall use either 1) or 2) over Wa reference point.

The Application-Id to be advertised over Wa reference point corresponds to the EAP or Diameter Base Protocol Application-Id, depending on the command sent over Wa.

**** End of change #2 ****

****** Start of change #3 ******

4.4 Information Element Contents

4.4.1 RADIUS based Information Elements Contents

Table 4.4.1: RADIUS based Information Elements Contents

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
USER ID	This Attribute indicates the identity of the user as defined in 3GPP TS 23.003 [22].	Mandatory	Mandatory	Mandatory	Mandatory	User-Name
RADIUS Client Address	This Attribute indicates the identifying IP Address of the RADIUS Client. It should be unique to the RADIUS Client within the scope of the RADIUS server. More detailed description of the IE can be found in IETF RFC 3580 [15].	Mandatory	NA	NA	NA	NAS-IP Address
Operator Name	Hot Spot Operator Name as defined in IETF Draft draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	NA	NA	Operator Name
Location Name	Location Type of the hot spot operator as defined in IETF Draft draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	NA	NA	Location Name
Location Information	Location information regarding the hotspot operator as defined in IETF Draft draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	NA	NA	Location information
EAP Message	This attribute encapsulates Extensible Authentication Protocol packets so as to allow the NAS to authenticate users via EAP without having to understand the EAP protocol. More detailed description of the IE can be found in IETF RFC 3580 [15].	Mandatory	Mandatory	Mandatory	Mandatory	EAP-Message
Diameter Session ID + 3GPP AAA Server Host AVP + prefix "Diameter"	This attribute is relayed from the 3GPP AAA Proxy to the WLAN-AN when the 3GPP AAA Proxy acts as translation agent. If the WLAN-AN receives such an attribute, it MUST include it in Access Requests.	Conditional	NA	NA	Conditional	State
Diameter Session ID + prefix "Diameter"	This attribute is sent by 3GPP AAA Proxy when acting as a translation agent. If WLAN-AN receives it, is should include it in subsequent accounting messages.	NA	Conditional	NA	NA	Class
State Information	A 3GPP AAA Server using RADIUS may include this attribute in Access Challenges. If the Radius Client in WLAN-AN receives	Conditional	NA	NA	Optional	State

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
	such an attribute, it shall be present in Access-Request that is sent in response to the Access-Challenge. This IE is used when no Diameter-RADIUS translation takes place.					
Session ID	A 3GPP AAA Server using RADIUS shall include this attribute to facilitate charging correlation between accounting and authorization messaging. If the Radius Client in WLAN-AN receives it, it shall be included in subsequent accounting messages. This IE is used when no Diameter-RADIUS translation takes place.	NA	Conditional	NA	NA	Class
Session Alive Time	This Attribute sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt. A more detailed description of the IE can be found in IETF RFC 3580 [15].	NA	Optional	NA	Optional	Session-Time-Out

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
Charging Duration	This attribute indicates the time between each interim update in seconds for this specific session. A more detailed description of the IE can be found in IETF RFC 2869 [9].	NA	Optional	NA	NA	Acct-Interim-Interval
Termination Action	This Attribute indicates what action the NAS should take when the specified service is completed. More detailed description of the IE can be found in IETF RFC 3580 [15].	NA	Optional	NA	Optional	Termination-Action
Pairwise Master Key (PMK)	This IE is used to carry the Pairwise Master Key. More detailed description of the IE can be found in IETF Draft draft-haverinen-pppext-eap-sim-16 [28] and IETF Draft draft-arkko-pppext-eap-aka-15 [29].	NA	Mandatory	NA	NA	Vendor-Specific (MS-MPPE-Recv-Key)
Message Authenticator	Message Authenticator.	Mandatory	Mandatory	Mandatory	Mandatory	Message Authenticator
WLAN-UE MAC address	Carries the MAC address of the WLAN-UE for verification at the 3GPP AAA Server.	Mandatory	NA	NA	NA	Calling Station ID
Chargeable User Identity	This Attribute shall contain the MSISDN of the user as specified in IETF Draft draft-adrangi-radius-chargeable-user-identity-02 [26].	Optional	Mandatory	NA	NA	Chargeable-User-Id
Filter ID	This IE indicates the name of the filter list for the user.	NA	Optional	NA	NA	Filter-Id
NAS Filter Rule	This IE enables the provisioning of Layer 2-4/7 filter and redirection rules on the NAS by 3GPP AAA Server/Proxy. More detailed description of the IE can be found in IETF Draft draft-congdon-radext-ieee802-03 [xx].	NA	Optional	NA	NA	NAS-Filter-Rule
Tunnel Type	This IE contains the used tunnelling protocol.	NA	Optional	NA	NA	Tunnel-Type
Tunnel Medium Type	This IE contains the transport medium to use when creating a tunnel.	NA	Optional	NA	NA	Tunnel-Medium-Type
Tunnel Private Group Id	This IE indicates the group ID for a particular tunneled session.	NA	Optional	NA	NA	Tunnel-Private-Group-Id
Tunnel Client Endpoint	This IE indicates the address of the client end of the tunnel.	NA	Optional	NA	NA	Tunnel-Client-Endpoint
Tunnel Server Endpoint	This Attribute indicates the address of the server end of the tunnel.	NA	Optional	NA	NA	Tunnel-Server-Endpoint

The parameters listed above as 'mandatory' are only optional in the particular RADIUS (extension) specification in which they are originally defined. However, in order for 3GPP WLAN-IW to function, these attributes shall be passed in messaging over the Wa interface as per the definition in the table. In this sense they are mandatory. In practice, this means that, should any of these parameters labelled 'mandatory' be missing from the RADIUS messaging over Wa, this will result in a higher level failure of WLAN-IW procedures to function properly and consequently in a denial of the RADIUS request (even though this was a valid RADIUS message).

****** End of change #3 ******

3GPP TSG CN WG4 Meeting #27
Cancun, MEXICO, 25th – 29th April 2005

C4-050760

CR-Form-v7

CHANGE REQUEST

⌘ **29.234** **CR** **050** ⌘ **rev** **1** ⌘ Current version: **6.2.0** ⌘

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

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

Title:	⌘	Addition of missing functionality to Wa Interface Diameter profile
Source:	⌘	TeliaSonera
Work item code:	⌘	WLAN-IW
Date:	⌘	07/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Stage 2 (23.234) says for the Wa interface that it 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. Also Stage 2 requires support for providing access scope limitation information to the WLAN based on the authorised services for each user (for example, IP address filters). Currently Stage 3 Wa Diameter profile does not have any support for the Stage 2 requirement.
Summary of change:	⌘	This contribution adds the following: • New Diameter AVPs to Wa profile. • New Diameter AVPs to DEA command that can be used to implement routing enforcement and tunnelling.
Consequences if not approved:	⌘	The 29.234 is not compliant with the 23.234 requirements for Diameter Wa.

Clauses affected:	⌘	4.2, 4.3.1, 4.4.2.1

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

Other comments:	⌘	

How to create CRs using this form:

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

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

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

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

**** Start of change #1 ****

4.2 Protocols

The Wa reference point inter-works between 3GPP networks and WLAN ANs. In early deployments of WLAN-3GPP inter-working, a significant amount of WLAN ANs will provide RADIUS-based interfaces. It is expected that WLAN ANs will migrate gradually towards Diameter-based interfaces.

Therefore, in order to inter-work with the two kinds of WLAN ANs, the 3GPP AAA Proxy in the roaming case and the 3GPP AAA Server in the non-roaming case, both have to support Diameter-based and RADIUS-based protocols at the Wa reference point towards WLAN ANs.

Therefore the Wa reference point shall contain the following protocols:

1) RADIUS, as defined in IETF RFC 2865 [17], including the following extensions:

   - IETF RFC 3579 [14], which provides RADIUS extensions to support the transport of EAP frames over RADIUS.

   - IETF Draft "Carrying Location Objects in RADIUS", draft-ietf-geopriv-radius-lo-01 [16], which provides RADIUS Extensions for Public WLAN are also used in order to identify uniquely the owner and location of the WLAN.

   - IETF RFC 3576 [13], which provides RADIUS extensions to supports, amongst other capabilities, the capability to immediately disconnect a user from the WLAN AN.

2) Diameter Base, as defined in IETF RFC 3588 [7], including the following additional specifications:

   - ~~as well as~~ IETF Draft " Diameter Extensible Authentication Protocol (EAP) Application" [8], which provides a Diameter application to support the transport of EAP (IETF RFC 3748 [21] frames over Diameter.

   - IETF Draft "Diameter Network Access Server Application" [12], draft-ietf-aaa-diameter-nasreq-12.txt, which defines a Diameter protocol application used for Authentication, Authorization and Accounting (AAA) services in the Network Access Server (NAS) environment.

The 3GPP AAA Proxy in the roaming case and 3GPP AAA Server in the non-roaming case shall support both 1) and 2) over Wa reference point.

WLAN ANs, depending on their characteristics, shall use either 1) or 2) over Wa reference point.

The Application-Id to be advertised over Wa reference point corresponds to the EAP or Diameter Base Protocol Application-Id, depending on the command sent over Wa.

**** End of change #1 ****

**** Start of change #2 ****

4.3.1 WLAN Access Authentication and Authorization

This procedure is used to transport over RADIUS or Diameter, the WLAN Access (Re)Authentication and Authorization between the WLAN AN and the 3GPP AAA Proxy.

Diameter usage in Wa:

- This procedure is mapped to the Diameter-EAP-Request and Diameter-EAP-Answer command codes specified in [8].
- For (re)authentication procedures, the messaging described below is reused.

Table 4.3.1.1: Authentication request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.
EAP payload	EAP-payload	M	Encapsulated EAP payload used for WLAN UE-3GPP AAA Server mutual authentication
Authentication Request Type	Auth Request-Type	M	Defines whether authentication is required or authorization. AUTHENTICATE_ONLY is required in this case.
NAS-IP address	NAS-IP Address	C	IP address of the hot-spot
NAS-Ipv6 address	NAS-Ipv6 address	C	Ipv6 address of the hot-spot
WLAN UE MAC address	Calling Station-ID	M	Carries the MAC address of the WLAN-UE.

Table 4.3.1.2: Authentication response

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.
EAP payload	EAP payload	M	Encapsulated EAP payload used for UE- 3GPP AAA Server mutual authentication
Result code	Result-Code	M	Result of the operation. Result codes are as per in NASREQ. 1xxx should be used for multi-round, 2xxx for success.
Session Alive Time	Session-Timeout	O	Max no of seconds the user session should remain active
Accounting Interim - Interval	Accounting Interim-Interval	O	Charging duration
Encryption-Key	EAP-Master-Session-Key	C	Shall be sent if Result Code is set to "Success".
Filter Id	Filter-Id	O	This IE indicates the name of the filter list for the user.
NAS Filter Rule	NAS-Filter-Rule	O	This IE provides filter rules that need to be configured on the NAS for the user by 3GPP Server/Proxy.
Tunneling	Tunneling	O	This IE can be used to provide needed tunnelling configuration on the NAS for the user by 3GPP Server/Proxy.

RADIUS usage in Wa:

- This procedure is mapped to the RADIUS Access Request, RADIUS Access Challenge, RADIUS Access Accept and RADIUS Access Reject specified in RFC 3579 [14].
- See Annex A.1 for signalling flow reference.

**** End of change #2 ****

**** Start of change #3 ****

4.4.2.1 DER and DEA Commands

ABNF for the DER and DEA messages are given below:

```
<Diameter-EAP-Request> ::= < Diameter Header: 268, REQ, PXY >
    < Session-Id >
    { Auth-Application-Id }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    { Auth-Request-Type }
    { EAP-Payload }
    [ Destination-Host ]
    [ User-Name ]
    [ NAS-IP-Address ]
    [ NAS-IPv6-Address ]
    [Calling Station-ID ]
    * [ Proxy-Info ]
    * [ Route-Record ]
    * [ AVP ]
```

For the DEA, the following are necessary:

```
<Diameter-EAP-Answer> ::= < Diameter Header: 268, PXY >
    < Session-Id >
    { Auth-Application-Id }
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    { Auth-Request-Type }
    [ EAP-Payload ]
    [ User-Name ]
    [ Session-Timeout ]
    [ Accounting-Interim-Interval ]
    [ EAP-Master-Session-Key]
    * [Filter-Id]
    * [NAS-Filter-Rule]
    * [Tunneling]
    * [ Proxy-Info ]
    * [ AVP ]
```

**** End of change #3 ****

3GPP TSG CN WG4 Meeting #27
Cancun, Mexico, 25th – 29th April 2005

C4-050761

CR-Form-v7

CHANGE REQUEST

⌘ **29.234** **CR** **054** ⌘ **rev** **1** ⌘ Current version: **6.2.0** ⌘

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

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

Title:	⌘	Visited Network Identifier on the Wx interface
Source:	⌘	Nokia
Work item code:	⌘	WLAN-IW
Date:	⌘	28/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Current Wx specification lists Visited-Network-Identifier to be a mandatory parameter sent over the Wx interface in the MAR message. However, this parameter is only available/valid in the roaming case. Therefore this parameter should be made conditional.
Summary of change:	⌘	Modified the interface elements table in 6.3.1 to changed the VPLMN AVP to conditional, tidying up of the detailed behaviour in 6.3.1.1 accordingly; modification of the ABNF in section 6.4.1 to make VPLMN optional.
Consequences if not approved:	⌘	Potential bug in the non-roaming case, since the Wx interface insists on a VPLMN-ID being present in the MAR command, but the 3GPP AAA Server not having such a parameter.

Clauses affected:	⌘	6.3.1, 6.3.1.1, 6.4.1

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

Other comments:	⌘	

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

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

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

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

**** Start of change #1 ****

6.3 Procedures Description

6.3.1 Authentication Procedures

According to the requirements described in clause 6.1, Wx reference point shall enable:

- Retrieval of authentication vectors (triplets and quintuplets) from HSS.
- Checking of user subscription information at the HSS

This procedure is used between the 3GPP AAA Server and the HSS. The procedure is invoked by the 3GPP AAA Server when a new set of authentication information for a given subscriber is to be retrieved from an HSS. This can happen for example, when a new 3GPP subscriber has accessed the 3GPP AAA Server for authentication or when a new set of authentication information is required for one of the 3GPP subscribers already registered in the 3GPP AAA server.

The Wx reference point performs the authentication data download based on the reuse of the existing Cx authentication command code set (MAR/MAA), see 3GPP TS 29.228 [5] and 3GPP TS 29.229 [6]. It corresponds to the combination of the operations Auth-Info-Request and Auth-Info-Response (see 3GPP TS 23.234 [4]) and is used:

- To retrieve authentication vectors from the HSS.
- To resolve synchronization failures between the sequence numbers in the WLAN-UE and the HSS.

Table 6.3.1.1: Authentication request

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element contains the permanent identity of the user, i.e. the IMSI.
Visited Network Identifier	Visited-Network-Identifier	C~~M~~	Identifier that allows the home network to identify the Visited Network. The 3GPP AAA Server shall include this information element in the roaming case i.e. when 3GPP AAA Server receives this information element from signalling across the Wd. Editor's note: See 3GPP TS 29.229 [6] for a description of this parameter
Number Authentication Items	SIP-Number-Auth-Items	M	This information element indicates the number of authentication vectors requested
Authentication Data	SIP-Auth-Data-Item	C	See tables 6.3.1.2 and 6.3.1.3 for the contents of this information element. The content shown in table 6.3.1.2 shall be used for a normal authentication request; the content shown in table 6.3.1.3 shall be used for an authentication request after synchronization failure.
Routing Information	Destination-Host	C	If the 3GPP AAA Server knows the HSS name, this AVP shall be present. This information is available if the 3GPP AAA Server already has the HSS name stored. The HSS name is obtained from the Origin-Host AVP, which is received from a previous command from the HSS or from the SLF. Otherwise only the Destination-Realm is included so that it is resolved to an HSS address in an SLF-like function. Once resolved the Destination-Host AVP is included with the suitable HSS address and it is stored in the 3GPP AAA Server for further usage.
EAP Lower Layer	EAP Lower Layer	M	This AVP shall contain the value "2" to indicate the user accessed the I-WLAN network by WLAN 3GPP Direct access and shall contain value “3” to indicate the user accessed the I-WLAN network by WLAN 3GPP IP access, according to IETFdraft-mariblanca-aaa-eap-lla-01 [27].

Table 6.3.1.2: Authentication Data content - request

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Method	Authentication Method	M	This information element indicates the authentication method compatible with the smart card (SIM or USIM). It shall contain EAP/SIM or EAP/AKA values.

Table 6.3.1.3: Authentication Data content - request, synchronization failure

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Method	Authentication Method	M	This information element indicates the authentication method compatible with the smart card (SIM or USIM). It shall contain EAP/SIM or EAP/AKA values.
Authorization Information	SIP-Authorization	M	It shall contain the concatenation of nonce, as sent to the terminal, and auts, as received from the terminal. Nonce and auts shall both be binary encoded.

