3GPP TSG CN Plenary Meeting #26 **NP-040541**
8th – 10th December 2004 Athens, Greece.

Source: TSG CN WG4

Title: Corrections on WLAN

Agenda item: 9.17

Document for: APPROVAL

Spec	CR	Rev	Doc-2nd-Level N4-040	Phase	Subject	Cat	Ver_C
29.234	001	2	1694	Rel-6	PLMN advertising and selection	D	6.0.0
29.234	002		1362	Rel-6	WLAN User Profile update	F	6.0.0
29.234	003		1363	Rel-6	Charging related data from 3GPP AAA Server to PDG	B	6.0.0
29.234	004	1	1527	Rel-6	3GPP WLAN IP Access parameter rename	B	6.3.0
29.234	005	1	1577	Rel-6	Static Remote IP address	F	6.0.0
29.234	006		1366	Rel-6	Removal of “Scenario” wording	D	6.0.0
29.234	007		1367	Rel-6	Editorial correction on Auth-Req-Type AVP	D	6.0.0
29.234	008	1	1578	Rel-6	Online charging failure report	F	6.0.0
29.234	009		1369	Rel-6	Rejection of Multiple WLAN connections	B	6.0.0
29.234	010		1371	Rel-6	Application-Ids to Wa, Wd, Wm and Wg	F	6.0.0
29.234	012	2	1695	Rel-6	Wd Interface RADIUS profile clarifications	F	6.0.0
29.234	014	2	1696	Rel-6	RADIUS Profile for Wa and Wd	F	6.0.0
29.234	015	1	1585	Rel-6	Addition of ABNF definitions missing onWa, Wd Wm, Wg interfaces	B	6.0.0
29.234	016	1	1586	Rel-6	Access Independence for WLAN 3GPP IP access	B	6.0.0
29.234	019	1	1591	Rel-6	Editorial Modifications	D	6.0.0
29.234	021	1	1592	Rel-6	Re-authentication clarification on the Wa interface	F	6.0.0
29.234	023	1	1593	Rel-6	To replace ‘Permanent User ID’ by ‘User Id’	F	6.0.0
29.234	025	2	1697	Rel-6	To make VPLMN-Id Conditional in Wd interface	F	6.0.0
29.234	026		1414	Rel-6	Addition of calling station id in DEA. Deletion of the same from DER.	F	6.0.0
29.234	028	1	1596	Rel-6	Editorial Changes	D	6.0.0
29.234	029		1481	Rel-6	Handling of Information Element marked as (M), (C) or (O)	D	6.0.0
23.003	092	2	1693	Rel-6	'otherrealm' format of Decorated NAI	F	6.4.0
23.003	093	1	1575	Rel-6	Definition of Alternative NAI	B	6.4.0
23.008	142	1	1572	Rel-6	WLAN-IW data handling: additions to 23.008	B	6.3.0

3GPP TSG-CN WG4 Meeting #25 ***N4-041362***

Seoul, KOREA. 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **002** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	WLAN User Profile update
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	04/11/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:
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: ⌘ According to approved S2-042934 CR, the WLAN User Profile has been updated:

–1 MSISDN is now mandatory

–2 Charging Info now includes Charging Characteristics as defined in TS 32.215

–3 Charging information can be defined also per W-APN

–4 Added Optional Static Remote WLAN UE IP address

–5 Re-definition of barring flags for the W-APN according to TS 22.234/23.234

Summary of change: ⌘ Alignment with agreed SA2 User Profile:

–6 MSISDN is made mandatory in the profile downlaoded to the 3GPP AAA Server. Also MSISDN AVP is replaced by already existing Subscription-ID AVP (from IETF Diameter Credit Control draft) set to MSISDN value,

–7 Charging Info includes Charging Characteristics as defined in TS 32.215

		–8 Charging node for on-line is changed to OCS instead of ECF as it as described in TS 32.240. –9 Charging information defined also per W-APN, –10 Optional Static Remote WLAN UE IP address as part of the user profile has not been included since it is covered in CR N4-041365. –11 Re-definition of barring flags for the W-APN according to TS 22.234. Also APN-Authorisation AVP has been changed to APN-Barring-Type AVP since the former was very similar to an existing one (APN-Authorised) and indicates better the purpose of the AVP. –12 Editorial change: The AVP code reference has been removed from each AVP description since this information is already present is the AVPs table. It is also aligned with the decision made in the IMS specs on the same issue in the Sophia Meeting.
Consequences if not approved:	⌘	Misalignment between Stage 2 and 3 for the definition of the WLAN user profile.

Clauses affected:	⌘	2, 10			
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.

****** First modified section ******

2 References

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

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

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

[2] 3GPP TR 22.934: "Feasibility Study on 3GPP system to WLAN interworking"

[3] 3GPP TR 23.934: "3GPP system to WLAN Interworking; Functional and architectural definition"

[4] 3GPP TS 23.234: "3GPP system to 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, TS 29.229, Protocol details"

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

[8] IETF Draft: "Diameter Extensible Authentication Protocol (EAP) Application", draft-ietf-aaa-eap-06.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, "Attributes for Access Network Location and Ownership Information", http://www.ietf.org/internet-drafts/draft-tschofenig-geopriv-radius-lo-00.txt, work in progress

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

[18] 3GPP TS 33.234: "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"

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

****** Second modified section ******

10 Information Elements Contents

10.1 AVPs

The following table describes the Diameter AVPs defined for the WLAN reference point, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted. The Vendor-Id header of all AVPs defined in this specification shall be set to 3GPP (10415).

Only those AVPs defined by 3GPP TS 29.234 reference point are listed here.