Table 6.3.1.4: Authentication answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element contains the permanent identity of the user, i.e. the IMSI.
Number Authentication Items	SIP-Number-Auth-Items	C	This AVP indicates the number of authentication vectors delivered in the Authentication Data information element. It shall be present when the result is DIAMETER_SUCCESS.
Authentication Data	SIP-Auth-Data-Item	C	If the SIP-Number-Auth-Items AVP is equal to zero or it is not present, then this AVP shall not be present. See table 6.3.1.5 for the contents of this information element.
3GPP AAA Server Name	3GPP-AAA Server-Name	C	This AVP contains the Diameter address of the 3GPP AAA Server. This AVP shall be sent when the user has been previously authenticated by another 3GPP AAA Server and therefore there is another 3GPP AAA Server serving the user.
Result	Result-Code / Experimental-Result	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Wx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

Table 6.3.1.5: Authentication Data content - response

Information element name	Mapping to Diameter AVP	Cat.	Description
Item Number	SIP-Item-Number	C	This information element shall be present in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVPs, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.
Authentication Method	Authentication Method	M	This information element indicates the authentication method compatible with the smart card (SIM or USIM). It shall contain EAP/SIM or EAP/AKA values.
Authentication Information AKA	SIP-Authenticate	C	It shall contain, binary encoded, the concatenation of the authentication challenge RAND and the token AUTN. See 3GPP TS 33.203 [3] for further details about RAND and AUTN. It shall be present when SIP_Authentication_Scheme AVP is set to EAP/AKA.
Authorization Information AKA	SIP-Authorization	C	It shall contain binary encoded, the expected response XRES. See 3GPP TS 33.203 [3] for further details about XRES. It shall be present when SIP_Authentication_Scheme AVP is set to EAP/AKA.
Confidentiality Key AKA	Confidentiality-Key	C	This information element, if present, shall contain the confidentiality key. It shall be binary encoded. It shall be present when SIP_Authentication_Scheme AVP is set to EAP/AKA.
Integrity Key AKA	Integrity-Key	C	This information element shall contain the integrity key. It shall be binary encoded. It shall be present when SIP_Authentication_Scheme AVP is set to EAP/AKA.
Authentication Information SIM	Authentication_Information_SIM	C	This information element shall contain the concatenation of authentication challenge RAND and the ciphering key Kc. It shall be binary encoded. It shall be present when SIP_Authentication_Scheme AVP is set to EAP/SIM.
Authorization Information	Authorization_Information_SIM	C	This information element shall contain the response SRES. It shall be binary encoded. It shall be present when SIP_Authentication_Scheme AVP is set to EAP/SIM.

6.3.1.1 Detailed behaviour

The HSS shall, in the following order (if there is an error in any of the steps, the HSS shall stop processing and return the corresponding error code):

1. Check that the user exists in the HSS. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2. Check that the user has 3GPP-WLAN subscription. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_NO_WLAN_SUBSCRIPTON.

3. If a Visited-Network-Identifier is present, c~~C~~heck that the user is allowed to roam in the visited network. If the user is not allowed to roam in the visited network~~not~~, Experimental-Result-Code shall be set to DIAMETER_ERROR _ROAMING_NOT_ALLOWED.

4. Check WLAN-3GPP-Access-Type AVP. If the access type indicates WLAN 3GPP Direct access, the process continues as stated in step 5. If the access type indicates WLAN 3GPP IP access, the HSS shall check the dependence permissions that the user has with regard to the access type.

   - If the Access_Dependence flag of the user is set and the user has been already authenticated by WLAN 3GPP Direct access, the process continues as stated in step 5.

   - If the Access_Dependence flag of the user is set and the user has not been already authenticated by WLAN 3GPP Direct access, the authentication shall be denied by sending to the 3GPP AAA Server

an answer message with Experimental-Result-Code set to DIAMETER_ERROR_NO_ACCESS_INDEPENDENT_SUBSCRIPTION.

- If the Access_Dependence flag of the user is cleared, the user is allowed to request WLAN 3GPP IP access authentication with no regard to any other previous authentication, so the process continues as stated in step 5.

5. The HSS shall check if there is an existing 3GPP AAA Server already assisting the user

   - If there is a 3GPP AAA Server already serving the user, the HSS shall check the request type.

     - If the request indicates there is a synchronization failure, the HSS shall compare the 3GPP AAA Server name received in the request to the 3GPP AAA Server name stored in the HSS. If they are identical, the HSS shall process AUTS as described in 3GPP TS 33.203 [3] and return the requested authentication information. The Result-Code shall be set to DIAMETER_SUCCESS.

     - If the request indicates authentication, the HSS shall return the old 3GPP AAA Server to the requester 3GPP AAA Server. The Result-Code shall be set to DIAMETER_SUCCESS.

       The requester 3GPP AAA Server, upon detection of a 3GPP AAA Server name in the response assumes that the user already has a 3GPP AAA Server assigned, so makes use of Diameter redirect function to indicate the 3GPP AAA Server name where to address the authentication request.

NOTE: This behaviour is not possible when Wa and Wd are over RADIUS since RADIUS does not implement redirect function. It is FFS how RADIUS shall comply with the Stage 2 requirement on avoiding multiple WLAN connections for the same subscriber over different 3GPP AAA Servers.

   - If there is no a 3GPP AAA Server already serving the user, the HSS shall store the 3GPP AAA Server name. The HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The Result-Code shall be set to DIAMETER_SUCCESS.Exceptions to the cases specified here shall be treated by HSS as error situations, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY. No authentication information shall be returned.

NOTE: Origin-Host AVP shall contain the 3GPP AAA Server identity.

**** End of change #1 ****

**** Start of change #2 ****

6.4 Information Elements Contents

6.4.1 Authentication Procedures

The Multimedia-Authentication-Request (MAR) command, indicated by the Command-Code field set to 303 and the 'R' bit set in the Command Flags field, is sent by the 3GPP AAA Server to the HSS in order to request security information.

Message Format

```
< Multimedia-Authentication-Request > ::= < Diameter Header: 303, YYYY, REQ >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    [ Destination-Host ]
```

```
    {EAP Lower Layer}
    { User-Name}
    [{ Visited-Network-Identifier]}
    [ SIP-Auth-Data-Item ]
    [ SIP-Number-Auth-Items ]
    * [ AVP ]
    * [ Proxy-Info ]
    * [ Route-Record ]
```

The Multimedia-Authentication-Answer (MAA) command, indicated by the Command-Code field set to 303 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Multimedia-Authentication-Request command. The Result-Code or Experimental-Result AVP may contain one of the values defined in section x.x in addition to the values defined in RFC 3588 [7].

Message Format

```
< Multimedia-Authentication-Answer > ::=  < Diameter Header: 303, YYYY >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    [ Result-Code ]
    [ Experimental-Result ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    { User-Name}
    [ SIP-Number-Auth-Items ]
    [SIP-Auth-Data-Item ]
    [ AVP ]
    [ Proxy-Info ]
    [ Route-Record ]
```

**** End of change #2 ****

3GPP TSG CN WG4 Meeting #27 **N4-050762**
Cancun, MEXICO, 25th – 29th April 2005

CR-Form-v7

CHANGE REQUEST

⌘ **29.234** **CR** **056** ⌘ **rev** **1** ⌘ Current version: **6.2.0** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Clarifications on Wa and Wd RADIUS profiles
Source:	⌘	TeliaSonera
Work item code:	⌘	WLAN-IW
Date:	⌘	07/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*

Reason for change:	⌘	The latest update on the IETF Draft draft-ietf-radext-chargeable-user-id-04.txt does not anymore define the encoding for identities carried inside the attribute. The Chargeable-user-id RADIUS attribute is used in both Wa and Wd RADIUS profiles. The exact encoding for the MSISDN that is carried inside the Chargeable-user-id needs to be defined somewhere.
Summary of change:	⌘	This contribution adds a reference to the GSMA PRD IR.61, which defines encoding for the MSISDN carried inside the Chargeable-user-id. The changes are the following: • In chapter 2 update reference to the latest IETF Draft • In sub-clause 4.4.1 a reference to GSMA PRD IR.61 is added to the Chargeable User Identity Information Element in the Wa RADIUS profile table • In sub-clause 4.5.1.1 a reference to GSMA PRD IR.61 is added to the Chargeable User Identity Information Element in the Wa RADIUS profile table • In sub-clause 5.2 references are updated as they are incorrect currently • In sub-clause 5.5.4 a reference to GSMA PRD IR.61 is added to the Chargeable User Identity Information Element in the Wd RADIUS profile table • In sub-clause 5.5.5 a reference to GSMA PRD IR.61 is added to the Chargeable User Identity Information Element in the Wd RADIUS profile table
Consequences if not approved:	⌘	No exact MSISDN encoding format for the chargeable-user-id attribute in both Wa and Wd RADIUS profiles.

Clauses affected:	⌘	2, 4.4.1, 4.5.1.1, 5.2, 5.5.4, 5.5.5

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

How to create CRs using this form:

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

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

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

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

**** Start of change #1 ****

2 References

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

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

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 22.934: "Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking".

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

[4] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; System description".

[5] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents".

[6] 3GPP TS 29.229: "Cx and Dx interfaces based on the Diameter protocol; Protocol details".

[7] IETF RFC 3588: "Diameter Base Protocol".

[8] IETF Draft: "Diameter Extensible Authentication Protocol (EAP) Application", draft-ietf-aaa-eap-09.txt, work in progress.

[9] IETF RFC 2869: "RADIUS Extensions".

[10] IETF RFC 2284: "Extensible Authentication Protocol (EAP)".

[11] IETF Draft: "Extensible Authentication Protocol (EAP) ", draft-ietf-eap-rfc2284bis-02.txt, work in progress.

[12] IETF Draft: "Diameter Network Access Server Application", draft-ietf-aaa-diameter-nasreq-12.txt, work in progress.

[13] IETF RFC 3576: "Dynamic Extensions to Remote Authentication Dial In User Service (RADIUS)".

[14] IETF RFC 3579: "RADIUS (Remote Authentication Dial-In User Service) Support For Extensible Authentication Protocol (EAP) ".

[15] IETF RFC 3580: "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines".

[16] IETF Draft, " Carrying Location Objects in RADIUS ", draft-ietf-geopriv-radius-lo-01.txt, work in progress .

[17] IETF RFC 2865: "Remote Authentication Dial In User Service (RADIUS)".

[18] 3GPP TS 33.234: "3G security; Wireless Local Area Network (WLAN) interworking security".

[19] IETF Draft, "Diameter Credit-control Application", draft-ietf-aaa-diameter-cc-04.txt, work in progress.

[20] IETF RFC 2866: "RADIUS Accounting".

[21] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[22] 3GPP TS 23.003: "Numbering, addressing and identification".

[23] 3GPP TS 32.240: " Charging architecture and principles".

[24] 3GPP TS 32.215: "Charging data description for the Packet Switched (PS) domain".

[25] GSMA PRD IR.61, "WLAN Roaming Guidelines".

[26] IETF Draft, "Chargeable User Identity", draft-~~adrangi-radius~~ietf-radext-chargeable-user-identity-~~02~~04.txt, work in progress.

[27] IETF Draft "EAP lower layer attributes for AAA protocols", <draft-mariblanca-aaa-eap-lla-01.txt>, work in progress

[28] IETF Draft "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)", draft-haverinen-pppext-eap-sim-16.txt, work in progress

[29] IETF Draft "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", draft-arkko-pppext-eap-aka-15.txt, work in progress

**** End of change #1 ****

****** Start of change #2 ******

4.4 Information Element Contents

4.4.1 RADIUS based Information Elements Contents

Table 4.4.1: RADIUS based Information Elements Contents

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
USER ID	This Attribute indicates the identity of the user as defined in 3GPP TS 23.003 [22].	Mandatory	Mandatory	Mandatory	Mandatory	User-Name
RADIUS Client Address	This Attribute indicates the identifying IP Address of the RADIUS Client. It should be unique to the RADIUS Client within the scope of the RADIUS server. More detailed description of the IE can be found in IETF RFC 3580 [15].	Mandatory	NA	NA	NA	NAS-IP Address
Operator Name	Hot Spot Operator Name as defined in IETF Draft draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	NA	NA	Operator Name
Location Name	Location Type of the hot spot operator as defined in IETF Draft draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	NA	NA	Location Name
Location Information	Location information regarding the hotspot operator as defined in IETF Draft draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	NA	NA	Location information
EAP Message	This attribute encapsulates Extensible Authentication Protocol packets so as to allow the NAS to authenticate users via EAP without having to understand the EAP protocol. More detailed description of the IE can be found in IETF RFC 3580 [15].	Mandatory	Mandatory	Mandatory	Mandatory	EAP-Message
Diameter Session ID + 3GPP AAA Server Host AVP + prefix "Diameter"	This attribute is relayed from the 3GPP AAA Proxy to the WLAN-AN when the 3GPP AAA Proxy acts as translation agent. If the WLAN-AN receives such an attribute, it MUST include it in Access Requests.	Conditional	NA	NA	Conditional	State
Diameter Session ID + prefix "Diameter"	This attribute is sent by 3GPP AAA Proxy when acting as a translation agent. If WLAN-AN receives it, is should include it in subsequent accounting messages.	NA	Conditional	NA	NA	Class
State Information	A 3GPP AAA Server using RADIUS may include this attribute in Access Challenges. If the Radius Client in WLAN-AN receives	Conditional	NA	NA	Optional	State

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
	such an attribute, it shall be present in Access-Request that is sent in response to the Access-Challenge. This IE is used when no Diameter-RADIUS translation takes place.					
Session ID	A 3GPP AAA Server using RADIUS shall include this attribute to facilitate charging correlation between accounting and authorization messaging. If the Radius Client in WLAN-AN receives it, it shall be included in subsequent accounting messages. This IE is used when no Diameter-RADIUS translation takes place.	NA	Conditional	NA	NA	Class
Session Alive Time	This Attribute sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt. A more detailed description of the IE can be found in IETF RFC 3580 [15].	NA	Optional	NA	Optional	Session-Time-Out
Charging Duration	This attribute indicates the time between each interim update in seconds for this specific session. A more detailed description of the IE can be found in IETF RFC 2869 [9].	NA	Optional	NA	NA	Acct-Interim-Interval
Termination Action	This Attribute indicates what action the NAS should take when the specified service is completed. More detailed description of the IE can be found in IETF RFC 3580 [15].	NA	Optional	NA	Optional	Termination-Action
Pairwise Master Key (PMK)	This IE is used to carry the Pairwise Master Key. More detailed description of the IE can be found in IETF Draft draft-haverinen-pppext-eap-sim-16 [28] and IETF Draft draft-arkko-pppext-eap-aka-15 [29].	NA	Mandatory	NA	NA	Vendor-Specific (MS-MPPE-Recv-Key)
Message Authenticator	Message Authenticator.	Mandatory	Mandatory	Mandatory	Mandatory	Message Authenticator
WLAN-UE MAC address	Carries the MAC address of the WLAN-UE for verification at the 3GPP AAA Server.	Mandatory	NA	NA	NA	Calling Station ID
Chargeable User Identity	This Attribute shall contain the MSISDN of the user ~~as specified in IETF Draft draft-adrangi-radius-chargeable-user-identity-02 [26]~~. The encoding of the MSISDN is defined in GSMA PRD IR.61 [25].	Optional	Mandatory	NA	NA	Chargeable-User-Id

The parameters listed above as 'mandatory' are only optional in the particular RADIUS (extension) specification in which they are originally defined. However, in order for 3GPP WLAN-IW to function, these attributes shall be passed in messaging over the Wa interface as per the definition in the table. In this sense they are mandatory. In practice, this means that, should any of these parameters labelled 'mandatory' be missing from the RADIUS messaging over Wa, this will result in a higher level failure of WLAN-IW procedures to function properly and consequently in a denial of the RADIUS request (even though this was a valid RADIUS message).

**** End of change #2 ****

**** Start of change #3 ****

4.5.1.1 RADIUS Attributes in accounting messages

Table 4.5.1 gives the information elements included in the accounting messaging exchanged over the Wa interface.

Table 4.5.1: RADIUS based Information Elements Contents

IE NAME	IE description	Accounting Request	Accounting Response	Attribute
USER ID	This Attribute indicates the identity of the user. More detailed description of the IE can be found in IETF RFC 3580 [15] and 3GPP TS 23.234 [4].	Mandatory	Mandatory	User-Name
RADIUS Client Address	This Attribute indicates the identifying IP Address of the RADIUS Client. It should be unique to the RADIUS Client within the scope of the RADIUS server. More detailed description of the IE can be found in IETF RFC 3580 [15].	Mandatory	NA	NAS-IP Address
Acc-Session-ID	According to IETF RFC 2866 [20], this attribute is an accounting ID which uniquely identifies the user's session. If the WLAN AN receives an Access Accept containing a Class attribute with prefix "Diameter", then the Session-ID contained therein is used as the Acc-Session-ID.	Mandatory	Mandatory	Acc-Session-ID
Operator Name	Hot Spot Operator Name as defined in [16].	Mandatory	NA	Operator Name
Location Type	Location Name of the hot spot operator as defined in IETF Draft draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	Location Type
Location Information	Location information regarding the hotspot operator as defined in IETF Draft draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	Location information
Acct.Status Type	Indicates whether this is: (i) Accounting Start. (ii) Stop. (iii) Interim Report. Accounting start indicates that this is the beginning of the user service, Account stop the end.	Mandatory	N/A	Acct.Status Type
Acc-Input-octets	Indicates the number of octets sent by the WLAN UE over the course of the session. According to IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop".	Optional	N/A	Acc-Input-octets
Acc-Output Octets	Indicates the number of octets received by the WLAN-UE. According to IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop".	Optional	N/A	
Acc-Session-Time	This attribute indicates how many seconds the user has received service for.	Conditional. Shall be present if Acct-Status-Type set to Accounting Stop	N/A	Acc-Session-Time
Acc-Input-Packets	Indicates the number of packets sent by the WLAN UE over the course of the session. According to IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop"	Optional	N/A	Acc-Input-Packets
Acc-Output-Packets	Indicates the number of packets received by the WLAN-UE over the course of the session. According to IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop".	Optional	N/A	Acc-Output-Packets
Acc-Terminate-Cause	Indicates how the session was stopped. Cause values are as per specified in IETF	Conditional. Shall be present if Acct-	N/A	Acc-Terminate-Cause

IE NAME	IE description	Accounting Request	Accounting Response	Attribute
	RFC 3580 [15].	Status-Type set to "Accounting Stop".		
Chargeable User Identity	This Attribute shall contain the MSISDN of the user ~~as specified in IETF Draft draft-adrangi-radius-chargeable-user-identity-02 [26]~~. The encoding of the MSISDN is defined in GSMA PRD IR.61 [25].	Mandatory	NA	Chargeable-User-Id
Event Time Stamp	Number of second elapsed since January 1st 1970. UTC time.	Mandatory	NA	Event-Time-Stamp
Session ID	This attribute is used to link related authentication and accounting sessions and should be included unmodified to accounting request messages. This IE is used when no Diameter-RADIUS translation takes place.	Optional	NA	Class

The parameters listed above as "mandatory" are only optional in the particular RADIUS (extension) specification in which they are originally defined. However, in order for 3GPP WLAN-IW to function, these attributes shall be passed in messaging over the Wa interface as per the definition in the table. In this sense they are mandatory. In practice, this means that, should any of these parameters labelled "mandatory" be missing from the RADIUS messaging over Wa, this will result in a higher level failure of WLAN-IW procedures to function properly and consequently in a denial of the RADIUS request (even though this was a valid RADIUS message).