Table 10.1.1: Diameter Multimedia Application AVPs

				AVP Flag rules				
Attribute Name	**AVP Code**	**Section defined**	**Value Type**	**Shall**	**May**	**Should not**	**Must not**	**May Encr.**
Authentication-Method	~~X~~tbd	~~x.1.5~~	~~UTF8String~~	~~M, V~~				~~No~~
~~Authentication-Information-SIM~~	tbd~~X~~	~~x.1.6~~	~~OctetString~~	~~M, V~~				~~No~~
~~Authorization-Information-SIM~~	tbd~~X~~	~~x.1.7~~	~~OctetString~~	~~M,V~~				~~No~~
~~WLAN-User-Data~~	tbd~~X~~	~~x.1.8~~	~~Grouped~~	~~M, V~~				~~No~~
~~WLAN-Access~~	tbd~~X~~	~~x.1.11~~	~~Enumerated~~	~~M, V~~				~~No~~
~~WLAN-Tunneling~~	tbd~~X~~	~~x.1.12~~	~~Enumerated~~	~~M, V~~				~~No~~
~~APN-Authorised~~	tbd~~X~~	~~x.1.14~~	~~Grouped~~	~~M, V~~				~~No~~
~~APN-Id~~	tbd~~X~~	~~x.1.15~~	~~OctetString~~	~~M, V~~				~~No~~
~~APN-Barring-Type~~~~Authorisation~~	tbd~~X~~	~~x.1.16~~	~~Enumerated~~	~~M, V~~				~~No~~
~~Local-Access~~	tbd~~X~~	~~x.1.17~~	~~Enumerated~~	~~M, V~~				~~No~~

	EAP payload	tbdX	x.1.20	OctetString	M, V				No
	Auth Req Type	tbdX	x.1.21	Enumerated	M,V				No
	EAP Master Session Key	tbdX	x.1.22	OctetString	M, V				No
	Session-Request-Type	tbdX	x.1.23	Enumerated	M, V				No
	Routing-Policy	tbdX	x.1.24	OctetString	M, V				No
	Max-Requested-Bandwidth	tbdX	x.1.26	Enumerated	M, V				No
	Charging-Data	tbd	10.1.10	Grouped	M, V				No
	Charging-Characteristics	tbd	10.1.a	Grouped	M, V				No
	Charging-Nodes	tbd	10.1.b	Grouped	M, V				No
	Primary-OCS-Charging-Function-Name	tbd	10.1.c	DiameterIdentity	M, V				No
	Secondary-OCS-Charging-Function-Name	tbd	10.1.d	DiameterIdentity	M, V				No
	NOTE 1: The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see IETF RFC 3588 [7].								

10.1.1 Auth-Session-State

Between the 3GPP AAA server and the HSS, Diameter sessions are implicitly terminated. An implicitly terminated session is one for which the server does not maintain state information. The client does not need to send any re-authorization or session termination requests to the server.

The Diameter base protocol includes the Auth-Session-State AVP as the mechanism for the implementation of implicitly terminated sessions.

The client (server) shall include in its requests (responses) the Auth-Session-State AVP set to the value NO_STATE_MAINTAINED (1), as described in IETF RFC 3588 [7]. As a consequence, the server does not maintain any state information about this session and the client does not need to send any session termination request. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP shall be present in requests or responses.

10.1.2 User-Name

The User-Name AVP is defined in the IETF RFC 3588 [7] and contains the user identity.

For the WLAN Wx referende point, the User-Name AVP contains the IMSI of the subscriber.

10.1.3 Visited-Network-Identifier

The Visited-Network-Identifier AVP is defined in 3GPP TS 29.229[6] and indicates the 3GPP VPLMN where the user is roaming.

10.1.4 SIP-Auth-Data-Item

The SIP-Auth-Data-Item AVP is defined in 3GPP TS 29.229[6]. However three new more conditional AVPs are needed for WLAN Wx reference point.

AVP format

SIP-Auth-Data-Item :: = < AVP Header : TBD >

[SIP-Item-Number]

[SIP-Authentication-Scheme]

[SIP-Authenticate]

[SIP-Authorization]

[SIP-Authentication-Context]

[Confidentiality-Key]

[Integrity-Key]

[Authentication-Method]

[Authentication-Information-SIM]

[Authorization-Information-SIM]

* [AVP]

10.1.5 Authentication-Method

The Authentication-Method AVP (AVP code X) is of type UTF8String and indicates the authentication method required for the user. The following values are defined:

WLAN_EAP_SIM (0)

The UE indicates to the HSS that the required authentication method is EAP/SIM.

WLAN_EAP_AKA (1)

The UE indicates to the HSS that the required authentication method is EAP/AKA.

10.1.6 Authentication-Information-SIM

The Authentication-Information-SIM AVP (AVP code X) is of type OctetString and contains the concatenation of authentication challenge RAND and the ciphering key Kc.

10.1.7 Authorization –Information-SIM

The Authentication-Information-SIM AVP (AVP code X) is of type OctetString and contains the response SRES.

10.1.8 WLAN-User-Data

The WLAN-User-Data AVP (AVP code X) 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>

[{ MSISDN Subscription-ID }]

{ WLAN-Access }

{ WLAN-Tunneling }

[Session-Timeout]

1* { Charging-Data }

*[APN-Authorised]

{ Local-Access }

* [AVP]

10.1.9 MSISDN

The MSISDN AVP (AVP code 101) is defined in 3GPP TS 29.329 [x]. This identification could be used for example used for charging purposes.

Editor's Note: The optionality/presence could be modified by the SA1 and SA5 decision.

10.1.10 Charging-Information10.1.10 Charging-Data

The Charging-Mode Data AVP (AVP code 19) is of type is of type Grouped, and contains the addresses of the charging functions. It is defined in 3GPP TS 29.229 [6].

AVP format

Charging-Data::= <AVP header: TBD>

{ Charging-Characteristics }

{ Charging-Nodes}

* [AVP]

When this AVP is present within the APN-Authorised AVP, charging data apply to the specific W-APN within the APN-Authorised AVP and shall prevail over the general received Charging-Data.

10.1.11 WLAN-Access

The WLAN-Access AVP (AVP code xx) is of type Enumerated, and allows operators to determine barring of 3GPP-WLAN interworking subscription. The following values are defined:

WLAN_SUBSCRIPTION_ALLOWED (0)

The subscriber has WLAN subscription.

WLAN_SUBSCRIPTION_BARRED (1)

The subscriber has no WLAN subscription.