**** End of change #3 ****

**** Start of change #4 ****

5.2 Protocols

The Wd reference point shall use only a single AAA protocol per WLAN session. RADIUS or Diameter based protocols shall be used, respective of which protocol the WLAN AN is using.

The Wd protocol reference point shall contain the following protocols:

1) RADIUS, as defined in IETF RFC 2865 [17], including the following extensions:

   - IETF RFC 2869 [9], which provides RADIUS extensions to support the transport of EAP frames over RADIUS.

   - IETF Draft "Carrying Location Objects in RADIUS", draft-ietf-geopriv-radius-lo-01 [16], which provides RADIUS Extensions for Public WLAN ~~are~~ to identify uniquely the owner and location of the WLAN.

   - IETF RFC 3576 [13], which provides RADIUS extensions to supports, amongst other capabilities, the capability to immediately disconnect a user from the WLAN AN.

   - GSMA PRD IR.61 [~~xx~~25], which provides a Visited-operator-id attribute and a detailed encoding of a chargeable user identity (e.g. MSISDN or IMSI) for the ~~a~~ RADIUS Chargeable-User-Id attribute ~~to carry a chargeable user identity (e.g. MSISDN or IMSI) from Home PLMN to Visited PLMN~~.

   - IETF Draft "Chargeable User Identity", draft-ietf-radext-chargeable-user-identity-04.txt, which provides RADIUS Extensions for carrying a chargeable user identity from Home PLMN to Visited PLMN.

2) Diameter Base, as defined in IETF RFC 3588 [7], as well as IETF Draft "Diameter EAP Application" [8], which provides a Diameter application to support the transport of EAP (IETF RFC 2284 [10] and IETF Draft "EAP" [11]) frames over Diameter. In addition, Diameter Base (IETF RFC 3588 [7]) and NASREQ IETF Draft draft-ietf-aaa-diameter-nasreq-12 [12] specify the accounting messaging to be exchanged.

The 3GPP AAA Proxy and the 3GPP AAA Server shall support both 1) and 2) over the Wd reference point. The 3GPP AAA Proxy, depending on the WLAN ANs characteristics, shall use either 1) or 2) over the Wd reference point. See subclause 5.3 for more information of when either 1) or 2) is used.

The Application-Id to be advertised over Wd reference point corresponds to the EAP or Diameter Base Protocol Application-Id, depending on the command sent over Wd.

**** End of change #4 ****

**** Start of change #5 ****

5.5.4 RADIUS based Information Elements Contents for Authentication and Authorization

Table 5.5.4.1: RADIUS based Information Elements Contents

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
RADIUS Client Address	This Attribute indicates the identifying IP Address of the RADIUS Client. It should be unique to the RADIUS Client within the scope of the RADIUS server. More detailed description of the IE can be found in IETF RFC 3580 [15].	Mandatory	NA	NA	NA	NAS-IP Address
USER ID	This Attribute indicates the identity of the user to be authenticated. More detailed description of the IE can be found in IETF RFC 3580 [15] and 3GPP TS 23.234 [4].	Mandatory	Mandatory	Mandatory	Mandatory	User-Name
Operator Name	Hot Spot Operator Name as defined in IETF draft-ietf-geopriv-radius-lo-01.txt [16].	Mandatory	NA	NA	NA	Operator-Name
Location Type	Location Name of the hot spot operator as defined in IETF draft-ietf-geopriv-radius-lo-01.txt [16].	Mandatory	NA	NA	NA	Location-Type
Location Information	Location information regarding the hotspot operator as defined in IETF draft-ietf-geopriv-radius-lo-01.txt [16].	Mandatory	NA	NA	NA	Location-information
EAP Message	This attribute encapsulates Extensible Authentication Protocol packets so as to allow the NAS to authenticate users via EAP without having to understand the EAP protocol. More detailed description of the IE can be found in IETF RFC 3580 [15].	Mandatory	Mandatory	Mandatory	Mandatory	EAP-Message
State information	This attribute may be sent by the 3GPP AAA server to the WLAN-AN . If the RADIUS client in the WLAN-AN receives such an attribute, it shall be included in subsequent Access Requests.	Conditional	NA	NA	Optional	State
Session ID	This attribute is sent by 3GPP AAA server to the visited network. If the RADIUS client in the WLAN-AN receives it, it should be included in subsequent accounting messages.	NA	Mandatory	NA	NA	Class
Session Alive Time	This Attribute sets the maximum number of seconds of service to be provided to the user before termination of the session or	NA	Optional	NA	Optional	Session-Time-Out

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
	prompt. A more detailed description of the IE can be found in IETF RFC 3580 [15].					
Charging Duration	This attribute indicates the time between each interim update in seconds for this specific session. A more detailed description of the IE can be found in IETF RFC 2869 [9].	NA	Optional	NA	NA	Acct-Interim-Interval
Termination Action	This Attribute indicates what action the NAS should take when the specified service is completed. More detailed description of the IE can be found in IETF RFC 3580 [15].	NA	Optional	NA	Optional	Termination-Action
Pairwise Master Key (PMK)	This IE is used to carry the Pairwise Master Key. More detailed description of the IE can be found in IETF Draft draft-haverinen-pppext-eap-sim-16 [28] and IETF Draft draft-arkko-pppext-eap-aka-15 [29].	NA	Mandatory	NA	NA	Vendor-Specific (MS-MPPE-Recv-Key)
Master Session Key (MSK)	This IE is used to carry the Master Session Key for WLAN 3GPP IP Access. More detailed description of the IE can be found in IETF Draft draft-haverinen-pppext-eap-sim-16 [xx] and IETF Draft draft-arkko-pppext-eap-aka-15 [yy].	NA	Mandatory	NA	NA	Vendor-Specific (MS-MPP-Recv-Key) and Vendor-Specific (MS-MPP-Send-Key)
Message Authenticator	Message Authenticator.	Mandatory	Mandatory	Mandatory	Mandatory	Message-Authenticator
WLAN-UE MAC address	Carries the MAC address of the WLAN-UE for verification at the 3GPP AAA Server.	Mandatory	NA	NA	NA	Calling-Station-ID
Chargeable User Identity	This Attribute shall contain the MSISDN of the user ~~as specified in IETF Draft draft-adrangi-radius-chargeable-user-identity-02 [26]~~. The encoding of the MSISDN is defined in GSMA PRD IR.61 [25].	Optional	Mandatory	NA	NA	Chargeable-User-Id
Visited Operator Identity	Identifies the VPLMN as specified in GSMA PRD IR.61 [25]	Mandatory	NA	NA	NA	Vendor-Specific (Visited-Operator-Id)

The parameters listed above as 'mandatory' are only optional in the particular RADIUS (extension) specification in which they are originally defined. However, in order for 3GPP WLAN-IW to function, these attributes shall be passed in messaging over the Wd interface as per the definition in the table. In this sense they are mandatory. In practice, this means that, should any of these parameters labelled 'mandatory' be missing from the RADIUS messaging over Wd, this will result in a higher level failure of WLAN-IW procedures to function properly and consequently in a denial of the RADIUS request (even though this was a valid RADIUS message).

**** End of change #5 ****

**** Start of change #6 ****

5.5.5 RADIUS based Information Elements Contents for Accounting

Table 5.5.5.1: RADIUS based Information Elements Contents

IE NAME	IE description	Accounting Request	Accounting Response	Attribute
USER ID	This Attribute indicates the identity of the user. More detailed description of the IE can be found in IETF RFC 3580 [15] and 3GPP TS 23.234 [4].	Mandatory	Mandatory	User-Name
RADIUS Client Address	This Attribute indicates the identifying IP Address of the RADIUS Client. It should be unique to the RADIUS Client within the scope of the RADIUS server. More detailed description of the IE can be found in IETF RFC 3580 [15].	Mandatory	NA	NAS-IP Address
Acc-Session-ID	According to IETF RFC 2866 [20], this attribute is an accounting ID which uniquely identifies the user's session.	Mandatory	Mandatory	Acc-Session-ID
Operator Name	Hot Spot Operator Name as defined in IETF draft-ietf-geopriv-radius-lo-01.txt [16].	Mandatory	NA	Operator Name
Location Type	Location Name of the hot spot operator as defined in IETF draft-ietf-geopriv-radius-lo-01.txt [16].	Mandatory	NA	Location Type
Location Information	Location information regarding the hotspot operator as defined in IETF draft-ietf-geopriv-radius-lo-01.txt [16].	Mandatory	NA	Location-information
Acct.Status Type	Indicates whether this is: (i) Accounting Start. (ii) Stop. (iii) Interim Report. Accounting start indicates that this is the beginning of the user service, Account stop the end.	Mandatory	N/A	Acct.Status Type
Acc-Input-octets	Indicates the number of octets sent by the WLAN UE over the course of the session. According to IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop".	Optional	N/A	Acc-Input-octets
Acc-Output Octets	Indicates the number of octets received by the WLAN-UE. According to IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop".	Optional	N/A	Acc-Output-Octets
Acc-Session-Time	This attribute indicates how many seconds the user has received service for.	Conditional. Shall be present if Acct-Status-Type set to Accounting Stop	N/A	Acc-Session-Time
Acc-Input-Packets	Indicates the number of packets sent by the WLAN UE over the course of the session. According to IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop"	Optional	N/A	Acc-Input-Packets
Acc-Output-Packets	Indicates the number of packets received by the WLAN-UE over the course of the session. According to IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop".	Optional	N/A	Acc-Output-Packets
Acc-Terminate-Cause	Indicates how the session was stopped. Cause values are as per specified in IETF RFC 3580 [15].	Conditional. Shall be present if Acct-Status-Type set to "Accounting Stop".	N/A	Acc-Terminate-Cause
Event Time Stamp	Number of second elapsed since January 1st 1970. UTC time.	Mandatory	NA	Event-Time-Stamp
Chargeable User Identity	This attribute shall contain the MSISDN of	Mandatory	NA	Chargeable-

IE NAME	IE description	Accounting Request	Accounting Response	Attribute
	the user ~~as specified in IETF Draft draft-adrangi-radius-chargeable-user-identity-02 [26]~~. The encoding of the MSISDN is defined in GSMA PDR IR.61 [25].			User-Id
Visited Operator Identity	Identifies the VPLMN as specified in GSMA PRD IR.61 [25]	Mandatory	NA	Vendor-Specific (Visited-Operator-Id)
Session ID	This attribute is used to link related authentication and accounting sessions and should be included unmodified to accounting request messages.	Optional	NA	Class

The parameters listed above as 'mandatory' are only optional in the particular RADIUS (extension) specification in which they are originally defined. However, in order for 3GPP WLAN-IW to function, these attributes shall be passed in messaging over the Wd interface as per the definition in the table. In this sense they are mandatory. In practice, this means that, should any of these parameters labelled 'mandatory' be missing from the RADIUS messaging over Wd, this will result in a higher level failure of WLAN-IW procedures to function properly and consequently in a denial of the RADIUS request (even though this was a valid RADIUS message).

**** End of change #6 ****

3GPP TSG-CT WG4 Meeting #27 **C4-050765**
Cancun, MEXICO. 25th to 29th April 2005. **Rev. C4-050613**

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.008** **CR** **145** ⌘**rev** **2** ⌘ Current version: **6.5.0** ⌘

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

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

Title:	⌘	Corrections on WLAN UE Remote IP Address
Source:	⌘	NEC
Work item code:	⌘	WLAN-IW
Date:	⌘	14/04/2005
Category:	⌘	**F**
Release:	⌘	REL-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*
Rel-7 *(Release 7)*

Reason for change:	⌘	The WLAN UE Remote IP Address are defined twice in table 5.5. We understand 2 definisions are as follows. • The first entry that corresponds to the section 3B.1.10 stands for subscriber data. • The second entry that corresponds to the section 3B.5.4.4 stands for WLAN UE Remote addresses as the subject for Operator Determined Barring.
Summary of change:	⌘	• Rename the second entry (3B.5.4.4) to the Static WLAN UE Remote IP address • In the section 3.B.5.4.4, the referred section 3B.1.12 is changed to section 3B.1.10.
Consequences if not approved:	⌘	Since one entry name is applied to two different information, this causes misleading.

Clauses affected:	⌘	3B.5.4.4, 5.5

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	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 ******

3B.5.4.4 Static WLAN UE Remote IP Address

WLAN UE IP Address field identifies the IPv4/IPv6 address that the operator has statically assigned to the WLAN UE. See subclause 3B.1.1~~2~~0.

****** Next modified section ******

5.5 I-WLAN Service Data Storage

Table 5.5: Overview of data used for I-WLAN services

PARAMETER	Subclause	HSS	3GPP AAA Server	3GPP AAA Proxy	PDG	WAG	TYPE
IMSI	3B.1.1	M	M				P
MSISDN	3B.1.2	M	M	M	M	M	P
W-APN	3B.1.3	M	M		M		P
List of authorized visited network identifiers	3B.1.4	M					P
3GPP AAA Proxy Identifier	3B.1.5		M		M	M	T
3GPP AAA Server Name	3B.1.6	M		M	M	C	T
Serving PDG List	3B.1.7		M	M			P
Serving WAG	3B.1.8		M	M	M		P
WLAN UE Local IP address	3B.1.9				M	M	T
WLAN UE Remote IP address	3B.1.10	C	C		M		P
User Status	3B.2.1		M				T
RAND, SRES, Kc	3B.3.1	M	M		-		T
RAND, XRES CK, IK, AUTN	3B.3.2		M		-		T
Master Key (MK)	3B.3.3		M				T
Transient EAP Keys (TEKs)	3B.3.3		M				T
Session Identifier	3B.4.1		M				T
Session-Timeout	3B.4.2		C				P
Quota	3B.4.3		C				P
WLAN Access	3B.5.1	M					P
WLAN Tunnelling	3B.5.2	M					P
WLAN Direct IP Access	3B.5.3	M					P
W APN Authorised	3B.5.4	M					P
W APN Identifier	3B.5.4.1						P
W-APN Barring Type	3B.5.4.2	M					P
W-APN Charging Data	3B.5.4.3	C			C		P
Static WLAN UE Remote IP Address	3B.5.4.4	C			P		P
Access Independence Flag	3B.5.5	M					P
I-WLAN Access Type	3B.5.6	M					P
Max Requested Bandwidth	3B.6.1		P		T		P
Routing Policy	3B.6.2				C	C	T
Charging Data	3B.7.1	M			M		P
Charging Characteristics	3B.7.1.1	M	-		M		P
Primary OCS Charging Function Name	3B.7.2	M			M		P
Secondary OCS Charging Function Name	3B.7.3	M			M		P
Primary Charging Collection Function Name	3B.7.4	M			M		P
Secondary Charging Collection Function Name	3B.7.5	M			M		P

3GPP TSG-CT WG4 Meeting #27 **C4-050766**
Cancun, Mexico. 25th to 29th April 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **060** ⌘ **rev** **2** ⌘ Current version: **6.2.0** ⌘

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

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

Title:	⌘	Missing functionality in stage 3
Source:	⌘	Huawei, France Télécom
Work item code:	⌘	WLAN-IW
Date:	⌘	03/02/2005
Category:	⌘	**B**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	In the 23.234, the function of subscriber profile update has been described in section 7.3.0 and 7.3.1 but in 29.234, there are not corresponding words to describe it. This CR is proposed to align the function in Stage2 and Stage3, and it is the complementarity of "HSS Initiated Update of User Profile" procedure described in clause 6.3.3.2. Moreover, additional corrections are proposed in order to align the stage 3 specification with the Stage 2 requirements on authorization management. **Essential Correction**
Summary of change:	⌘	Supply subscriber profile updating descriptions in the relevant sections.
Consequences if not approved:	⌘	Stage 3 functionality pertaining to stage 2 is missing

Clauses affected:	⌘	4.3, 4.4.2, 5.2, 5.4, 5.5, 8.2, 8.3, 8.4

Other specs affected:	⌘	Y	N		⌘
			X	Other core specifications	
			X	Test specifications	
			X	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.

*******Beginning of the change******

4.3 Procedures Description

4.3.1 WLAN Access Authentication and Authorization

This procedure is used to transport over RADIUS or Diameter, the WLAN Access (Re)Authentication and Authorization between the WLAN AN and the 3GPP AAA Proxy.

Diameter usage in Wa:

- This procedure is mapped to the Diameter-EAP-Request and Diameter-EAP-Answer command codes specified in [8] The Diameter-EAP-Request Message shall contain the following information elements.
- For reauthentication procedures, the messaging described below is reused.

Table 4.3.1.1: WLAN Access Authentication and Authorization request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.
EAP payload	EAP-payload	M	Encapsulated EAP payload used for UE-3GPP AAA Server mutual authentication
Authentication Request Type	Auth--Request-Type	M	Defines whether the user is to be authenticated only, authorized only or both.~~authentication is required or authorization.~~ AUTHORIZE_AUTHENTICATE~~_ONLY~~ is required in this case.
NAS-IP address	NAS-IP Address	C	IP address of the hot-spot
NAS-Ipv6 address	NAS-Ipv6 address	C	Ipv6 address of the hot-spot
WLAN UE MAC address	Calling Station-ID	M	Carries the MAC address of the WLAN-UE.

The Diameter-EAP response message shall contain the following.

Table 4.3.1.2: WLAN Acess Authentication and Authorization response

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.
EAP payload	EAP payload	M	Encapsulated EAP payload used for UE- 3GPP AAA Server mutual authentication
Result code	Result Code	M	Result of the operation. Result codes are as per in NASREQ. 1xxx should be used for multi-round, 2xxx for success.
Session Alive Time	Session Alive Time	O	Max no of seconds the user session should remain active
Accounting Interim - Interval	Accounting Interim - Interval	O	Charging duration
Encryption-Key	EAP-Master-Session-Key	C	Shall be sent if Result Code is set to "Success". This is defined in Diameter EAP specification [8]

RADIUS usage in Wa:

- This procedure is mapped to the RADIUS Access Request, RADIUS Access Challenge, RADIUS Access Accept and RADIUS Access Reject specified in RFC 3579 [14].