10.1.12 WLAN-Tunneling

The WLAN-Tunneling AVP (AVP code xx) is of type Enumerated, and allows operator to disable all W-APNs for a subscriber at one time. If there is a conflict between this item and the "access allowedAPN-Barring type" flag of any W-APN, the most restrictive will prevail. The following values are defined:

WLAN_APNS_ENABLE (0)

Enable all APNs for a subscriber.

WLAN_APNS_DISABLE (1)

Disable all APNs for a subscriber.

10.1.13 Session-Timeout

The Session-TimeOut AVP (AVP code 27) is defined in IETF RFC 3588 [7] and indicates the maximum period for a session measured in seconds.

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

10.1.14 APN-Authorised

The APN-Authorised AVP (AVP code xx) is of type Grouped and contains authorization information for the APNs. This AVP indicates the list of allowed W-APNs and the environment where the access is allowed (visited or home PLMN).

AVP format

APN-Authorised::= <AVP header: TBD>

{ APN-Id }

{ APN-Authorisation Barring-Type }

[Charging-Data]

* [AVP]

10.1.15 APN-Id

The APN-Id AVP (AVP code xx) 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.

10.1.16 APN-Authorisation10.1.16 APN-Barring-Type

The APN-Authorisation AVP (AVP code xx) is of type Enumerated, and contains a flag indicating whether access is allowed in visited PLMNs or in the home PLMN.

WLAN_APN_NO_BARRING (0)

Access is allowed in visited PLMNs and home PLMN.

WLAN_APN_HOME_BARRED_WHEN_ROAMING (01)

The subscriber is barred to activate the W-APN that access a PDG within the HPLMN when he is located in a VPLMN Access is allowed in home PLMN only.

WLAN_APN_VISITED_BARRED (12)

The subscriber is barred to activate the W-APN that access a PDG within the VPLMN when he is located in a VPLMN Access is allowed in visited PLMNs and home PLMN.

WLAN_APN_HOME_BARRED (3)

The subscriber is barred to activate the W-APN that access a PDG within the HPLMN when he is located in the HPLMN.

10.1.17 Local-Access

The Local-Access AVP (AVP code xx) is of type Enumerated, and indicate whether the user has direct access to external IP networks, e.g. Internet, from the WLAN Access Network or not.

WLAN_LOCAL_ACCESS (0)

The user is allowed to access directly to external IP networks.

WLAN_NO_LOCAL_ACCESS (1)

The user is not allowed to access directly to external IP networks.

10.1.18 Server-Assignment-Type

The Server-Assignment-Type AVP (AVP code 15) 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.

10.1.19 Deregistration-Reason

The Deregistration-Reason AVP (AVP code 16) is defined in 3GPP TS 29.229 [6] and indicates reason for a de-registration operation.

This grouped AVP contains a Reason-Code AVP to indicate the reason for the de-registration. Reasons are listed in 3GPP TS 29.229 [6]. Wx reference point defines as valid only PERMANENT_TERMINATION value.

10.1.20 EAP-Payload

The EAP-Payload AVP (AVP code xx) is defined in the IETF draft ietf-aaa-eap-08.txt [8] and contains the encapsulated EAP packet that is being exchanged between the EAP client and the home Diameter server.

10.1.21 Auth-Req-Type

The Auth-Req-Type AVP (AVP code xx) is of type Enumerated and indicates the action that the PDG is asking to the 3GPP AAA Server to perform (Authentication, authorization or both). Wm interface only makes use of the AUTHENTICATION_ONLY value. It is defined in the IETF draft ietf-aaa-eap-08.txt [8]

10.1.22 EAP-Master-Session-Key

The EAP-Master-Session-Key AVP (AVP code xx) is of type OctetString and contains keying material for protecting the communications between the user and the NAS. It is defined in the IETF draft-ietf-aaa-eap-08.txt [8]

10.1.23 Session-Request-Type

The Session-Request-Type AVP (AVP code xx) is of type Enumerated and indicates the action that the PDG is asking to the 3GPP AAA Server to perform (authorization or routing policy). The following values are defined:

AUTHORIZATION REQUEST (0)

The PDG is requesting authorization for a user for a given W-APN.

ROUTING POLICY (1)

The PDG is indicating that routing policy information is present.

10.1.24 Routing-Policy

The Routing-Policy AVP (AVP code xx) is of type OctetString and indicates routing policies of the tunnel set up.

Editor's Note: Its exact format is ffs.

10.1.25 Subscription-ID

The Subscription-ID AVP (AVP code xx) is of type Enumerated and indicates the user identity to be used for charging purposes. It is defined in the IETF Diameter Credit-Control Application draft [19].

WLAN shall make use only of the value MSISDN. This grouped AVP shall set the sub-AVP Subscription-Id-Type to value "END_USER_E164" and shall set the sub-AVP Subscription-Id-Data to the MSISDN value.

10.1.26 Max-Requested-Bandwidth

The Max-Requested-Bandwidth AVP (AVP code xx) is of type OctetString and indicates the Max requested bandwidth. If present, shall be sent from the 3GPP AAA Server to the PDG.

10.1.27 Routing Policy

The Routing Policy AVP (AVP code tbd) is of type IPFilterRule, and defines a packet filter for an IP flow with the following information:

8Direction (in or out)

9Source and destination IP address (possibly masked)

10Protocol

11Source and destination port (list or ranges)

Where the protocol type shall be set to ESP (50).

The IPFilterRule type shall be used with the following restrictions:

8Only the Action "permit" shall be used.

9No "options" shall be used.

10The invert modifier "!" for addresses shall not be used.

11The keyword "assigned" shall not be used.

12For direction "out", an IPv4 destination IP address shall not be wildcarded. For direction "out", the 64 bits network prefix of an IPv6 destination IP address shall not be wildcarded.

The Flow description AVP shall be used to describe a single IP flow.

The direction "in" refers to uplink IP flows, and the direction "out" refers to downlink IP flows.

10.1.a Charging-Characteristics

The Charging-Characteristics AVP is of type Integer, and contains the charging mode to be applied as described in 3GPP TS 32.215 [xx].