See Annex A.1.1 for signalling flow reference.

4.3.2 Immediate Purging of a User from WLAN access

This procedure is used to communicate between the WLAN AN and the 3GPP AAA Proxy that the 3GPP AAA Server has decided that a specific WLAN-UE shall be disconnected from accessing the WLAN interworking service. The procedure is Diameter or RADIUS based. The RADIUS case is only considered if the WLAN AN and the 3GPP AAA Proxy support RFC 3576 [13]. WLAN ANs supporting RADIUS RFC 2865 [17] but not supporting RFC 3576 [13] do

not have the required capabilities to react to server-initiated messages, therefore "Immediate purging of a user from WLAN Access" procedure shall not be performed towards clients located in this kind of WLAN AN.

Diameter usage in Wa:

- This procedure is mapped to the Diameter command codes Diameter-Abort-Session-Request and Diameter-Abort-Session-Answer specified in RFC 3588 [7]. Information element content for these messages are shown in tables 4.3.2.1 and 4.3.2.2.

Table 4.3.2.1: Information Elements passed in ASR message

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.

Table 4.3.2.2: Information Elements passed in ASA message

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.
Result-Code	Result-Code	M	Informs of success of procedure

See Annex A.1.2 for signalling flow reference.

RADIUS usage in Wa:

- This procedure is mapped to the RADIUS messages Disconnect-Request and Disconnect-Response specified in RFC 3576 [13].

4.3.3 Ending a Session

Session termination is initiated when the WLAN-AN needs to inform the 3GPP AAA Server of the WLAN-UEs disconnection from the hot-spot. This occurs via the Session Termination Request (STR) and Session Termination Answer commands (STA) from the base protocol RFC 3588 [7]. Information elements to be carried in the STR, STA messages are shown in tables 4.4.3.1 and 4.4.3.2.

Table 4.3.3.1: Information Elements passed in STR message

Information element name	Mapping to Diameter AVP	Cat.	Description
Username NAI	User-Name	M	This information element contains the identity of the user.
Termination-Cause	Termination Cause	M	Reason for termination of the session.

Table 4.3.3.2: Information Elements passed in STA message

Information element name	Mapping to Diameter AVP	Cat.	Description
Username NAI	User-Name	M	This information element contains the identity of the user.
Result Code	Result-Code	M	Informs of success or failure of the procedure.

4.3.x WLAN Access Authorization Information Update Procedure

The~~is~~ WLAN access authorization information update procedure is used to modify the authorization parameters provided to the WLAN AN. This procedure is invoked by the 3GPP AAA Server when the subscriber's access authorization information has been modified and needs to be sent to the WLAN AN. The WLAN access authorization information update procedure shall trigger a new WLAN access authentication and authorization procedure towards to the WLAN-UE.-This may happen due to a modification of WLAN subscriber profile in the HSS.

The procedure is Diameter or RADIUS based.

Diameter usage in Wa:

This procedure is performed in two steps:

- The 3GPP AAA server issues an unsolicited re-authentication and re-authorization request towards the WLAN AN. Upon receipt of such a request, the WLAN AN shall respond to the request and indicate the disposition of the request. This procedure is mapped to the Diameter command codes Re-Auth-Request and Re-Auth-Answer specified in RFC 3588 [7]. Information element content for these messages are shown in tables 4.3.4.x and 4.3.4.y.

- Receiving the re-authentication and re-authorization request, the WLAN AN shall initiate a re-authentication procedure towards the WLAN-UE and shall then invoke the WLAN access authentication and authorization procedure as described in the section 4.3.1. Information element content for these messages are shown in tables 4.3.1.1 and 4.3.1.2.

Table 4.3.4.x: Re-Authentication and Re-Authorization request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.
Re-Auth Request Type	Re-Auth–Request-Type	M	Defines whether the user is to be re-authenticated only, re-authorized only or both. AUTHORIZE_AUTHENTICATE is required in this case.
Routing Information	Destination-Host	M	This information element is obtained from the Origin-Host AVP, which was included in a previous command received from the WLAN AN.

Table 4.3.4.y: Re-Authentication and Re-Authorization response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Wa errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
User Identity	User-Name	M	This information element contains the identity of the user.

RADIUS usage in Wa:

- This procedure is mapped to the RADIUS messages CoA-Request and CoA-Response specified in RFC 3576 [13].

*******Beginning of the next change*******

4.4.2 Diameter based Information Elements Contents

Editors Note: operator name, location name and location information AVPs should be included once RADIUS extensions working group have agreed with Diameter working groups how this is done.

4.4.2.1 DER and DEA Commands

ABNF for the DER and DEA messages are given below:

```
<Diameter-EAP-Request> ::= < Diameter Header: 268, REQ, PXY >
    < Session-Id >
    { Auth-Application-Id }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    { Auth-Request-Type }
    { EAP-Payload }
    [ Destination-Host ]
```

```
    [ User-Name ]
    [ NAS-IP-Address ]
    [ NAS-IPv6-Address ]
    [Calling Station-ID ]
    * [ Proxy-Info ]
    * [ Route-Record ]
    * [ AVP ]
```

For the DEA, the following are necessary:

```
<Diameter-EAP-Answer> ::= < Diameter Header: 268, PXY >
    < Session-Id >
    { Auth-Application-Id }
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    { Auth-Request-Type }
    [ EAP-Payload ]
    [ User-Name ]
    [ Session-Timeout ]
    [ Accounting-Interim-Interval ]
    [ EAP-Master-Session-Key]
    * [ Proxy-Info ]
    * [ AVP ]
```

4.4.2.2 Abort Session Request and Answer AVPs

ABNF for the ASR and ASA commands are as follows:

```
<ASR>  ::= < Diameter Header: 274, REQ, PXY >
    < Session-Id >
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    { Destination-Host }
    { Auth-Application-Id }
    [ User-Name ]
    [ Origin-State-Id ]
    * [ Proxy-Info ]
    * [ Route-Record ]
     *[ AVP ]

<ASA>  ::= < Diameter Header: 274, PXY >
    < Session-Id >
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    [ User-Name ]
    [ Origin-State-Id ]
    [ Error-Message ]
    [ Error-Reporting-Host ]
    * [ Failed-AVP ]
    * [ Redirected-Host ]
    [ Redirected-Host-Usage ]
     [ Redirected-Max-Cache-Time ]
    * [ Proxy-Info ]
    * [ AVP ]
```

4.4.2.3 Session Termination Request and Answer AVPs

```
<STR> ::= < Diameter Header: 275, REQ, PXY >
    < Session-Id >
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    { Auth-Application-Id }
    { Termination-Cause }
    [ User-Name ]
    [ Destination-Host ]
    * [ Class ]
    [ Origin-State-Id ]
    * [ Proxy-Info ]
    * [ Route-Record ]
    * [ AVP ]
```

4.4.2.x Re-Auth Request and Answer AVPs

ABNF for the RAR/RAA commands are as follows:

```
<RAR>  ::= < Diameter Header: 258, REQ, PXY >
           < Session-Id >
          { Origin-Host }
          { Origin-Realm }
          { Destination-Realm }
          { Destination-Host }
          { Auth-Application-Id }
          { Re-Auth-Request-Type }
          [ User-Name ]
          [ Destination-Host ]
          [ Origin-State-Id ]
          * [ Proxy-Info ]
          * [ Route-Record ]
          * [ AVP ]

<RAA>  ::= < Diameter Header: 258, PXY >
           < Session-Id >
          { Result-Code }
          { Origin-Host }
          { Origin-Realm }
          [ User-Name ]
          [ Origin-State-Id ]
          [ Error-Message ]
          [ Error-Reporting-Host ]
          * [ Failed-AVP ]
          * [ Redirect-Host ]
          [ Redirect-Host-Usage ]
          [ Redirect-Host-Cache-Time ]
          * [ Proxy-Info ]
          * [ AVP ]
```

*******Beginning of the next change******

5.2 Protocols

The Wd reference point shall use only a single AAA protocol per WLAN session. RADIUS or Diameter based protocols shall be used, respective of which protocol the WLAN AN is using.

The Wd protocol reference point shall contain the following protocols:

1) RADIUS, as defined in IETF RFC 2865 [17], including the following extensions:

   - IETF RFC 2869 [9], which provides RADIUS extensions to support the transport of EAP frames over RADIUS.

   - IETF Draft "Carrying Location Objects in RADIUS", draft-ietf-geopriv-radius-lo-01 [16], which provides RADIUS Extensions for Public WLAN are to identify uniquely the owner and location of the WLAN.

   - IETF RFC 3576 [13], which provides RADIUS extensions to supports, amongst other capabilities, the capability to immediately disconnect a user from the WLAN AN.

   - GSMA PRD IR.61 [xx], which provides a RADIUS Chargeable-User-Id attribute to carry a chargeable user identity (e.g. MSISDN or IMSI) from Home PLMN to Visited PLMN.

2) Diameter Base, as defined in IETF RFC 3588 [7], as well as IETF Draft "Diameter EAP Application" [8], which provides a Diameter application to support the transport of EAP (IETF RFC 2284 [10] and IETF Draft "EAP" [11]) frames over Diameter. In addition, Diameter Base (IETF RFC 3588 [7]) and NASREQ IETF Draft draft-ietf-aaa-diameter-nasreq-12 [12] specify the accounting messaging to be exchanged.

The 3GPP AAA Proxy and the 3GPP AAA Server shall support both 1) and 2) over the Wd reference point. The 3GPP AAA Proxy, depending on the WLAN ANs characteristics, shall use either 1) or 2) over the Wd reference point. See subclause 5.3 for more information of when either 1) or 2) is used.

The Application-Id to be advertised over Wd reference point corresponds to the EAP, NASREQ or Diameter Base Protocol Application-Id, depending on the command sent over Wd.

*******Beginning of the next change******

5.4 Procedures description

5.4.1 WLAN Access Authentication and Authorization

This procedure is used to transport the WLAN Access Authentication and Authorization information between the 3GPP AAA Proxy and the 3GPP AAA Server over Diameter.

Diameter usage in Wd:

This procedure is mapped to the Diameter-EAP-Request and Diameter-EAP-Answer command codes specified in [8] tables 5.4.1.1 and 5.4.1.2 show the information elements that should be exchanged across Wd.

Table 5.4.1.1: Diameter EAP Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User Name	M	This information element shall contain the identity of the user
EAP payload	EAP payload	M	Encapsulated EAP payload used for WLAN-UE/-3GPP AAA Server mutual authentication
Authentication Request Type	Auth–Request-Type	M	Defines whether the user is to be re-authenticated only, re-authorized only or both.~~authentication or authentication procedure is requested~~. AUTHORIZE_AUTHENTICATE~~_ONLY~~ is required in this case.
NAS-IP address	NAS-IP Address	C	IP address of the hot-spot
NAS-Ipv6 address	NAS-Ipv6 address	C	IP~~p~~v6 address of the hot-spot
Visited-Network-Identifier	Visited-Network-Identifier	C	Identifies the VPLMN and shall be present during the first DER message of either authentication or reauthentication sent by the 3GPP AAA Proxy to 3GPP AAA Server.
WLAN UE MAC address	Calling Station-ID		Carries the MAC address of the WLAN-UE.

Editors Note: RADIUS Extensions for Location ID etc should be added once these have been defined within Diameter schema.

Table 5.4.1.2: Diameter EAP answer message

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User Name	M	This information element contains the identity of the user.
EAP payload	EAP payload	M	Encapsulated EAP payload used for UE-3GPP AAA Server mutual authentication
Result code	Result Code	M	Result of the operation. Result code as per definition in NASREQ.1xxx shall be used for multi-round, 2xxx for success.
Session Alive Time	Session-Timeout	O	Max no of seconds the user session should remain active
Accounting Interim-Interval	Accounting Interim-Interval	O	Charging duration
Subscription-ID	Subscription-ID	C	This AVP shall contain the MSISDN of the user. This AVP shall be present if the result code is set to "Success", 2xxx.

RADIUS usage in Wd:

- This procedure is mapped to the RADIUS Access Request, RADIUS Access Challenge, RADIUS Access Accept and RADIUS Access Reject specified in RFC 3579 [14].

5.4.2 Immediate Purging of a User from WLAN access

This procedure is used to communicate between the 3GPP AAA Proxy and the 3GPP AAA Server that the 3GPP AAA Server has decided that a specific WLAN-UE shall be disconnected from accessing the WLAN interworking service. The procedure is Diameter or RADIUS based.

Diameter usage in Wd:

- This procedure is mapped to the Diameter command codes Diameter-Abort-Session-Request and Diameter-Abort-Session-Answer specified in RFC 3588 [7]. Information elements are as per described in section 6.4.2.

RADIUS usage in Wd:

- This procedure is mapped to the RADIUS messages Disconnect-Request and Disconnect-Response specified in RFC 3576 [13].

5.4.3 Ending a Session

Session termination occurs when a user de-registers from the 3GPP AAA Server. This occurs via the Session Termination Request (STR) and Session Termination Answer commands (STA), defined in the base protocol [8]. Information elements are as per described in subclause 6.4.3.

5.4.x Authorization Information Update Procedure

The authorization information update procedure is used in roaming case to modify the authorization parameters provided either to the WLAN AN or to a PDG located in the visited network. This procedure is invoked by the 3GPP AAA Server and is used to communicate with the WLAN AN or the PDG through the 3GPP AAA proxy.

The procedure is Diameter or RADIUS based.

- Diameter usage in Wd:

  - If the 3GPP AAA server issues an unsolicited re-authentication and/or re-authorization request towards the WLAN AN, the 3GPP AAA proxy shall forward the request to the WLAN AN, which triggers the WLAN access authentication and authorization information update procedure described in the section 4.3.x.

  - If the 3GPP AAA server issues an unsolicited re-authentication and/or re-authorization request towards the PDG located in the visited network, the 3GPP AAA proxy shall forward the request to the PDG, which triggers the access and service authorization information update procedure described in the section 8.3.x.

RADIUS usage in Wd:

- The Wd interface is used to transport the RADIUS messages CoA-Request and CoA-Response only for communication between the WLAN AN and the 3GPP AAA server. These messages are specified in RFC 3576 [13].

*******Beginning of the next change******

5.5 Information Elements Contents

5.5.1 Authentication Procedures

ABNF for the Wd Diameter EAP Request/Ansewer messages are given below:

<Diameter-EAP-Request> ::= < Diameter Header: 268, REQ, PXY >
< Session-Id >
{ Auth-Application-Id }
{ Origin-Host }

{ Origin-Realm }
{ Destination-Realm }
{ Auth-Request-Type }
{ EAP-Payload }
[Destination-Host]
[User-Name]
[NAS-IP-Address]
[NAS-IPv6-Address]
[Calling Station-ID]
[Visited-Network-Identifier]
* [Proxy-Info]
* [Route-Record]
* [AVP]

For the DEA, the following are necessary:

<Diameter-EAP-Answer> ::= < Diameter Header: 268, PXY >
< Session-Id >
{ Auth-Application-Id }
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
{ Auth-Request-Type }
[EAP-Payload]
[User-Name]
[Subscription-ID]
* [Proxy-Info]
* [AVP]

5.5.2 Abort Session Requests and Answer AVPs

ABNF for the ASR and ASA commands on the Wd interface are identical to those on the Wa interface described in section 4.4.2.2

5.5.3 Session Termination Request and Answer AVPs

ABNF for the STR and STA commands on the Wd interface are identical to those on the Wa interface described in section 4.4.2.2

5.5.x Authorization Information Update Procedure~~AVPs~~

ABNF for the RAR and RAA commands on the Wd interface are identical to those described in section 4.4.2.x

ABNF for the AAR/AAA commands on the Wd interface are identical to those described in section 8.4.2

*******Beginning of the next change******

8.2 Protocols

Diameter EAP application is used for authentication of the user. In this case, the PDG shall act as the NAS, as described in 3GPP TS 33.234 [18].For authorization and other Wm functionalities, NASREQ and base protocol procedures are used.

The Application-Id to be advertised over Wm reference point corresponds to the EAP, NASREQ or Diameter Base Protocol Application-Id, depending on the command sent over Wm.

*******Beginning of the next change******

8.3 Procedures Description

[Skipped]

8.3.x Access and Service Authorization information Update Procedure

This procedure is used between the 3GPP AAA Server and the PDG and is used to modify the authorization parameters provided to the PDG. This may happen due to a modification of WLAN subscriber profile in the HSS

This procedure is performed in two steps:

- The 3GPP AAA server issues an unsolicited re-authentication and/or re-authorization request towards the PDG. Upon receipt of such a request, the PDG shall respond to the request and indicate the disposition of the request. This procedure is mapped to the Diameter command codes Re-Auth-Request and Re-Auth-Answer specified in RFC 3588 [7]. Information element content for these messages are shown in tables 8.3.x.1 and 8.3.x.2.

- Receiving the re-authentication and re-authorization request, the PDG shall initiate a re-authentication and/or re-authorization procedure towards the WLAN-UE and shall then invoke the authentication and/or authorization procedure as described in the sections 8.2.1 and 8.3.2. Information element content for these messages are shown in tables 8.3.2.1 and 8.3.2.2.

Table 8.3.x.1: Access and Service Authorization Information Update request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.
Re-Auth Request Type	Re-Auth–Request-Type	M	Defines whether the user is to be re-authenticated only, re-authorized only or both. If it indicates AUTHENTICATE_ONLY, the PDG shall just perform an authentication procedure as described in section 8.2.1. If it indicates AUTHORIZE_ONLY, the PDG shall just perform an autorization procedure as described in section 8.2.2. If it indicates AUTHORIZE_AUTHENTICATE, the PDG shall perform both authentication and authorization.
Routing Information	Destination-Host	M	This information element is obtained from the Origin-Host AVP, which was included in a previous command received from the PDG.