10.1.b Charging-Nodes

The Charging-Nodes AVP is of type Grouped, and contains the addresses of the charging functions, as described in 3GPP TS 32.240 [yy].

AVP format

Charging-Data::= <AVP header: TBD>

[Primary-OCS-Charging-Function-Name]

[Secondary-OCS-Charging-Function-Name]

{ Primary-Charging-Collection-Function-Name }

[Secondary-Charging-Collection-Function-Name]

* [AVP]

10.1.c Primary-OCS-Charging-Function-Name

The Primary-OCS-Charging-Function-Name AVP (AVP code tbd) is of type DiameterIdentity, and defines the address of the Primary Online Charging System (OCS)

10.1.d Secondary-OCS-Charging-Function-Name

The Secondary-OCS-Charging-Function-Name AVP (AVP code tbd) is of type DiameterIdentity, and defines the address of the Secondary Online Charging System (OCS).

When this value is not present, the PDG shall dynamically assign an IP address to the WLAN UE.

10.1.e Primary-Charging-Collection-Function-Name

The Primary-Charging-Collection-Charging-Function-Name AVP is defined in 3GPP TS 29.229 [6] and contains the address of the Primary Event Charging Function.

~~10.1.f Secondary-Charging-Collection-Function-Name~~

~~The Secondary-Event-Charging-Collection-Function-Name AVP is defined in 3GPP TS 29.229 [6] and contains the address of the Secondary Event Charging Function.~~

3GPP TSG-CN WG4 Meeting #25 ***N4-041363***

Seoul, KOREA. 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **003** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Charging related data from 3GPP AAA Server to PDG
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	04/11/2004
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:	⌘	According to approved CR S2-042930: "The 3GPP AAA Server to provide the PDG with charging data (subscribed Charging Characteristics or W-APN Charging Characteristics) for 3GPP PS based services charging." This is not currently performed in the TS 29.234, where the charging information is only downloaded from the HSS to the 3GPP AAA Server upon authorisation success.
Summary of change:	⌘	Charging information is sent form the 3GPP AAA Server to the PDG after sucessful authorisation of the user for the requested W-APN. Charging information shall be the one provided by the HSS to the 3GPP AAA Server.
Consequences if not approved:	⌘	Charging functions are not properly performed. Misalignment between Sage 2 and 3.

Clauses affected:	⌘	8.4.1

		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.

****** First modified section ******

8.4 Procedures Description

8.4.1 Authorization Procedures

According to the requirements stated in Chapter 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 tunneling 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.

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

Table 8.4.1.1 Wm Authorization 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.
Request-Type	Session-	M	Type of Wm specific Diameter application request. The following values

	Request-Type		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 8.4.1.2: 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.

8.4.1.1.1 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:

    1 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.

        2 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.

        3 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.

        4 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.

        5 The 3GPP AAA Server shall store the PDG IP address. The 3GPP AAA Server shall download APN-User-Data AVP and the charging information as received from the HSS. The Result-Code shall be set to DIAMETER_SUCCESS.

    6 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 authorisation information shall be returned.

8.4.1.1.2 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:

b. 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.

3GPP TSG-CN WG4 Meeting #25 ***N4-041366***

Seoul, KOREA. 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **006** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Removal of "Scenario" wording
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	04/11/2004
Category:	⌘	**D**
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:	⌘	SA2 decided to remove "scenario" for the different steps of I-WLAN deployment. New names has been identified
Summary of change:	⌘	Replace –1 "Scenario 3" by "WLAN 3GPP IP Access functionality"
Consequences if not approved:	⌘	Wrong naming convention

Clauses affected:	⌘	9.1

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.

****** First modified section ******

9.1 Functionality

This; clause specifies a Diameter application that allows the following messaging to take place between the 3GPP AAA Server and the WAG for the case where the PDG is in the HPLMN, and between the 3GPP AAA Proxy and the WAG for the case where the PDG is in the VPLMN:

7 data carrying policy Enforcement rules to be applied to packets to/from WLAN AN.

8 transport per-tunnel based charging information from the WAG to the AAA Proxy/Server.

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 ~~scenario 3 are not stable yet.~~

3GPP TSG-CN WG4 Meeting #25 ***N4-041367***

Seoul, KOREA. 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **007** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Editorial correction on Auth-Req-Type AVP
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	11/11/2004
Category:	⌘	**D**
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:	⌘	Authentication Request Type information element is mapped into Auth-Req-Type AVP in both Wa and Wd Diameter reference points. However, this AVP ahould be Auth-Request-Type as per RFC3588 and RFC2284.
Summary of change:	⌘	Auth-Req-Type AVP in Wa and Wd Diameter reference points changed to Auth-Request-Type
Consequences if not approved:	⌘	Unexistant AVP – interoperability problems

Clauses affected:	⌘	Table 4.3.1.1, Table 5.4.1.1

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.

**** First modified section ****

Table 4.3.1.1: Authentication Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Username NAI	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 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.~~

~~**** Second modified section ****~~

~~**Table 5.4.1.1: Diameter EAP Request**~~

~~Information element name~~	~~Mapping to Diameter AVP~~	~~Cat.~~	~~Description~~
~~Username NAI~~	~~User-Name~~	~~M~~	~~This information element shall contain 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 authentication or authentication procedure is requested . 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~~
~~Visited-Network-Identifier~~	~~Visited-Network-Identifier~~	~~M~~	~~Identifies the VPLMN~~

3GPP TSG-CN WG4 Meeting #25 ***N4-041369***

Seoul, KOREA. 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **009** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Rejection of Multiple WLAN connections
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	04/11/2004
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: ⌘ According to approved CRs S2-042518 and S2-0402519:

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

"During the information retrieval the HSS/HLR checks if there is a 3GPP AAA server already registered to serve for the user. In case the HSS/HLR detects that another 3GPP AAA server has already registered for this user, it shall provide the current 3GPP AAA server with the previously registered AAA server address. The authentication signalling is then routed to the previously registered 3GPP AAA server"

So, according to Stage 2 when there are multiple wlan connections for the same subscriber, they have to be handled by the same 3GPP AAA Server.

Summary of change: ⌘ The HSS checks at authentication request whether the user is already registered in any 3GPP AAA Server. In this case, the HSS shall return the 3GPP AAA Server assisting the user to the requester 3GPP AAA Server. The 3GPP AAA

		Server shall make use of the redirect function to indicate to the WLAN AN or 3GPP AAA Proxy the old 3GPP AAA Server name. A note has been added to indicate that when RADIUS is used over Wa and Wd, since RADIUS does not support the redirect functionality, it is FFS how to prevent a user of having simultaneous WLAN connections handled by different 3GPP AAAA Servers as mandated by Stage 2.
Consequences if not approved:	⌘	Multiple WLAN connections, against WLAN requirements.

Clauses affected:	⌘	6.3.2.1., 6.3.1			
		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.

****** First modified section ******

6.3.2.1 WLAN Registration/DeRegistration Notification

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

- Registration of the 3GPP AAA Server of an authorised WLAN user in the HSS
- Retrieval of online charging / offline charging function addresses from HSS
- Purge procedure between the 3GPP AAA Server and the HSS
- Retrieval of WLAN subscriber profile from HSS

This procedure is used between the 3GPP AAA Server and the HSS. The procedure is invoked by the 3GPP AAA Server after a new subscriber has been authenticated and authorised by the 3GPP AAA Server:

- to register the current 3GPP AAA Server address in the HSS for a given 3GPP user.
- to de-register the current 3GPP AAA Server address in the HSS for a given 3GPP user. When

WLAN WLAN-UE has disappeared from WLAN coverage or when the OCS has initiated a disconnection, the 3GPP AAA Server informs the HSS about an ongoing disconnection process and the HSS de-registers the WLAN user.

- to download the subscriber profile under 3GPP AAA Server demand. This procedure is invoked when for some reason the subscription profile of a subscriber is lost.

The Wx interface performs these functions based on the reuse of the existing Cx server assignment command code set (SAR/SAA), see 3GPP TS 29.228 [5] and 3GPP TS 29.229 [6]. It corresponds to the combination of the operations WLAN-Registration and WLAN-Registration-Confirm for the registration procedure, Purge_WLAN_INFO and Purge_WLAN_INFO_Ack for the de-registration procedure initiated by the 3GPP AAA server and Subscriber-Profile-Request (see 3GPP TS 23.234 [4]) for the profile download procedure initiated by the 3GPP AAA server.

Table 6.3.2.1: WLAN Registration 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 requests in the HSS. When this IE contains REGISTRATION value, the HSS performs a registration of the WLAN user. When this IE contains USER_DEREGISTRATION / ADMINISTRATIVE_DEREGISTRATION / REAUTHENTICATION_FAILURE / ONLINE_CHARGING_FAILURE the HSS performs a de-registration of the WLAN user. When this IE contains NO_ASSIGNMENT value, the HSS initiates the download of the subscriber user profile towards the 3GPP AAA Server, but no registration is performed. Any other value is considered as an error case.
Routing Information (See 7.13)	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 the HSS, e.g. included in the MAA command. 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.

Table 6.3.2.2: Subscriber profile retrieval response

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	Permanent-User-Identity	M	This information element contains the permanent identity of the user, i.e., the IMSI.
Registration result	Result-Code / Experimental-	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base

	Result		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.
User Profile	User-Data	C	Relevant user profile. It shall be present when Server-Assignment-Type in the request is equal to NO_ASSIGNMENT.
Charging Information	Charging-Information	C	Addresses of the charging functions. It shall be present when Server-Assignment-Type in the request is equal to REGISTRATION and when Result-Code is equal to DIAMETER_SUCCESS. When this parameter is included, the Primary Charging Collection Function address shall be included. All other elements shall be included if they are available.

6.3.2.1.1 Detailed behaviour

When a new 3GPP subscriber has been authenticated and authorised by the 3GPP AAA Server, the 3GPP AAA Server initiates the registration towards the HSS. The HSS 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 HSS indicating the registration procedure. The subscriber is identified by the User-Name AVP.

At reception of Server-Assignment-Request command, the HSS 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, the HSS shall store the 3GPP AAA Server name for the authenticated and authorised 3GPP subscriber and set the Result-Code AVP to DIAMETER_SUCCESS in the Server-Assignment-Response command.

   - If it indicates USER_DEREGISTRATION / ADMINISTRATIVE_DEREGISTRATION / REAUTHENTICATION_FAILURE / ONLINE_CHARGING_FAILURE, the HSS 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 NO_ASSIGNMENT, the HSS shall download the relevant user identity information 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 registration/de-registration or profile download procedure shall be performed.

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

****** Second modified section ******

6.3.1 Authentication Procedures

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

- Retrieval of authentication vectors (triplets and quintuplets) from 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 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	M	Identifier that allows the home network to identify the Visited Network. 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 the HSS, e.g. included in the MAA command. 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.

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
Private 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
Authotization 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. Check that the user is allowed to roam in the visited network. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR _ROAMING_NOT_ALLOWED.

4. Check that the authentication method indicated in the request is supported. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_AUTH_METHOD_UNSUPPORTED.

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.

  5 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.

  6 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.

~~5. 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.~~

~~6. 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.~~

~~** Third modified section ****~~**

10 Information Elements Contents

10.1 AVPs

The following table describes the Diameter AVPs defined for the WLAN reference point, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted. The Vendor-Id header of all AVPs defined in this specification shall be set to 3GPP (10415).

Only those AVPs defined by 3GPP TS 29.234 reference point are listed here.