Table 8.3.x.2: Access and Service Authorization information Update response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Wm errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
User Identity	User-Name	M	This information element contains the identity of the user.

8.3.x.1 Detailed behaviour

The 3GPP AAA server shall make use of this procedure to indicate and update relevant service authorization information in the PDG.

The PDG shall overwrite, for the subscriber identity indicated in the request, current information with the information received from the 3GPP AAA server. A deactivation of service may be initiated if the subscriber lost the authorization of the activated service.

*******Beginning of the next change******

8.4 Information Element Contents

[Skipped]

8.4.x Access and Service Authorization Information Update Procedure

ABNF for the RAR/RAA commands on the Wm interface are identical to those described in section 4.4.2.x.

ABNF for the AAR/AAA commands on the Wm interface are identical to those described in section 8.4.2

******* **end of the changes********

3GPP TSG-CT WG4 Meeting #27
Cancun, Mexico, 25th – 29th April 2005

C4-050864

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **061** ⌘ **rev** **2** ⌘ Current version: **6.2.0** ⌘

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

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

Title:	⌘	Pr Interface for Presence via I-WLAN
Source:	⌘	Huawei, Lucent, China Mobile
Work item code:	⌘	WLAN-IW
Date:	⌘	21/03/2005
Category:	⌘	**B**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change:	⌘	The Pr interface needs to be specified. As per the stage 2 specification 23.141, Pr interface is described as follows: 4.3.12 Reference point Presence Network Agent – 3GPP AAA Server (Pr) This reference point shall allow the 3GPP AAA Server to report IP-connectivity related events to the Presence Network Agent (such as WLAN UE attaching/detaching and tunnel establishment/removal). The Pr reference point shall be based on mechanisms of existing interfaces of the 3GPP-WLAN interworking architecture defined in 3GPP TS 23.234 [19]. **Essential Correction**
Summary of change:	⌘	A profile for the Diameter interface based on Cx reference point is added for the Pr reference point.
Consequences if not approved:	⌘	Missing functionality

Clauses affected:	⌘	1, 2, 3, 11

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	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.

1 Scope

The present document defines the stage-3 protocol description for several reference points in the WLAN-3GPP Interworking System.

The present document is applicable to:

- The Dw reference point between the 3GPP AAA Server and an SLF.
- The Wa reference point between the WLAN AN and the 3GPP AAA Proxy.
- The Wd reference point between the 3GPP AAA Proxy and 3GPP AAA Server.
- The Wx reference point between the 3GPP AAA Server and the HSS.
- The Wm reference point between the 3GPP AAA Server and the PDG.
- The Wn reference point between the WLAN AN and the 3GPP WAG.
- The Wg reference point between the 3GPP AAA Server/Proxy and the WAG.
- The Pr reference point between the 3GPP AAA Server and the PNA.

2 References

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

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

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 22.934: "Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking".

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

[4] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; System description".

[5] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents".

[6] 3GPP TS 29.229: "Cx and Dx interfaces based on the Diameter protocol; Protocol details".

[7] IETF RFC 3588: "Diameter Base Protocol".

[8] IETF Draft: "Diameter Extensible Authentication Protocol (EAP) Application", draft-ietf-aaa-eap-09.txt, work in progress.

[9] IETF RFC 2869: "RADIUS Extensions".

[10] IETF RFC 2284: "Extensible Authentication Protocol (EAP)".

[11] IETF Draft: "Extensible Authentication Protocol (EAP) ", draft-ietf-eap-rfc2284bis-02.txt, work in progress.

[12] IETF Draft: "Diameter Network Access Server Application", draft-ietf-aaa-diameter-nasreq-12.txt, work in progress.

[13] IETF RFC 3576: "Dynamic Extensions to Remote Authentication Dial In User Service (RADIUS)".

[14] IETF RFC 3579: "RADIUS (Remote Authentication Dial-In User Service) Support For Extensible Authentication Protocol (EAP) ".

[15] IETF RFC 3580: "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines".

[16] IETF Draft, "~~-~~Carrying Location Objects in RADIUS ", draft-ietf-geopriv-radius-lo-01.txt, work in progress .

[17] IETF RFC 2865: "Remote Authentication Dial In User Service (RADIUS)".

[18] 3GPP TS 33.234: "3G security; Wireless Local Area Network (WLAN) interworking security".

[19] IETF Draft, "Diameter Credit-control Application", draft-ietf-aaa-diameter-cc-04.txt, work in progress.

[20] IETF RFC 2866: "RADIUS Accounting".

[21] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[22] 3GPP TS 23.003: "Numbering, addressing and identification".

[23] 3GPP TS 32.240: "~~-~~Charging architecture and principles".

[24] 3GPP TS 32.215: "Charging data description for the Packet Switched (PS) domain".

[25] GSMA PRD IR.61, "WLAN Roaming Guidelines".

[26] IETF Draft, "Chargeable User Identity", draft-adrangi-radius-chargeable-user-identity-02.txt, work in progress.

[27] IETF Draft "EAP lower layer attributes for AAA protocols", <draft-mariblanca-aaa-eap-lla-01.txt>, work in progress.

[xx] 3GPP TS 23.141: "Presence Service; Architecture and functional description".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.234 [4] apply.

3GPP - WLAN Interworking
External IP Network/External Packet Data Network
Home WLAN
Interworking WLAN
Offline charging
Online charging
PS based services
Service Authorization
Visited WLAN
WLAN-UE

In addition, for the purposes of the present document, the following terms and definitions given in 3GPP TS 23.141 [28] apply.

Presence Network Agent

3.2 Symbols

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

Wa	Reference point between a WLAN Access Network and a 3GPP AAA Proxy in the roaming case and a 3GPP AAA Server in the Non-Roaming case (charging and control signalling)
Wd	reference point between a 3GPP AAA Proxy and a 3GPP AAA Server (charging and control signalling)
Wf	Reference point between a Offline Charging System and a 3GPP AAA Server/Proxy
Wg	Reference point between a 3GPP AAA Proxy and a 3GPP WAG
Wi	Reference point between a Packet Data Gateway and an external IP Network
Wm	Reference point between a Packet Data Gateway and a 3GPP AAA Server
Wn	Reference point between a WLAN Access Network and a 3GPP WAG
Wo	Reference point between a 3GPP AAA Server and an OCS
Wp	Reference point between a 3GPP WAG and a 3GPP PDG.
Wx	Reference point between an HSS and a 3GPP AAA Server
Pr	Reference point between a 3GPP AAA Server and a PNA

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAA	Authentication, Authorization and Accounting
AVP	Attribute Value Pair
CCF	Charging Collection Function
CG	Charging Gateway
EAP	Extensible Authentication Protocol
HSS	Home Subscriber Server
IMS	IP Multimedia Subsystem
OCS	On-line Charging System
PDG	Packet Data Gateway
PNA	Presence Network Agent
RADIUS	Remote Authentication Dial-In User Service
WAG	WLAN Access Gateway
WLAN AN	WLAN Access Network
WLAN	Wireless Local Area Network
WLAN-UE	WLAN User Equipment

Next Modification

11 Pr Description

The Pr Reference Point is defined in 3GPP TS 23.141 [28] and allows the 3GPP AAA Server to report presence relevant events to the Presence Network Agent (PNA).

11.1 Functionality

The functionality of the Pr reference point is to enable:

- Indication of the Attach/Detach to the PNA by the 3GPP AAA Server of a WLAN user.

- Indication of the W-APN Activation/DeActivation to the PNA by the 3GPP AAA Server of a WLAN user.

11.2 Protocols

The Pr reference point shall be Diameter based and shall have an application ID defined for it. It is defined as an IETF vendor specific Diameter application, where the vendor is 3GPP. The application identifier is to TBA. It is to be assigned by IANA (http://www.iana.org/assignments/enterprise-numbers).

Editor's note: Pr has been specified to reuse Cx and Diameter Network Access Server Application [12] as much as possible. However, changes to the mandatory AVPs in the procedure definitions require that a new Diameter application ID is needed for Pr interface.

11.3 Procedures Description

11.3.1 WLAN Attach/Detach Indication

According to the requirements given in clause 11.1, the Pr reference point shall enable:

-an indication of the Attach /Detach to the PNA.

This procedure is used between the 3GPP AAA Server and the PNA.

The procedure of Attach indication shall be invoked by the 3GPP AAA Server after a new subscriber has been authenticated and authorised successfully by the 3GPP AAA Server.

The procedure of Detach indication shall be invoked by the 3GPP AAA Server when a WLAN user becomes detached, e.g. the WLAN UE has disappeared from WLAN coverage, or the OSC has initiated a disconnection.

The Pr reference point performs these functions based on the reuse of the existing Cx Server Assignment command code set (SAR/SAA).

Table 11.3.1.1: WLAN Attach / Detach Indication Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element contains the permanent identity of the user, i.e. the IMSI.
Server Assignment Type	Server-Assignment-Type	M	Type of procedure the 3GPP AAA Server indicated to the PNA. When this IE contains REGISTRATION value, the 3GPP AAA Server indicates to the PNA a WLAN user is attached. When this IE contains USER_DEREGISTRATION, the 3GPP AAA Server indicates to the PNA a WLAN user is detached. Any other value is considered as an error case.
Visited Network Identifier	Visited-Network-Identifier	C	An identifier that allows the home network to identify the Visited Network. This AVP shall be present if the PDG is not in the WLAN-UE's home network i.e. the WLAN-UE is roaming.
Routing Information	Destination-Host	C	If the 3GPP AAA Server knows the PNA name, this AVP shall be present. This information is available if the 3GPP AAA Server already has the PNA name stored. The PNA name is obtained from the Origin-Host AVP, which is received from the PNA, e.g. included in the SAA command. Otherwise only the Destination-Realm is included, so that it is resolved to a PNA address.

Editor's Note: Wa/Wd Location Attributes to be added to this table once they are defined as Diameter attributes

Table 11.3.1.2: WLAN Attach / Detach Indication Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	Result of the operation. A Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. An Experimental-Result AVP shall be used for Pr errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

11.3.1.1 Detailed behaviour

When a new 3GPP subscriber has been authenticated and authorized by the 3GPP AAA Server, the 3GPP AAA Server indicates the status of "Attach" towards the PNA. The PNA shall, in the event of an error in any of the steps, stop processing and return the corresponding error code, see 3GPP TS 29.229 [6]).

When a WLAN user is in Detach satus, the 3GPP AAA Server indicates the status of "Detach" towards the PNA. The PNA shall, in the event of an error in any of the steps, stop processing and return the corresponding error code, see 3GPP TS 29.229 [6]).

The 3GPP AAA server sends Server-Assignment-Request command to the PNA indicating the Attach/Detach status. The subscriber is identified by the User-Name AVP.

At reception of Server-Assignment-Request command, the PNA shall perform (in the following order):

1. Check that the user is known. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2. Check the Server Assignment Type value received in the request:

   - If it indicates REGISTRATION, that means the WLAN user is in Attach status, the PNA shall store the 3GPP AAA Server name for the authenticated and authorized 3GPP subscriber and set the Result-Code AVP to DIAMETER_SUCCESS in the Server-Assignment-Response command.

   - If it indicates USER_DEREGISTRATION, that means the WLAN user is in Detach status, the PNA shall remove the 3GPP AAA Server name previously assigned for the 3GPP subscriber and set the Result-Code AVP to DIAMETER_SUCCESS in the Server-Assignment-Response command.

   - If it indicates any other value, the Result-Code shall be set to DIAMETER_UNABLE_TO COMPLY, and no WLAN Attach/Detach indication procedure shall be performed.

The Origin-Host AVP shall contain the 3GPP AAA server identity.

11.3.2 W-APN Activation/De-Activation Indication

11.3.2.1 W-APN Activation Indication

According to the requirements given in clause 11.1, the Pr reference point shall enable:

- an indication of the W-APN Activation to the PNA.

This procedure is used between the 3GPP AAA Server and the PNA.

The procedure of W-APN Activation indication shall be invoked by the 3GPP AAA Server when a tunnel to a W-APN is established successfully as defined in section 7.9; see 3GPP TS 23.234 [4].

The W-APN Activation Indication Request/Response are mapped onto the NASREQ AAR/AAA messages.

Table 11.3.2.1: W-APN Activation Indication request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.
Visited Network Identifier	Visited-Network-Identifier	C	An identifier that allows the home network to identify the Visited Network. This AVP shall be present if the PDG is not in the WLAN-UE's home network, i.e. the WLAN-UE is roaming.
W-APN-ID	APN-Id	M	This information element shall contain the W-APN for which the UE has been granted authorization.
Routing Information	Destination-Host	M	The PNA name is obtained from the Origin-Host AVP of a previously received message.

Table 11.3.2.2:W-APN Activation Indication Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	Result of the operation. A Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. An Experimental-Result AVP shall be used for Pr errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

11.3.2.1.1 Detailed behaviour

If this message is received at the PNA, it indicates that the WLAN-UE now has been authorised for such a W-APN and has one (or more) tunnel(s) active to the particular W-APN at the PDG. The PNA shall, in the following order (if there is an error in any of the steps, the PNA shall stop processing and return the corresponding error code):

1) Check that the user exists in the PNA. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2) Store the current active W-APN

3) Optionally, the PNA shall store the PDG IP address associated with the W-APN.

4) The Result-Code shall be set to DIAMETER_SUCCESS.

Exceptions to the cases specified here shall be treated by a PNA as error situations, so the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY. No information shall be stored in PNA.

11.3.2.2 W-APN De-Activation Indication

According to the requirements given in clause 11.1, Pr reference point shall enable:

- an indication of the W-APN Deactivation to the PNA.

This procedure is used between the 3GPP AAA Server and the PNA.

The procedure of W-APN Deactivation indication is invoked by the 3GPP AAA Server when a particular W-APN is deactivated.

TheW-APN Deactivation Indication Request/Response are mapped onto the Abort Session Request/Answer (AAR/AAA) messages defined in RFC 3588 [7].

Table 11.3.3.1: W-APN Deactivation Indication Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user.
W-APN-Id	APN-Id	M	This information element shall contain the W-APN Identification associated with the deactivation.
Routing Information	Destination-Host	M	The PNA name shall be obtained from the Origin-Host AVP of a previous message received from the PNA.

Table 11.3.3.2: W-APN DeActivation Indication Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	Result of the operation. A Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. An Experimental-Result AVP shall be used for Pr errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

11.3.2.2.1 Detailed behaviour

The 3GPP AAA Server shall make use of this procedure to indicate the PNA that a particular W-APN has no active tunnel left for a specific user. On receipt of the message, the PNA shall:

1) Check that the user is known in the PNA. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2) The PNA shall set the Result-Code to DIAMETER_SUCCESS and send back the SAA command to the 3GPP AAA Server.

11.4 Information Elements Contents

11.4.1 WLAN Attach/Detach Indication

The **Server-Assignment-Request (SAR)** command, indicated by the Command-Code field being set to 301 and the 'R' bit set in the Command Flags field, is sent by the 3GPP AAA Server to the PNA, in order to indicate to the PNA a WLAN user is in the status of Attached or Detached.

Message Format

```
<Server-Assignment-Request> ::= < Diameter Header: 301, REQ, PXY, XXXX>
                                < Session-Id >
                                { Vendor-Specific-Application-Id }
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                [ Destination-Host ]
                                { Destination-Realm }
                                [ User-Name ]
                                [Visited-Network-Identifier]
                                { Server-Assignment-Type }
                                *[ AVP ]
                                *[ Proxy-Info ]
                                *[ Route-Record ]
```

The **Server-Assignment-Answer (SAA)** command, indicated by the Command-Code field being set to 301 and the 'R' bit cleared in the Command Flags field, is sent by the PNA to the 3GPP AAA Server, to confirm the Attached or Detached indication.

Message Format

<Server-Assignment-Answer> ::= < Diameter Header: 301, PXY, XXXX >
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[User-Name]
*[AVP]
*[Proxy-Info]
*[Route-Record]

11.4.2 W-APN Activation/DeActivation Indication

11.4.2.1 W-APN Activation Indication

The W-APN Activation Indication request and response messages are mapped onto the NASREQ AAR/AAA messages. The ABNF for this is defined below:

```
<AA-Request> ::= < Diameter Header: 265, REQ, PXY >
            < Session-Id >
            { Auth-Application-Id }
            { Origin-Host }
            { Origin-Realm }
            { Destination-Realm }
            { Auth-Request-Type }
            [ Destination-Host ]
            [ Visited-Network-Identifier]
            { APN-ID}
            [ User-Name ]
            [ Authorization-Lifetime ]
            [ Auth-Grace-Period ]
            [ Auth-Session-State ]
            [ Framed-IP-Address ]
            [ Framed-IP-Netmask ]
            * [ Tunneling ]
            * [ Proxy-Info ]
            * [ Route-Record ]
            * [ AVP ]
```

The ABNF for the AAA is defined as follows:

```
     <AA-Answer> ::= < Diameter Header: 265, PXY >
            < Session-Id >
            { Auth-Application-Id }
            { Auth-Request-Type }
            { Result-Code }
            { Origin-Host }
            { Origin-Realm }
            [ Subscription-ID-AVP]
            [ Error-Message ]
            [ Error-Reporting-Host ]
            * [ Failed-AVP ]
            * [ Proxy-Info ]
            * [ AVP ]
```

11.4.2.2 W-APN Deactivation Indication

The ABNF for the W-APN Deactivation Indication Procedure is mapped onto the ASR and ASA commands as defined below:

```
<ASR>  ::= < Diameter Header: 274, REQ, PXY >
            < Session-Id >
            { Origin-Host }
```

```
            { Origin-Realm }
            { Destination-Realm }
            { Destination-Host }
            { Auth-Application-Id }
            [ User-Name ]
            { APN-Id }
            [ Origin-State-Id ]
            * [ Proxy-Info ]
            * [ Route-Record ]
             *[ AVP ]


<ASA>  ::= < Diameter Header: 274, PXY >
             < Session-Id >
            { Result-Code }
            { Origin-Host }
            { Origin-Realm }
            [ User-Name ]
            [ Origin-State-Id ]
            [ Error-Message ]
            [ Error-Reporting-Host ]
            * [ Failed-AVP ]
            * [ Redirected-Host ]
            [ Redirected-Host-Usage ]
             [ Redirected-Max-Cache-Time ]
            * [ Proxy-Info ]
            * [ AVP ]
```

Next Modification

10.1.18 Server-Assignment-Type

The Server-Assignment-Type AVP is defined in 3GPP TS 29.229 [6] and indicates the type of procedure the 3GPP AAA Server is asking to the HSS.