Table 10.1.1: Diameter Multimedia Application AVPs

					AVP Flag rules				
	Attribute Name	**AVP Code**	**Section defined**	**Value Type**	**Shall**	**May**	**Should not**	**Must not**	**May Encr.**
	Authentication-Method	X	x.1.5	UTF8String	M, V				No
	Authentication-Information-SIM	X	x.1.6	OctetString	M, V				No
	Authorization-Information-SIM	X	x.1.7	OctetString	M,V				No
	WLAN-User-Data	X	x.1.8	Grouped	M, V				No
	WLAN-Access	X	x.1.11	Enumerated	M, V				No
	WLAN-Tunneling	X	x.1.12	Enumerated	M, V				No
	APN-Authorised	X	x.1.14	Grouped	M, V				No
	APN-Id	X	x.1.15	OctetString	M, V				No
	APN-Authorisation	X	x.1.16	Enumerated	M, V				No
	Local-Access	X	x.1.17	Enumerated	M, V				No
	EAP-payload	X	x.1.20	OctetString	M, V				No
	Auth-Req-Type	X	x.1.21	Enumerated	M,V				No
	EAP-Master-Session-Key	X	x.1.22	OctetString	M, V				No
	Session-Request-Type	X	x.1.23	Enumerated	M, V				No
	Routing-Policy	X	x.1.24	OctetString	M, V				No
	Max-Requested-Bandwidth	X	x.1.26	Enumerated	M, V				No
	3GPP-AAA-Server-Name	tbd	10.1.xx	DiameterIdentity	M, V				No

NOTE 1: The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see IETF RFC 3588 [7].

10.1.1 Auth-Session-State

Between the 3GPP AAA server and the HSS, Diameter sessions are implicitly terminated. An implicitly terminated session is one for which the server does not maintain state information. The client does not need to send any re-authorization or session termination requests to the server.

The Diameter base protocol includes the Auth-Session-State AVP as the mechanism for the implementation of implicitly terminated sessions.

The client (server) shall include in its requests (responses) the Auth-Session-State AVP set to the value NO_STATE_MAINTAINED (1), as described in IETF RFC 3588 [7]. As a consequence, the server does not maintain any state information about this session and the client does not need to send any session termination request. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP shall be present in requests or responses.

10.1.2 User-Name

The User-Name AVP is defined in the IETF RFC 3588 [7] and contains the user identity.

For the WLAN Wx referende point, the User-Name AVP contains the IMSI of the subscriber.

10.1.3 Visited-Network-Identifier

The Visited-Network-Identifier AVP is defined in 3GPP TS 29.229[6] and indicates the 3GPP VPLMN where the user is roaming.

10.1.4 SIP-Auth-Data-Item

The SIP-Auth-Data-Item AVP is defined in 3GPP TS 29.229[6]. However three new more conditional AVPs are needed for WLAN Wx reference point.

AVP format

SIP-Auth-Data-Item :: = < AVP Header : TBD >

[SIP-Item-Number]

[SIP-Authentication-Scheme]

[SIP-Authenticate]

[SIP-Authorization]

[SIP-Authentication-Context]

[Confidentiality-Key]

[Integrity-Key]

[Authentication-Method]

~~**[Authentication-Information-SIM]**~~

~~**[Authorization-Information-SIM]**~~

~~* [AVP]~~

~~10.1.5 Authentication-Method~~

~~The Authentication-Method AVP (AVP code X) is of type UTF8String and indicates the authentication method required for the user. The following values are defined:~~

~~WLAN_EAP_SIM (0)~~

~~The UE indicates to the HSS that the required authentication method is EAP/SIM.~~

~~WLAN_EAP_AKA (1)~~

~~The UE indicates to the HSS that the required authentication method is EAP/AKA.~~

~~10.1.6 Authentication-Information-SIM~~

~~The Authentication-Information-SIM AVP (AVP code X) is of type OctetString and contains the concatenation of authentication challenge RAND and the ciphering key Kc.~~

~~10.1.7 Authorization - Information-SIM~~

~~The Authentication-Information-SIM AVP (AVP code X) is of type OctetString and contains the response SRES.~~

~~10.1.8 WLAN-User-Data~~

~~The WLAN-User-Data AVP (AVP code X) 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>~~

~~[MSISDN]~~

~~{ WLAN-Access }~~

~~{ WLAN-Tunneling }~~

~~[Session-Timeout]~~

~~1* { Charging-Data }~~

~~*[APN-Authorised]~~

~~{ Local-Access }~~

~~* [AVP]~~

~~10.1.9 MSISDN~~

~~The MSISDN AVP (AVP code 101) is defined in 3GPP TS 29.329 [x]. This identification could be used for example used for charging purposes.~~

Editor's Note: The optionality/presence could be modified by the SA1 and SA5 decision.

10.1.10 Charging-Information

The Charging Mode AVP (AVP code 19) is of type is of type Grouped, and contains the addresses of the charging functions. It is defined in 3GPP TS 29.229 [6].

10.1.11 WLAN-Access

The WLAN-Access AVP (AVP code xx) is of type Enumerated, and allows operators to determine barring of 3GPP WLAN interworking subscription. The following values are defined:

WLAN_SUBSCRIPTION_ALLOWED (0)

The subscriber has WLAN subscription.

WLAN_SUBSCRIPTION_BARRED (1)

The subscriber has no WLAN subscription.

10.1.12 WLAN-Tunneling

The WLAN-Tunneling AVP (AVP code xx) is of type Enumerated, and allows operator to disable all W-APNs at one time. If there is a conflict between this item and the "access allowed" flag of any W-APN, the most restrictive will prevail. The following values are defined:

WLAN_ APNS _ENABLE (0)

Enable all APNs.

WLAN_ APNS _DISABLE (1)

Disable all APNs

10.1.13 Session-Timeout

The Session-TimeOut AVP (AVP code 27) is defined in IETF RFC 3588 [7] and indicates the maximum period for a session measured in seconds.

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

10.1.14 APN-Authorised

The APN-Authorised AVP (AVP code xx) is of type Grouped and contains authorization information for the APNs. This AVP indicates the list of allowed APNs and the environment where the access is allowed (visited or home PLMN).

AVP format

APN-Authorised::= <AVP header: TBD>

{ APN-Id }

{ APN-Authorisation }

* [AVP]

10.1.15 APN-Id

The APN-Id AVP (AVP code xx) 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.

10.1.16 APN-Authorisation

The APN-Authorisation AVP (AVP code xx) is of type Enumerated, and contains a flag indicating whether access is allowed in visited PLMNs or in the home PLMN.