Wx reference point defines as valid only NO_ASSIGNMENT, REGISTRATION, USER_DEREGISTRATION, ADMINISTRATIVE_DEREGISTRATION and REAUTHENTICATION_FAILURE.

Pr reference point defines as valid only REGISTRATION, USER_DEREGISTRATION.

3GPP TSG CN WG4 Meeting #27
Cancun, Mexico, 25th – 29th April 2005

C4-050866

CR-Form-v7

CHANGE REQUEST

⌘ **29.234** **CR** **051** ⌘ **rev** **2** ⌘ Current version: **6.2.0** ⌘

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

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

Title:	⌘	Mandating RFC 3576 in WLAN-IW
Source:	⌘	Nokia
Work item code:	⌘	WLAN-IW
Date:	⌘	29/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	To quote the LS from SA1,S1-050512, *"SA1 confirms that the immediate purging of a user from a I-WLAN, driven by the 3GPP network, **is a mandatory requirement**. This is reflected in the current SA1 specifications (namely section 4.4 of TS 22.105, and section 5.1.4 of TS 22.324)."* This CR therefore updates 29.234 accordingly
Summary of change:	⌘	Removal of text that discusses the optionaility of RFC3576 in the case of Disconnect Messages
Consequences if not approved:	⌘	The spec assumes that Disconnect Messages in RFC3576 may not be supported by all WLAN AN, which is clearly not in line with SA1 requirements. It is therefore unclear that support for the reader that RFC is a mandatory and that a WLAN AN must support it if it wishes to interwork with a 3GPP network for WLAN-IW purposes. an operator At present, there is no text anywhere in the spec . This may lead to problems if a 3GPP AAA Server is implemented assuming that the WLAN AN will support Disconnect Messages in RFC3576 but the WLAN AN does not, in fact support it.
Clauses affected:	⌘	4.3.2, 5.3

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

Other comments: ⌘	

How to create CRs using this form:

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

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

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

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

**** Start of change #1 ****

4.3.2 Immediate Purging of a User from WLAN access

This procedure is used to communicate between the WLAN AN and the 3GPP AAA Proxy that the 3GPP AAA Server has decided that a specific WLAN-UE shall be disconnected from accessing the WLAN interworking service. The procedure is Diameter or RADIUS based. In ~~T~~the RADIUS case, ~~is only considered if~~ the WLAN AN and the 3GPP AAA Proxy shall support the Disconnect Messages specified in RFC 3576 [13] in order to enable such a procedure. ~~WLAN ANs supporting RADIUS RFC 2865 [17] but not supporting RFC 3576 [13] do not have the required capabilities to react to server-initiated messages, therefore "Immediate purging of a user from WLAN Access" procedure shall not be performed towards clients located in this kind of WLAN AN.~~

Diameter usage in Wa:

- This procedure is mapped to the Diameter command codes Diameter-Abort-Session-Request and Diameter-Abort-Session-Answer specified in RFC 3588 [7]. Information element content for these messages are shown in tables 4.3.2.1 and 4.3.2.2.

Table 4.3.2.1: Information Elements passed in ASR message

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.

Table 4.3.2.2: Information Elements passed in ASA message

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.
Result-Code	Result-Code	M	Result of the operation.

See Annex A.2 for signalling flow reference.

RADIUS usage in Wa:

- This procedure is mapped to the RADIUS messages Disconnect-Request and Disconnect-Response specified in RFC 3576 [13].

**** End of change #1 ****

**** Beginning of change #2 ****

5.3 3GPP AAA Proxy and 3GPP AAA Server behaviour when Interworking with RADIUS/Diameter WLAN ANs

If a WLAN AN attached to the 3GPP AAA Proxy is Diameter based, Diameter messages shall be passed on to the 3GPP AAA Server through the 3GPP AAA Proxy. If a WLAN AN attached to the 3GPP AAA Proxy is RADIUS based, the RADIUS messages sent by the WLAN AN shall be either passed on to the 3GPP AAA Server through the 3GPP AAA Proxy, or translated by the 3GPP AAA Proxy Translation Agent into Diameter messages to be sent on to the 3GPP AAA Server by the 3GPP AAA Proxy. This protocol translation shall be done as follows.

The 3GPP AAA Server needs to be aware of what kind of client it is serving in order to adapt its operation to the capabilities of the WLAN AN.

The 3GPP AAA Proxy is the only network element in direct contact with the WLAN AN and therefore it is the only network element aware of whether the WLAN AN is RADIUS or Diameter based. The following rules shall apply for the 3GPP AAA Server to determine this:

If the Wd reference point uses RADIUS then:

- The 3GPP AAA Server shall assume that the WLAN AN is RADIUS based.

If the Wd reference point uses Diameter then:

- The 3GPP AAA Server shall assume the WLAN AN to be Diameter- based unless the 3GPP AAA Proxy specifically indicates that the WLAN AN is RADIUS based (see subclause 6.3.3).

Once the 3GPP AAA Server is aware of which AAA protocol that the WLAN AN is using , it shall adapt its operation over the Wd reference point.

If the WLAN AN is determined to be Diameter based, the operation mode of the 3GPP AAA Server shall be the normal behaviour as described in Diameter (IETF Draft "EAP" [8]) and the Diameter Base (RFC 3588 [7]). for authentication and NASREQ[12] for accounting.

If the WLAN AN is determined to be RADIUS based, the operation mode of the 3GPP AAA Server shall be the following:

If the Wd reference point is using RADIUS then:

- Normal behaviour for RADIUS as specified in the first bullet in subclause 5.2.

If the Wd reference point is using Diameter then:

- The normal behaviour for Diameter as specified in the second bullet in subclause 5.2, but shall be modified as follows to ensure RADIUS compatibility:

  - Diameter AVPs to RADIUS attributes compatibility:

    - 3GPP AAA Server shall restrict itself to use only Diameter AVPs that are compatible with RADIUS attributes. In general, 3GPP AAA Server shall use Diameter AVPs with codes not greater than 255. See section 9.5 in [12] for further detail.

  - Diameter specific procedures when interacting with RADIUS clients:

    - 3GPP AAA Server shall not attempt server-initiated re-authentication.

    - 3GPP AAA Server may attempt server-initiated re-authorization and server-initiated session termination.

      - ~~If the WLAN AN and the 3GPP AAA Proxy support "Dynamic Authorization Extensions to gRADIUS" RFC 3576 [13], then the procedures are performed normally.~~

      - ~~If the WLAN AN and the 3GPP AAA Proxy do no support "Dynamic Authorization Extensions to RADIUS" RFC 3576 [13], then 3GPP AAA Proxy shall notify the 3GPP AAA Server of this by sending a protocol error such as DIAMETER_COMMAND_UNSUPPORTED. In that case, the 3GPP AAA Server shall not continue to attempt server-initiated re-authorization and/or server-initiated session termination.~~

**** End of change #2 ****

3GPP TSG-CT WG4 Meeting #27 **C4-050871**
Cancun, MEXICO. 25th to 29th April 2005. **Rev. C4-050799**

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **058** ⌘**rev** **2** ⌘ Current version: **6.2.0** ⌘

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

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

Title:	⌘	WAG address resolution on Wg interface
Source:	⌘	NEC
Work item code:	⌘	WLAN-IW
Date:	⌘	14/04/2005
Category:	⌘	**F**
Release:	⌘	REL-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*
Rel-7 *(Release 7)*

Reason for change:	⌘	In case of roaming, it is unclear how AAA server resolves the WAG address that is located in the visited network since WAG address is managed by the AAA proxy.
Summary of change:	⌘	Add the following explanatory text in section 9.3.1 • If the WAG is located in the VPLMN the 3GPP AAA Server shall send the AAR command over the Wd interface to the 3GPP AAA Proxy and then it is 3GPP AAA Proxy's task to find the WAG serving the user. • The other TEI corrections
Consequences if not approved:	⌘	The routing policy download procedure as defined over Wg reference point does not work.

Clauses affected:	⌘	9.1, 9.2, 9.3.1

Other specs affected:	Y	N			
⌘	X		Other core specifications	⌘	23.008-CR145
		X	Test specifications		
		X	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 ******

9 Wg Description

9.1 Functionality

The Wg reference point is defined between the 3GPP AAA Server and the WAG or between the 3GPP AAA Proxy and the WAG depending on the location of the WAG. The description of the reference point and its functionality is given in 3GPP TS 23.234 [4].

This clause specifies a Diameter application supports the functionality of this reference point.

The interface at this reference point is applicable only when a WLAN UE is allowed to access the 3GPP PS services from the I-WLAN.

Editor's Note: Remaining functionalities on this interface e.g. the charging rules to be applied, sending of MSISDN to WAG, that are necessary for WLAN 3GPP IP Access functionality are not stable yet.

9.2 Protocols

Diameter NASREQ is used for the policy download to the WAG. In this case, the 3GPP AAA Server or Proxy shall act as the NAS client and the WAG as the Diameter Server.

The Application-Id to be advertised over Wg reference point corresponds to the EAP, NASREQ or Diameter Base Protocol Application-Id, depending on the command sent over Wg.

9.3 Procedures Description

9.3.1 Policy Download Procedures

The policy download procedure is used between the 3GPP AAA Server and the WAG in the case where the PDG is in the HPLMN and between the 3GPP AAA Proxy and the WAG in the case where the PDG is in the VPLMN

The Wg reference point performs routing policy download based on the reuse of the NASREQ [12] AAR-AAA command set. If the WAG is located in the VPLMN the 3GPP AAA Server shall send the AAR command over the Wd interface to the 3GPP AAA Proxy and then it is 3GPP AAA Proxy's task to find the WAG serving the user.

The way to find the WAG address in AAA proxy/ AAA server is implementation dependent. For example, based on the source IP address of DER command if the WAG has the NAT functionality or manual network configuration.

Table 9.3.1.1: Wg Policy Download Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element contains the permanent identity of the user, i.e. the IMSI.
Routing Policy	Routing-Policy	M	This AVP includes the routing policy to apply for the user received in the User-Name AVP.
Routing Information	Destination-Host	C	This information element contains the WAG.
Subscription-ID AVP	Subscription-ID AVP	M	This AVP shall contain the MSISDN of the user.

Table 9.3.1.2: Wg Policy Download Response

Information element name	Mapping to Diameter AVP	Cat.	Description
Registration Result	Result Code/ Experimental Result Code	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. **Experimental-Result AVP shall be used for Wg errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.**

****** END ******

3GPP TSG-CT WG4 Meeting #27 **C4-050873**
Cancun, MEXICO. 25th to 29th April 2005. **Rev. C4-050779**

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.008** **CR** **145** ⌘**rev** **2** ⌘ Current version: **6.5.0** ⌘

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

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

Title:	⌘	Corrections on Serving WAG
Source:	⌘	NEC
Work item code:	⌘	WLAN-IW
Date:	⌘	14/04/2005
Category:	⌘	**F**
Release:	⌘	REL-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
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: ⌘

This CR has two updates.
Firstly, the current TS 23.008 defines that a UE might have multiple WAG addresses. This could be interpreted that WAG can be chosed by UE based on specified W-APN. However, we concluded that this is very difficult to achive. See the possible solutions that we have investigated.

1) WAG address is passed to AAA server when IPsec tunnel is established.
When IPsec tunnel is established, UE and PDG perform tunnel establishment procedure using IKE v2 protocol. There might be 2 ways to pass WAG address to PDG.
1-1) UE obtains the WAG address prior to IPsec tunnel establishement and informs WAG address to PDG. → Protocol between WAG and UE is not standarized in Rel-6.
1-2) PDG maps WAG address based on the source address on IKE message. → Since this mapping must be globally wide. It seems inpractical.

2) WAG address is passed to AAA server when UE performs user authentication.
2-1) When user authentication performs, the AAA proxy server sets WAG address onto the DIAMETER EAP request command. Thereaftrer, any IPsec tunnels to be established after successful user authentication will use the same WAG.

Based on our analysys above, the 2-1 is the best feasible solution in Rel-6. However, this solution limits the use of multiple WAGs at the same time.

Secondary, the WLAN Direct IP Access does not require WAG at all so that

	WAG should be defined as the conditional. In addition, PDG does not need to know WAG address based on the specified solution.
Summary of change: ⌘	• Redefine the Serving WAG to be single address per UE and set in AAA proxy/server when UE authenticated. • Update data strage attributes.
Consequences if not approved: ⌘	The routing policy download procedure as defined over Wg reference point does not work.

Clauses affected: ⌘	3B.1.8, 5.5				
	Y	**N**			
Other specs affected: ⌘	**X**		Other core specifications	⌘	29.234-CR058
		X	Test specifications		
		X	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 ******

3B.1.8 Serving WAG

The Serving WAG field contains the WAG address~~(es)~~ information obtained ~~of the WAG(s)~~ through the successful user authentication procedure.~~which the tunnel(s) is/are established.~~

****** Next modified section ******

5.5 I-WLAN Service Data Storage

Table 5.5: Overview of data used for I-WLAN services

PARAMETER	Subclause	HSS	3GPP AAA Server	3GPP AAA Proxy	PDG	WAG	TYPE
IMSI	3B.1.1	M	M				P
MSISDN	3B.1.2	M	M	M	M	M	P
W-APN	3B.1.3	M	M		M		P
List of authorized visited network identifiers	3B.1.4	M					P
3GPP AAA Proxy Identifier	3B.1.5		M		M	M	T
3GPP AAA Server Name	3B.1.6	M		M	M	C	T
Serving PDG List	3B.1.7		M	M			P
Serving WAG	3B.1.8		~~M~~C	~~M~~C	~~M~~		P
WLAN UE Local IP address	3B.1.9				M	M	T
WLAN UE Remote IP address	3B.1.10	C	C		M		P
User Status	3B.2.1		M				T
RAND, SRES, Kc	3B.3.1	M	M		-		T
RAND, XRES CK, IK, AUTN	3B.3.2		M		-		T
Master Key (MK)	3B.3.3		M				T
Transient EAP Keys (TEKs)	3B.3.3		M				T
Session Identifier	3B.4.1		M				T
Session-Timeout	3B.4.2		C				P
Quota	3B.4.3		C				P
WLAN Access	3B.5.1	M					P
WLAN Tunnelling	3B.5.2	M					P
WLAN Direct IP Access	3B.5.3	M					P
W APN Authorised	3B.5.4	M					P
W APN Identifier	3B.5.4.1						P
W-APN Barring Type	3B.5.4.2	M					P
W-APN Charging Data	3B.5.4.3	C			C		P
WLAN UE Remote IP Address	3B.5.4.4	C			P		P
Access Independence Flag	3B.5.5	M					P
I-WLAN Access Type	3B.5.6	M					P
Max Requested Bandwidth	3B.6.1		P		T		P
Routing Policy	3B.6.2				C	C	T
Charging Data	3B.7.1	M			M		P
Charging Characteristics	3B.7.1.1	M	-		M		P
Primary OCS Charging Function Name	3B.7.2	M			M		P
Secondary OCS Charging Function Name	3B.7.3	M			M		P
Primary Charging Collection Function Name	3B.7.4	M			M		P
Secondary Charging Collection Function Name	3B.7.5	M			M		P

3GPP TSG-CT WG4 Meeting #27 **C4-050874**
Cancun, MEXICO. 25th to 29th April 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **062** ⌘ **rev** **2** ⌘ Current version: **6.2.0** ⌘

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

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

Title:	⌘	Limit on the number of session in WLAN 3GPP IP Access
Source:	⌘	Ericsson, Nokia
Work item code:	⌘	WLAN-IW
Date:	⌘	29/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
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:	⌘	Comply with the simultaneous access control described in TS 33.234 clause 5.7
Summary of change:	⌘	In section 8.3.2.1, the needed procedure are added in one of the steps. The procedure consists of checking if the maximum number of simultaneous accesses (IKE SA) per W-APN has been reached and, if so, the previously established access for that same W-APN is terminated. In section 10.1.8 the AVP that transports the maximum number or accesses is included.
Consequences if not approved:	⌘	Simultaneous access control will not be implemented as specified.

Clauses affected:	⌘	8.3, 10.1.8

Other specs affected: ⌘	Y	N		
	X		Other core specifications	⌘ 29.230 CR 051, 23.008 CR 151
		X	Test specifications	
		X	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 <<<<<<<<<<<

8.3 Procedures Description

8.3.1 Authentication Procedures

According to the requirements specified in chapter 10.1, Wm reference point shall enable:

- Messaging for service authentication between WLAN UE and 3GPP AAA Server/Proxy.

The authentication procedure is used between the PDG and 3GPP AAA Server/Proxy. It is invoked by the PDG, on receipt from the WLAN-UE of a "tunnel establishment request" message. This takes the form of forwarding an IKE v2 (3GPP TS 33.234 [18]) exchange with the purpose of authenticating in order to set up a Security Association (SA) between the UE and the PDG. Once the SA has been authenticated, more than one tunnel SA can be negotiated inside the IKE v2 SA. Hence additional tunnels between the UE and PDG do not need to trigger further Diameter_EAP authentication messaging to the 3GPP AAA Server.

The Wm reference point performs authentication based on the reuse of the DER/DEA command set defined in Diameter_EAP (3GPP TS 33.234 [18]).

Table 8.3.1.1: Authentication Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.
EAP payload	EAP payload	M	Encapsulated EAP payload used for UE - 3GPP AAA Server mutual authentication
Authentication Request Type	Auth Req Type	M	Defines whether authentication only or authentication and authorization are required. AUTHENTICATION_ONLY is required in this case
Visited Network Identifier	Visited-Network-Identifier	C	Identifier that allows the home network to identify the Visited Network. This AVP shall be present if the PDG is not in the WLAN-UE's home network i.e. the WLAN-UE is roaming.
EAP Lower Layer	EAP Lower Layer	M	This AVP shall contain the value “3” to indicate IKE_v2 has been used to carry EAP messages to the PDG, according to [27]

Table 8.3.1.2: Authentication Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
EAP payload	EAP payload	M	Encapsulated EAP payload used for UE - 3GPP AAA Server mutual authentication
Master-Session-Key	Master-Session-Key	C	contains keying material for protecting the communication between the user and the NAS. Present when Result Code is set to "Success".
Result code	Result Code / Experimental-Result-Code	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol or as per in NASREQ. 1xxx should be used for multi-round, 2xxx for success. Experimental-Result AVP shall be used for Wm errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

8.3.1.1 3GPP AAA Server Detailed Behaviour

On receipt of the DER message, the 3GPP AAA Server shall check if the Session-ID corresponds to an ongoing session. If it corresponds to an on-going session, the 3GPP AAA Server shall process the DER message according to 3GPP TS 33.234 [18] and no Diameter EAP authentication shall be triggered over the Wm interface.

If the Session-ID does not correspond to an on-going session, the 3GPP AAA Server shall:

1) Check that the user exists in the 3GPP AAA Server. If not, the 3GPP AAA Server shall use the procedures defined for the Wx interface to authenticate the user.

2) Check that the user has 3GPP-WLAN subscription. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_NO_WLAN_SUBSCRIPTON.

Otherwise, DIAMETER_SUCCESS shall be returned to indicate successful authentication procedure and authentication information shall be returned.

Exceptions to the cases specified here shall be treated by 3GPP AAA Server as error situations, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY. No authentication information shall be returned.

8.3.1.2 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy is required to handle roaming cases in which the PDG is in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy.

On receipt of the DEA message, the AAA Proxy shall record the state of the connection (i.e. Authentication Successful).

8.3.2 Authorization Procedures

According to the requirements stated in subclause 10.1, Wm reference point shall enable:

- Carrying messages for service authorization between PDG and 3GPP AAA Server/Proxy.

- Allow the 3GPP AAA Server/Proxy to retrieve tunnelling attributes and WLAN UE's IP configuration parameters from/via Packet Data Gateway.

This procedure is used between the PDG and 3GPP AAA Server and Proxy. It is invoked by the PDG, on receipt from the WLAN-UE of a "tunnel establishment request" message and subsequent to the success of tunnel authentication i.e. on receipt of a DEA message from the 3GPP AAA Server with Result Code set to "Success".

The Wm reference point performs authorization download based on the reuse of the NASREQ [12] AAR-AAA command set.

Table 8.3.2.1 Wm Authorization Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.
Request-Type	Session-Request-Type	M	Type of Wm specific Diameter application request. The following values are to be used: AUTHORIZATION REQUEST (0) This value shall indicate the initial request for authorization of the user to the APN. ROUTING POLICY (1) This value shall indicate that routing policy AVP is present.
Visited Network Identifier	Visited-Network-Identifier	C	Identifier that allows the home network to identify the Visited Network. This AVP shall be present if the PDG is not in the WLAN-UE's home network, i.e. the WLAN-UE is roaming.
W-APN-ID	APN-Id	C	This information element contains the W-APN which the UE is requesting authorization. This AVP is present when Session-Request-Type AVP is set to AUTHORIZATION REQUEST.
Routing Policy	Routing-Policy	C	This AVP includes the routing policy of the tunnel set-up. This AVP shall be present when Session-Request-Type AVP is set to ROUTING POLICY. Editor's Note: Its exact format is ffs.
Routing Information	Destination-Host	M	The 3GPP AAA Server name is obtained from the Origin-Host AVP of a previously received message.

Table 8.3.2.2: AA-Response

Information element name	Mapping to Diameter AVP	Cat.	Description
Registration Result	Result Code/ Experimental Result Code	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. **Experimental-Result AVP shall be used for Wm errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP**
Subscription-ID AVP	Subscription-ID AVP	C	This AVP shall contain the MSISDN of the user. This AVP shall be present is the Diameter Result Code is set to DIAMETER_SUCCESS
Max-Subscribed-Bandwidth	Max-Requested-Bandwidth	O	The Max requested bandwidth AVP. Can be sent by the 3GPP AAA Server to the PDG if it is present in the user subscription info held at the 3GPP AAA Server.
Charging Data	Charging-Data	C	Charging information for the W-APN for that user. It shall be present when Result-Code is equal to DIAMETER_SUCCESS and when the received Session-Request–Type was set to AUTHORIZATION REQUEST.
Framed-IP-Address	Framed-IP-Address	O	This AVP contains the remote IPv4 address of the WLAN UE that the 3GPP AAA Server downloaded from the HSS. This AVP shall not be present when the 3GPP AAA Server received an authorisation request with Session-Request–Type AVP set to ROUTING POLICY.
Framed-IP-Prefix	Framed-IP-Prefix	O	This AVP contains the remote IPv6 prefix of the WLAN UE that the 3GPP AAA Server downloaded from the HSS. This AVP shall not be present when the 3GPP AAA Server received an authorisation request with Session-Request–Type AVP set to ROUTING POLICY.

8.3.2.1 3GPP AAA Server Detailed Behaviour

The 3GPP AAA Server shall, in the following order (if there is an error in any of the steps, the 3GPP AAA Server shall stop processing and return the corresponding error code):

1) Check that the user exists in the 3GPP AAA Server. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2) Check the Session-Request-Type AVP:

- If Request type is set to AUTHORIZATION REQUEST, it indicates that the WLAN-UE ~~does not have a tunnel active~~ is attempting to access ~~to~~ the particular W-APN at the PDG and is requesting authorization for such a W-APN access.

  - The 3GPP AAA Server shall check that the user has subscription for the W-APN requested. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_NO_APN_SUBSCRIPTON.

  - The 3GPP AAA Server shall check whether the user has access to that W-APN, otherwise Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED.

  - If the user is roaming (indicated by the presence of the Visited-Network-Identifier AVP), the 3GPP AAA Server shall check if the user is allowed to access the W-APN from a VPLMN. This information is obtained from the HSS within the APN-Authorization AVP. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR _ROAMING_NOT_ALLOWED.

  - If the WLAN UE does not already have an active access to this W-APN, the PDG shall initiate an Access-Number counter for that W-APN and set it to one. If the Access-Number counter has already been initiated, the PDG shall increment the counter by one. The PDG shall then check the counter value against the Maximum-Number-Accesses for that W-APN from that user's data. If the Access-Number exceeds Maximum-Number-Accesses, the 3GPP AAA Server shall use the 3GPP AAA Server initiated disconnection procedures towards the PDG with which the user has the oldest established access in order

to initiate the tear down of the SA associated with that access. The 3GPP AAA Server shall update accordingly the information of active accesses for the W-APN ~~The 3GPP AAA Server~~and ~~-~~shall store the PDG IP address.

- The 3GPP AAA Server shall download APN-User-Data AVP and the WLAN UE remote IP address if present and the charging information as received from the HSS. The Result-Code shall be set to DIAMETER_SUCCESS.

- If Request type is set to ROUTING POLICY, it indicates that the WLAN-UE already has an active tunnel to the given PDG and is informing the 3GPP AAA Server of the routing policy for the tunnel. The 3GPP AAA Server shall store the Routing-Policy AVP and use Wg procedures to install this policy at the WAG. If this is successful, 3GPP AAA Server shall set Result-Code AVP to DIAMETER_SUCCESS in the AAA message. If not, Result-Code shall be set to DIAMETER_UNABLE_TO COMPLY.

Exceptions to the cases specified here shall be treated by 3GPP AAA Server as error situations, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY. No authorization information shall be returned.

8.3.2.2 AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy is required to handle roaming cases in which the PDG is in the VPLMN. On this interface, it may act to limit policy enforcement by modifying messages. It shall therefore maintain session state. The 3GPP AAA Proxy shall, in the following order (if there is an error in any of the steps, the 3GPP AAA Proxy shall stop processing and return the corresponding error code).

Check the Request Type AVP:

1) If Request type indicates AUTHORIZATION REQUEST, it indicates that the WLAN-UE does not have a tunnel active to the particular APN at the PDG and is requesting authorization for such an APN.

   a) The 3GPP AAA Proxy shall check locally configured information whether users from the HPLMN are allowed to access to the W-APN requested from this (V)PLMN. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR _ROAMING_NOT_ALLOWED and the AA-A message sent to the PDG. In all other cases, the message shall be forwarded transparently to the 3GPP AAA Server.

2) If Request-Type indicates ROUTING POLICY:

   a) This indicates that the WLAN-UE already has an active tunnel to the given PDG and is informing the 3GPP AAA Server of the routing policy for the tunnel. The 3GPP AAA Proxy shall store the Routing-Policy AVP and use Wg procedures to download the policy to the WAG. If this is successful, 3GPP AAA Server shall set Result Code to "Success" and send the AAR reply. If not, Result Code shall be set to DIAMETER_UNABLE_TO COMPLY.

Exceptions to the cases specified here shall be treated by 3GPP AAA Proxy as error situations, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY and AA-A message sent to the PDG.

8.3.3 PDG Initiated Session Termination Procedure

This procedure is used between the PDG and the 3GPP AAA Server. It is invoked by the PDG when the user's tunnel associated with the W-APN has been disconnected.

Table 8.3.3~~.~~.1: Session Termination Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.
W-APN-ID	APN-Id	M	This information element contains the W-APN which the UE is requesting access.
Routing Information	Destination-Host	M	The 3GPP AAA Server name is obtained from the Origin-Host AVP of a previous received message.

Table 8.3.3.2: Session Termination Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Wm errors.

8.3.3.1 3GPP AAA Server Detailed behaviour

On receipt of the STR, the 3GPP AAA Server shall, in the following order (if there is an error in any of the steps, the 3GPP AAA Server shall stop processing and return the corresponding error code):

a) Check from the User Name AVP that this corresponds to a user. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

b) Check that the user has an active session on the received W- APN. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_W-APN_UNUSED_BY_USER.

c) If the User is known and the W-APN corresponds to a known session, the 3GPP AAA Server shall remove any PDG specific information connected to that user on that W-APN. and update the status of the subscriber if needed. If the user was a home user, the 3GPP AAA Server shall signal to the WAG to initiate procedures to remove any filtering policy associated with that user's session. The Result Code shall be set to DIAMETER_SUCCESS.

8.3.3.2 3GPP AAA Proxy Detailed Behaviour

In the roaming case, the 3GPP AAA Proxy shall forward the STR message to the 3GPP AAA Server. On receipt of an STA with Result-Code set to DIAMETER_SUCCESS, the 3GPP AAA Proxy shall remove any session specific information associated with that user at that W-APN. It shall signal to the WAG to initiate procedures to remove any filtering policy associated with that user's session.

8.3.4 3GPP AAA Server Initiated Tunnel Disconnect Procedure

This procedure is used between the 3GPP AAA Server and the PDG. It is invoked by the 3GPP AAA Server when the WLAN subscription for the user has been deleted/prohibited in the 3GPP AAA Server or if the particular session must be terminated for any reason and the PDG must be updated with respect to these changes.

The Wm reference point performs the disconnection of user tunnel initiated by the 3GPP AAA Server based on the use of the RFC 3588 [7] Abort-Session-Request / Answer (ASR/ASA) commands.

Table 8.3.4.1: 3GPP AAA Server Initiated Tunnel Disconnection - Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.
W-APN-Id (see clause 8.5.15)	APN-Id	M	W-APN Identification.
Routing Information	Destination-Host	M	The PDG name is obtained from the Origin-Host AVP of a previous message received from the PDG e.g. included in the authentication command.

Table 8.3.4.2: 3GPP AAA Server Initiated Tunnel Disconnection - Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Wm errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

8.3.4.1 Detailed Behaviour

The 3GPP AAA Server shall make use of this procedure to instruct the PDG to disconnect a particular W-APN for a specific user. On receipt of the message, the PDG shall:

1) Check from the user is known in the PDG. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2) Check that the user has an active session on the received W-APN. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_W-APN_UNUSED_BY_USER.

3) If the User is known and the W-APN corresponds to a known session, the PDG shall perform tunnel disconnect procedure of the tunnels associated with that user on that W-APN. The PDG shall further remove any stored user information pertaining to that APN.

4) The PDG shall set the Result-Code to DIAMETER_SUCCESS and send back the SAA command to the 3GPP AAA Server.

On receipt of the message, the 3GPP AAA Server shall update the related service information and/or status of the subscriber and remove any filtering policy related to the disconnected tunnel from WAG if necessary.

8.3.4.2 3GPP AAA Proxy Behaviour

On receipt of the ASA message with Diameter Result Code set to DIAMETER_SUCCESS, the 3GPP AAA Proxy shall signal to the WAG to initiate procedures to remove any filtering policy- associated with that user's session.

>>>>>>>>>>> End of first modified section <<<<<<<<<<

>>>>>>>>>>> Second modified section <<<<<<<<<<<

10.1.8 WLAN-User-Data

The WLAN-User-Data AVP is of type Grouped. This AVP contains the WLAN User Profile information for the 3GPP AAA Server to authorize the service.

AVP format

```
WLAN-User-Data::= <AVP header: TBD>
    [Subscription-ID ]
    { WLAN-Access }
    { WLAN-3GPP-IP-Access }
    [ Session-Timeout ]
    1* { Charging-Data  }
    *[ APN-Authorized ]
    *[ Maximum-Number-Accesses ]
    { WLAN-Direct-IP-Access }
    * [AVP]
```

>>>>>>>>>>> End of second modified section <<<<<<<<<<<

3GPP TSG CN WG4 Meeting #27
Cancun, Mexico, 25th – 29th April 2005

C4-050875

CR-Form-v7

CHANGE REQUEST

⌘ **23.008** **CR** 151 ⌘ **rev** **1** ⌘ Current version: **6.5.0** ⌘

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

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

Title:	⌘	Addition of Maximum-Number-Accesses AVP and Number-Accesses Data types.
Source:	⌘	Nokia, Ericsson
Work item code:	⌘	WLAN-IW
Date:	⌘	29/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change:	⌘	SA3 have mandated that the network shall be able to configure a maximum number of simultaneous accesses to a give W-APN. This CR and the accompanying CRs to 23.008 and 29.234 enable this in the stage 3.
Summary of change:	⌘	Addition of Maximum-Number-Accesses AVP and Number-Accesses Data types to 23.008 for WLAN-IW data storage
Consequences if not approved:	⌘	Loophole in the spec that allows the user unlimited number of accesses to a W-APN

Clauses affected:	⌘	5.5, 3B

	Y	N			
Other specs affected: ⌘	X		Other core specifications	⌘	29.234-062, 29.230-051
		X	Test specifications		
		X	O&M Specifications		

Other comments:	⌘	Tdocss C1-050874, C1-050876 are related CRs

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 change #1 ****

3B Definition of subscriber data I-WLAN domain

3B.1 Data related to subscription, identification and numbering

3B.1.1 IMSI

The International Mobile Subscriber Identity (IMSI) is defined in 3GPP TS 23.003 [5]. The IMSI serves as the root of the subscriber data pseudo-tree.

3B.1.2 Mobile Subscriber ISDN Number (MSISDN)

Mobile Subscriber ISDN Number (MSISDN) is defined in 3GPP TS 23.003 [5]. One MSISDN is used for WLAN-IW subscription. If the multinumbering option applies, the MSISDN used is the Basic MSISDN (see section 2.1.3 for more information on MSISDNs for multinumbering option).

3B.1.3 W-APN

The WLAN Access Point Name (W-APN) is specified in 3GPP TS 29.234 [63]. This parameter identifies a data network and a point of interconnection to that network (Packet Data Gateway).

3B.1.4 List of authorized visited network identifiers

The list of authorized visited network identifiers field indicates which 3GPP visited network identifiers are allowed for roaming.

This list can be a linear list of visited network identifiers or a compound list of network identifier types e.g. home PLMN or home country; however the exact structure of the list is an implementation option.

3B.1.5 3GPP AAA Proxy Identifier

The 3GPP AAA Proxy Name, specified in 3GPP TS 29.234 [63], defines the Diameter or RADIUS Identity of the 3GPP AAA Proxy node.

3B.1.6 3GPP AAA Server Name

The 3GPP AAA Server Name, specified in 3GPP TS 29.234 [63], defines the Diameter or RADIUS Identity of the 3GPP AAA Server node.

3B.1.7 Serving PDG List

The Serving PDG List field contains the addresses of the PDGs to which the WLAN UE is connected.

3B.1.8 Serving WAG

The Serving WAG field contains the address(es) of the WAG(s) through which the tunnel(s) is/are established,

3B.1.9 WLAN UE Local IP Address

The WLAN UE Local IP Address field, specified in 3GPP TS 23.234 [62], represents the IPv4/IPv6 address of the WLAN UE in the WLAN AN. It is an address used to deliver the packet to a WLAN UE in a WLAN AN.

3B.1.10 WLAN UE Remote IP Address

The WLAN UE Remote IP Address field, specified in 3GPP TS 23.234 [62], represents the IPv4/IPv6 address of the WLAN UE in the network which the WLAN UE is accessing. It is an address used in the data packet encapsulated by the WLAN UE-initiated tunnel and is the source address used by applications in the WLAN UE. The WLAN UE Remote IP address is per W-APN, see section 3B.5.4.4.

3B.2 Data related to registration

3B.2.1 User Status

The User Status field identifies the registration status of the I-WLAN User. The User Status shall be either REGISTERED, in which case there is an associated Serving 3GPP AAA Server Name stored at the HSS, or UNREGISTERED, in which case no 3GPP AAA Server Name stored.

3B.3 Data related to authentication and ciphering

3B.3.1 Random Number (RAND), Signed Response (SRES) and Ciphering Key (Kc)

Random Number (RAND), Signed Response (SRES) and Ciphering Key (Kc) fields form a triplet vector used for authentication and encryption as defined in 3GPP TS 43.020 [31].