WLAN_APN_HOME (0)

Access is allowed in home PLMN only.

WLAN_APN_VISITED (1)

Access is allowed in visited PLMNs and home PLMN.

10.1.17 Local-Access

The Local-Access AVP (AVP code xx) is of type Enumerated, and indicate whether the user has direct access to external IP networks, e.g. Internet, from the WLAN Access Network or not.

WLAN_LOCAL_ACCESS (0)

The user is allowed to access directly to external IP networks.

WLAN_NO_LOCAL_ACCESS (1)

The user is not allowed to access directly to external IP networks.

10.1.18 Server-Assignment-Type

The Server-Assignment-Type AVP (AVP code 15) 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.

10.1.19 Deregistration-Reason

The Deregistration-Reason AVP (AVP code 16) is defined in 3GPP TS 29.229 [6] and indicates reason for a de-registration operation.

This grouped AVP contains a Reason-Code AVP to indicate the reason for the de-registration. Reasons are listed in 3GPP TS 29.229 [6]. Wx reference point defines as valid only PERMANENT_TERMINATION value.

10.1.20 EAP-Payload

The EAP-Payload AVP (AVP code xx) is defined in the IETF draft ietf-aaa-eap-08.txt [8] and contains the

encapsulated EAP packet that is being exchanged between the EAP client and the home Diameter server.

10.1.21 Auth Req Type

The Auth Req Type AVP (AVP code xx) is of type Enumerated and indicates the action that the PDG is asking to the 3GPP AAA Server to perform (Authentication, authorization or both). Wm interface only makes use of the AUTHENTICATION_ONLY value. It is defined in the IETF draft ietf-aaa-eap-08.txt [8]

10.1.22 EAP-Master-Session-Key

The EAP-Master-Session-Key AVP (AVP code xx) is of type OctetString and contains keying material for protecting the communications between the user and the NAS. It is defined in the IETF draft ietf-aaa-eap-08.txt [8]

10.1.23 Session-Request-Type

The Session-Request-Type AVP (AVP code xx) is of type Enumerated and indicates the action that the PDG is asking to the 3GPP AAA Server to perform (authorization or routing policy). The following values are defined:

AUTHORIZATION-REQUEST (0)

The PDG is requesting authorization for a user for a given W-APN.

ROUTING POLICY (1)

The PDG is indicating that routing policy information is present.

10.1.24 Routing-Policy

The Routing-Policy AVP (AVP code xx) is of type OctetString and indicates routing policies of the tunnel set-up.

Editor's Note: Its exact format is ffs.

10.1.25 Subscription-ID

The Subscription-ID AVP (AVP code xx) is of type Enumerated and indicates the user identity to be used for charging purposes. It is defined in the IETF Diameter Credit-Control Application draft [19].

WLAN shall make use only of the value MSISDN.

10.1.26 Max-Requested-Bandwidth

The Max-Requested-Bandwidth AVP (AVP code xx) is of type OctetString and indicates the Max requested bandwidth. If present, shall be sent from the 3GPP AAA Server to the PDG.

10.1.27 Routing Policy

The Routing Policy AVP (AVP code tbd) is of type IPFilterRule, and defines a packet filter for an IP flow with the following information:

8Direction (in or out)

9Source and destination IP address (possibly masked)

10Protocol

11Source and destination port (list or ranges)

Where the protocol type shall be set to ESP (50).

The IPFilterRule type shall be used with the following restrictions:

8Only the Action "permit" shall be used.

9No "options" shall be used.

10The invert modifier "!" for addresses shall not be used.

11The keyword "assigned" shall not be used.

12For direction "out", an IPv4 destination IP address shall not be wildcarded. For direction "out", the 64 bits network prefix of an IPv6 destination IP address shall not be wildcarded.

The Flow description AVP shall be used to describe a single IP flow.

The direction "in" refers to uplink IP flows, and the direction "out" refers to downlink IP flows.

10.1.xx 3GPP-AAA-Server-Name

The 3GPP-AAA-Server-Name AVP is of type DiameterIdentity, and defines the Diameter address of the 3GPP AAA Server node.

3GPP TSG-CN WG4 Meeting #25 ***N4-041371***

Seoul, KOREA. 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **010** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Application-Ids to Wa, Wd, Wm and Wg
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	04/11/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:

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:	⌘	Wa, Wd, Wg and Wm reference points lack of an Application-Id to be advertised. According to IETF, Application-Ids should be reused as much as possible.
Summary of change:	⌘	All I-WLAN mandatory parameters that modify the EAP, NASREQ or Diameter Base Protocol commands ABNF are added within I-WLAN spec as optional AVPs into the ABNF and as mandatory at application level. A note has been added to indicate that the Wa, Wd, Wg and Wm reference points shall advertise EAP, NASREQ or Diameter Base Protoocl Application-Id based on the command they are sending over the interface. So when e.g. an EAP command is being issued over Wm, it shall be advertised EAP as Application-Id.
Consequences if not approved:	⌘	Variants of the same protocol will appear with slight differents that can be solved at application level. Further implementations will not know what application to use for authorisation and authentication. Goes against IETF principles.

Clauses affected:	⌘	4.2, 4.4.2, 4.3.1, 5.2, 5.4.1, 8.2, 9.2			
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.

****** First modified section ******

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 RFC 2865 [17], including the following extensions:

   - RFC 2869 [9], which provides RADIUS extensions to support the transport of EAP frames over RADIUS.
   - IETF Draft "Attributes for Access Network Location and Ownership Information" [16], which provides RADIUS Extensions for Public WLAN [16] are also used in order to identify uniquely the owner and location of the WLAN.
   - 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 RFC 3588 [7], as well as IETF Draft " Diameter EAP Application", which [8] provides a Diameter application to support the transport of EAP (RFC 2284 [10] and IETF Draft "EAP" [11]) 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.