In I-WLAN for SIM based users, triplet vectors are calculated in the 2G AuC and provided to the 2G HLR/HSS (see GSM 12.03 [36]). For USIM based users, triplet vectors are derived from quintuplet vectors in the 3G HLR/HSS if needed (see 3GPP TS 33.102 [52]).

A set of up to 5 triplet values are sent from the 2G HLR/HSS to the 3GPP AAA Server upon request..

3B.3.2 Random Challenge (RAND), Expected Response (XRES), Cipher Key (CK), Integrity Key (IK) and Authentication Token (AUTN)

Random Challenge (RAND), Expected Response (XRES), Cipher Key (CK), Integrity Key (IK) and Authentication Token (AUTN) fields form a quintuplet vector used for user authentication, data confidentiality and data integrity as defined in 3GPP TS 33.102 [52].

In I-WLAN, a set of quintuplet vectors are calculated in the AuC, and up to 5 quintuplets are sent from the HLR/HSS to the 3GPP AAA Server upon request (see 3GPP TS 29.002 [27]).

3B.3.3 Master Key (MK)

The Master Key (MK) field is defined in 3GPP TS 33.234 [18]. It enables keys to be derived.

3B.3.4 Transient EAP Keys (TEKs)

The Transient EAP Keys (TEKs) field is defined in 3GPP TS 33.234 [18] and are used to protect the EAP packets.

3B.4 Data related to session

3B.4.1 Session Identifier

The Session Identifier field, specified in 3GPP TS 29.234 [63], indicates a unique Diameter signalling session specific to the user.

3B.4.2 Session-Timeout

The Session-Timeout field, specified in 3GPP TS 29.234 [63], indicates the maximum period for a session measured in seconds. It is used for re-authentication purposes. If this field does not appear, the WLAN AN shall apply default time intervals.

3B.4.3 Quota

The Quota field indicates the amount of credits available for the UE for the present session. It is measured in terms of Time or Volume.

3B.5 Operator Determined Barring general data

3B.5.1 WLAN Access

The WLAN Access flag is defined in 3GPP TS 29.234 [63]. It enables operators to apply barring of –I-WLAN access. The parameter takes either of the following values:

- Enable WLAN access;
- Bar WLAN access;

3B.5.2 WLAN Tunnelling

The WLAN Tunnelling flag is defined in 3GPP TS 29.234 [63]. It allows operator to disable all W-APNs at one time for a given user within an I-WLAN 3GPP PS based services architecture. If there is a conflict between this item and the "access allowed" flag of any W-APN, the most restrictive will prevail. The parameter takes either of the following values:

- Enable all W-APNs for a subscriber;
- Bar all W-APNs for a subscriber;

3B.5.3 WLAN Direct IP Access

The WLAN Direct IP Access flag is defined in 3GPP TS 29.234 [63]. It indicates whether or not the user has direct access to external IP networks, e.g. Internet, from the WLAN Access Network. The parameter takes either of the following values:

- Enable direct access to external IP networks;
- Bar direct access to external IP networks.

3B.5.4 W-APN Authorised

The W-APN Authorised field is specified in 3GPP TS 29.234 [63]. It contains authorization information for each W-APN. This parameter indicates the list of allowed W-APNs, the environment where the access is allowed and optionally the charging data specific for that W-APN and the Static IP address.

3B.5.4.1 W-APN Identifier

See subclause 3B.1.5.

3B.5.4.2 W-APN Barring Type

The W-APN Barring Type field is specified in 3GPP TS 29.234 [63]. It indicates the subscriber access type to the home and visited network's services. The parameter takes either of the following values:

- Allow access to all W-APNs regardless of whether the subscriber is located in a VPLMN or in the HPLMN;
- Prohibit access to all W-APNs that access a PDG within the HPLMN when the subscriber is located in a VPLMN;
- Prohibit access to all W-APNs that access a PDG within the VPLMN when the subscriber is located in a VPLMN;
- Prohibit access to all W-APNs that access a PDG within the HPLMN when the subscriber is located in the HPLMN.

3B.5.4.3 W-APN Charging Data

The W-APN Charging Data field is specified in 3GPP TS 29.234 [63]. When this parameter is present, it supersedes the general charging information to be applied for the subscriber. See subclause 3B.7.

3B.5.4.4 WLAN UE Remote IP Address

WLAN UE IP Address field identifies the IPv4/IPv6 address that the operator has statically assigned to the WLAN UE. See subclause 3B.1.12.

3B.5.4.X Maximum Number of Accesses

The Maximum Number of Accesses is defined in 3GPP TS 29.234[63]. It enables operators to specify the maximum number of concurrent accesses per W-APN.

3B.5.4.Y Access Number

Access Number is an integer counter kept at the PDG per W-APN.

3B.5.5 Access Independence Flag

The Access Independence Flag is defined in 3GPP TS 29.234 [63]. It enables operators to authenticate a subscriber accessing the I-WLAN by WLAN 3GPP IP Access independently of a previous WLAN 3GPP Direct WLAN Access. The parameter takes either of the following values:

- Allow access to WLAN 3GPP IP Access independently of a previous WLAN 3GPP Direct Access.
- Prohibit access to WLAN 3GPP IP Access independently of a previous WLAN 3GPP Direct Access.

3B.5.6 I-WLAN Access Type

The I-WLAN Access Type field is defined in 3GPP TS 29.234 [63]. It indicates the types of access the subscriber has used to access to the IWLAN. The parameter takes either of the following values:

- WLAN 3GPP IP Access;
- WLAN 3GPP Direct Access.

3B.6 QoS general data

3B.6.1 Max Requested Bandwidth

The Max Requested Bandwidth field, specified in 3GPP TS 29.234 [63], indicates the Max requested bandwidth.

3B.6.2 Routing Policy

The Routing Policy field, specified in 3GPP TS 29.234 [63], defines a packet filter for an IP flow.

3B.7 Data related to Charging

3B.7.1 Charging Data

The Charging Data field identifies the Charging Characteristics plus the Charging Nodes to be applied per user for all W-APNs or per user for individual W-APNs.

3B.7.1.1 Charging Characteristics

Charging Characteristics field is defined in 3GPP TS 32.215 [63]. It indicates the charging type to be applied to the user tunnel.

3B.7.2 Primary OCS Charging Function Name

The Primary OCS Charging Function Name field identifies the Primary OCS Function node that performs on-line based charging. The format is specified in 3GPP TS 29.234 [63].

3B.7.3 Secondary OCS Charging Function Name

The Secondary OCS Charging Function Name field identifies the Secondary OCS Charging Function node that performs on-line based charging. The format is specified in 3GPP TS 29.234 [63].

3B.7.4 Primary Charging Collection Function Name

The Primary Charging Collection Function Name field identifies the primary Charging Collection Function node that provides off-line charging support for the IMS subscribers. The format is specified in 3GPP TS 29.234 [63].

3B.7.5 Secondary Charging Collection Function Name

The Secondary Charging Collection Function Name field identifies the secondary Charging Collection Function node that provides off-line charging support for the IMS subscribers. The format is specified in 3GPP TS 29.234 [63].

**** End of change #1 ****

****** Start of change #2 ******

5.5 I-WLAN Service Data Storage

Table 5.5: Overview of data used for I-WLAN services

PARAMETER	Subclause	HSS	3GPP AAA Server	3GPP AAA Proxy	PDG	WAG	TYPE
IMSI	3B.1.1	M	M				P
MSISDN	3B.1.2	M	M	M	M	M	P
W-APN	3B.1.3	M	M		M		P
List of authorized visited network identifiers	3B.1.4	M					P
3GPP AAA Proxy Identifier	3B.1.5		M		M	M	T
3GPP AAA Server Name	3B.1.6	M		M	M	C	T
Serving PDG List	3B.1.7		M	M			P
Serving WAG	3B.1.8		M	M	M		P
WLAN UE Local IP address	3B.1.9				M	M	T
WLAN UE Remote IP address	3B.1.10	C	C		M		P
User Status	3B.2.1		M				T
RAND, SRES, Kc	3B.3.1	M	M		-		T
RAND, XRES CK, IK, AUTN	3B.3.2		M		-		T
Master Key (MK)	3B.3.3		M				T
Transient EAP Keys (TEKs)	3B.3.3		M				T
Session Identifier	3B.4.1		M				T
Session-Timeout	3B.4.2		C				P
Quota	3B.4.3		C				P
WLAN Access	3B.5.1	M					P
WLAN Tunnelling	3B.5.2	M					P
WLAN Direct IP Access	3B.5.3	M					P
W APN Authorised	3B.5.4	M					P
W APN Identifier	3B.5.4.1						P
W-APN Barring Type	3B.5.4.2	M					P
W-APN Charging Data	3B.5.4.3	C			C		P
WLAN UE Remote IP Address	3B.5.4.4	C			P		P
Access Independence Flag	3B.5.5	M					P
I-WLAN Access Type	3B.5.6	M					P
Max Requested Bandwidth	3B.6.1		P		T		P
Routing Policy	3B.6.2				C	C	T
Charging Data	3B.7.1	M			M		P
Charging Characteristics	3B.7.1.1	M	-		M		P
Primary OCS Charging Function Name	3B.7.2	M			M		P
Secondary OCS Charging Function Name	3B.7.3	M			M		P
Primary Charging Collection Function Name	3B.7.4	M			M		P
Secondary Charging Collection Function Name	3B.7.5	M			M		P
Maximum-Number-Accesses	3B.5.4.X	M	M				P
Access-Number	3B.5.4.Y		M				T

****** End of change #2**

3GPP TSG CN WG4 Meeting #27
Cancun, Mexico, 25th – 29th April 2005

C4-050876

CR-Form-v7

CHANGE REQUEST

⌘ **29.230** **CR** 051 ⌘ **rev** **1** ⌘ Current version: **6.3.0** ⌘

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

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

Title:	⌘	Addition of Maximum-Number-Accesses AVP
Source:	⌘	Nokia, Ericsson
Work item code:	⌘	WLAN-IW
Date:	⌘	29/04/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	SA3 have mandated that the network shall be able to configure a maximum number of simultaneous accesses to a give W-APN. This CR and the accompanying CRs to 23.008 and 29.234 enable this in the stage 3.
Summary of change:	⌘	Addition of Maximum-Number-Accesses AVP to the AVP list
Consequences if not approved:	⌘	Loophole in the spec that allows the user unlimited number of accesses to a W-APN

Clauses affected:	⌘	8.3.2.1, 10.1			
Other specs affected:	⌘	**Y** / **N**		⌘	29.234-062, 23.008-151
		X /	Other core specifications		
		/ **X**	Test specifications		
		/ **X**	O&M Specifications		
Other comments:	⌘	CRs C1-050874, C1-050875 are related CRs			

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 change #1 ******

7 Attribute-Value-Pair codes

The AVP codes are used together with the vendor identifier to identify each attribute uniquely. There are multiple AVP namespaces. The IETF IANA namespace, that is, the AVPs with vendor identifier zero or without vendor identifier, is controlled by IANA. Each vendor controls the AVP codes within their AVP namespaces.

7.1 3GPP specific AVP codes

The 3GPP specific AVPs have the Vendor-Specific bit ('V' bit) set in the AVP header and they carry the 3GPP's vendor identifier in the Vendor-ID field of the AVP header. The 3GPP specific AVP codes are presented in the following table.

Table 7.1: 3GPP specific AVP codes

AVP Code	Attribute Name	Data Type	Specified in the 3GPP TS
Note: The AVP codes from 1 to 255 are reserved for backwards compatibility with 3GPP RADIUS Vendor Specific Attributes (See TS 29.061 [13])			
Note: The AVP codes from 256 to 299 are reserved for future use.			
300	Authentication-Method		29.234 [6]
301	Authentication-Information-SIM		
302	Authorization -Information-SIM		
303	WLAN-User-Data		
304	Charging-Data		
305	WLAN-Access		
306	WLAN- 3GPP-IP-Access		
307	APN-Authorized		
308	APN-Id		
309	APN-Barring-Type		
310	WLAN-Direct-IP-Access		
311	Session-Request-Type		
312	Routing-Policy		
313	Max-Requested-Bandwidth		
314	Charging-Characteristics		
315	Charging-Nodes		
316	Primary-OCS-Charging-Function-Name		
317	Secondary-OCS-Charging-Function-Name		
318	3GPP-AAA-Server-Name		
XXX	Maximum-Number-Accesses	Unsigned32	
Note: The AVP codes from YYY~~319~~ to 399 are reserved for TS 29.234			
			29.109 [7]
Note: The AVP codes from 400 to 499 are reserved for TS 29.109			
500	Abort-Cause	Enumerated	29.209 [8]
501	Access-Network-Charging-Address	Address	
502	Access-Network-Charging-Identifier	Grouped	
503	Access-Network-Charging-Identifier-Value	OctetString	
504	AF-Application-Identifier	OctetString	
505	AF-Charging-Identifier	OctetString	
506	Authorization-Token	OctetString	
507	Flow-Description	IPFilterRule	
508	Flow-Grouping	Grouped	
509	Flow-Number	Unsigned32	
510	Flows	Grouped	
511	Flow-Status	Enumerated	
512	Flow-Usage	Enumerated	
513	Gq-Specific-Action	Enumerated	
514	Max-Requested-Bandwidth	Unsigned32	
515	Max-Requested-Bandwidth-DL	Unsigned32	
516	Max-Requested-Bandwidth-UL	Unsigned32	
517	Media-Component-Description	Grouped	
518	Media-Component-Number	Unsigned32	
519	Media-Sub-Component AVP	Grouped	
520	Media-Type	Enumerated	
521	RR-Bandwidth	Unsigned32	
522	RS-Bandwidth	Unsigned32	
523	SIP-Forking-Indication	Enumerated	
Note: The AVP codes from 524 to 599 are reserved for TS 29.209			
600	Visited-Network-Identifier	OctetString	29.229 [2]
601	Public-Identity	UTF8String	
602	Server-Name	UTF8String	
603	Server-Capabilities	Grouped	
604	Mandatory-Capability	Unsigned32	
605	Optional-Capability	Unsigned32	
606	User-Data	OctetString	
607	SIP-Number-Auth-Items	Unsigned32	
608	SIP-Authentication-Scheme	UTF8String	
609	SIP-Authenticate	OctetString	

610	SIP-Authorization	OctetString	
611	SIP-Authentication-Context	OctetString	
612	SIP-Auth-Data-Item	Grouped	29.229 [2], 29.234 [6]

613	SIP-Item-Number	Unsigned32	
614	Server-Assignment-Type	Enumerated	
615	Deregistration-Reason	Grouped	
616	Reason-Code	Enumerated	
617	Reason-Info	UTF8String	
618	Charging-Information	Grouped	
619	Primary-Event-Charging-Function-Name	DiameterURI	
620	Secondary-Event-Charging-Function-Name	DiameterURI	
621	Primary-Charging-Collection-Function-Name	DiameterURI	
622	Secondary-Charging-Collection-Function-Name	DiameterURI	29.229 [2]
623	User-Authorization-Type	Enumerated	
624	User-Data-Already-Available	Enumerated	
625	Confidentiality-Key	OctetString	
626	Integrity-Key	OctetString	
627	User-Data-Request-Type	Enumerated	
628	Supported-Features	Grouped	
629	Feature-List-ID	Unsigned32	
630	Feature-List	Unsigned32	
631	Supported-Applications	Grouped	
Note: The AVP codes from 632 to 699 are reserved for TS 29.229.			
700	User-Identity	Grouped	
701	MSISDN	OctetString	
702	User-Data	OctetString	
703	Data-Reference	Enumerated	
704	Service-Indication	OctetString	29.329 [4]
705	Subs-Req-Type	Enumerated	
706	Requested-Domain	Enumerated	
707	Current-Location	Enumerated	
708	Identity-Set	Enumerated	
Note: The AVP codes from 709 to799 are reserved for TS 29.329.			
			32.299 [5]
Note: The AVP codes from 800 to 899 are reserved for TS 32.299			
900	TMGI	OctectString	
901	Required-MBMS-Bearer-Capabilities	UTF8String	
902	MBMS-StartStop-Indication	Enumerated	
903	MBMS-Service-Area	OctectString	29.061 [13]
904	MBMS-Session-Duration	Unsigned32	
905	Alternative-APN	UTF8String	
906	MBMS-Service-Type	Enumerated	
Note: The AVP codes from 907 to 999 are reserved for TS 29.061			
1000	Bearer-Usage	Enumerated	
1001	Charging-Rule-Install	Grouped	
1002	Charging-Rule-Remove	Grouped	
1003	Charging-Rule-Definition	Grouped	
1004	Charging-Rule-Base-Name	OctetString	
1005	Charging-Rule-Name	OctetString	
1006	Event-Trigger	Enumerated	
1007	Metering-Method	Enumerated	
1008	Offline	Enumerated	
1009	Online	Enumerated	
1010	Precedence	Unsigned32	29.210 [15]
1011	RAT-Type	Enumerated	
1012	Reporting-Level	Enumerated	
1013	TFT-Filter	IPFilterRule	
1014	TFT-Packet-Filter-Information	Enumerated	
1015	ToS-Traffic-Class	OctetString	
Note: The AVP codes from 1016 to 1099 are reserved for TS 29.210			
1100	Served-User-Identity	Groupe	
1101	VASP-ID	UTF8Str	
1102	VAS-ID	UTF8Str	
1103	Trigger-Event	Enumer	
1104	Sender-Address	UTF8Str	
1105	Initial-Recipient-Address	Groupe	
1106	Result-Recipient-Address	Groupe	
1107	Sequence-Number	Unsigne	

1108	Recipient-Address	UTF8Str	29.140 [16]
1109	Routeing-Address	UTF8Str	
1110	Originating-Interface	Enumer	
1111	Delivery-Report	Enumer	
1112	Read-Reply	Enumer	
1113	Sender-Visibility	Enumer	
1114	Service-Key	UTF8Str	
1115	Billing-Information	UTF8Str	
1116	Status	Group	
1117	Status-Code	UTF8Str	
1118	Status-Text	UTF8Str	
Note: The AVP codes from 1119 to 1199 are reserved for TS 29.140			

**** End of change #1