****** Second modified section ******

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}
    * [ Proxy-Info ]
    * [ AVP ]
```

****** Third modified section ******

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 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.

~~Editors Note: AVPs such as User Name defined on the Wa interface and VPLMN ID defined on the Wd interface are parameters additional to those carried by the Diameter_EAP application. As defined below there parameters are defined as mandatory on the interface. It is an open point whether this implies that a new Diameter application is required, or whether these AVPs should be defined as conditional in order that the use of the Diameter_EAP application can be preserved.~~

****** Fourth modified section ******

5 Wd Description

The Wd reference point connects the 3GPP AAA Proxy, possibly via intermediate networks, to the 3GPP AAA Server. The prime purpose of the protocols crossing this reference point is to transport WLAN session authentication, authorization and related information from the visited 3GPP network to the home 3GPP network in a secure manner. Therefore, this reference point is used in the roaming case only.

5.1 Functionality

The functionality of the reference point is to transport:

- data for WLAN session authentication signalling between 3GPP AAA Proxy and 3GPP AAA Server;
- data for WLAN session authorization signalling between 3GPP AAA Proxy and 3GPP AAA server;
- keying data for the purpose of radio interface integrity protection and encryption;
- data used for purging a user from the WLAN access for immediate service termination;
- data to enable the identification of the operator networks within which roaming occurs;
- carrying accounting signalling per WLAN user.

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 RFC 2865 [17], including the following extensions:
   - RFC 2869 [9], which provides RADIUS extensions to support the transport of EAP frames over RADIUS.
   - IETF Draft "Attributes for Access Network Location and Ownership Information" [16], which provides RADIUS Extensions for Public WLAN are to identify uniquely the owner and location of the WLAN.
   - 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 RFC 3588 [7], as well as IETF Draft "Diameter EAP Application" [8], which provides a Diameter application to support the transport of EAP (RFC 2284 [10] and IETF Draft "EAP" [11]) frames over Diameter. In addition, Diameter Base (RFC 3588 [7]) and NASREQ [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.

****** Fifth modified section ******

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.

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.

~~Editors Note: AVPs such as User Name defined on the Wa interface and VPLMN ID defined on the Wd interface are parameters additional to those carried by the Diameter_EAP application. As defined below there parameters are defined as mandatory on the interface. It is an open point whether this implies that a new Diameter application is required, or whether these AVPs should be defined as conditional in order that the use of the Diameter_EAP application can be preserved.~~

****** Sixth modified section ******

8 Wm Description

8.1 Functionality

This clause specifies a Diameter application that allows the following messaging to take place between the 3GPP AAA Server and the PDG:

- The 3GPP AAA Server/Proxy retrieves tunnelling attributes and WLAN UE's IP configuration parameters from the Packet Data Gateway.
- Messaging for service authentication between WLAN UE and 3GPP AAA Server/Proxy.
- Messaging for service authorization between PDG and 3GPP AAA Server/Proxy.
- Messaging for carrying authentication data for the purpose of tunnel establishment, tunnel data authentication and encryption.

In the roaming case, the 3GPP AAA Proxy shall act as a stateful proxy between the PDG and 3GPP AAA Server.

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 or Diameter Base Protocol Application-Id, depending on the command sent over Wm.

****** Fifth modified section ******

9 Wg Description

Wg is the reference point that connects the 3GPP AAA Server/Proxy to the WAG. The prime purpose of this reference point is to transfer Policy Enforcement rules to the WAG, which would enable WAG to allow only authorized packets to/from the WLAN AN. This interface is applicable only when a WLAN UE is allowed to access the 3GPP PS services from the 3G-WLAN interworking network.

9.1 Functionality

This clause specifies a Diameter application that allows the following messaging to take place between the 3GPP AAA Server and the WAG for the case where the PDG is in the HPLMN, and between the 3GPP AAA Proxy and the WAG for the case where the PDG is in the VPLMN:

- data carrying policy Enforcement rules to be applied to packets to/from WLAN AN.
- transport per-tunnel based charging information from the WAG to the AAA Proxy/Server.

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 scenario 3 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 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 or Diameter Base Protocol Application-Id, depending on the command sent over Wg.

3GPP TSG-CN WG4 Meeting #25 ***N4-041414***

Seoul, KOREA. 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **026** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Addition of calling station id in DEA. Deletion of the same from DER.
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	05/11/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:
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 Diameter message in DEA has been mentioned to contain MAC Address of UE. However the DEA message is sent from AAA server towards UE. Hence the MAC Address of UE is not necessary (even when AAA server knows the MAC address of the UE). Also, according to present specifications 33.234, it is necessary to send MAC address of UE to AAA server.
Summary of change:	⌘	In Wd interface, for authorization and authentication request, removed the Calling Station ID AVP is DEA, Added the same to DER.
Consequences if not approved:	⌘	This specification will be mis-alligned with the 33.234. Also Diameter EAP application cannot be used as Calling Station ID is not included in DEA.

Clauses affected:	⌘	5.4.1

		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.

***** First modified section *****

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.

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.

Editors Note: AVPs such as User Name defined on the Wa interface and VPLMN-ID defined on the Wd interface are parameters additional to those carried by the Diameter_EAP application. As defined below there parameters are defined as mandatory on the interface. It is an open point whether this implies that a new Diameter application is required, or whether these AVPs should be defined as conditional in order that the use of the Diameter_EAP application can be preserved.

Table 5.4.1.1: Diameter EAP Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Username NAI	User Name	M	This information element shall contain 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 or authentication procedure is requested. 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
Visited-Network-Identifier	Visited-Network-Identifier	M	Identifies the VPLMN
WLAN UE MAC address	Calling Station-ID	M	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
Username NAI	User Name	M	This information element contains the permanent identity of the user, i.e. the IMSI.
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 Alive Time	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.
~~WLAN UE MAC address~~	~~Calling Station-ID~~	~~M~~	~~Carries the MAC address of the WLAN UE.~~

~~* End of document ***~~**

3GPP TSG-CN WG4 Meeting #25 ***N4-041481***

Seoul, KOREA. 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **029** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Handling of Information Element marked as (M), (C) or (O)
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	15/11/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
- ***F*** *(correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(addition of feature),*
- ***C*** *(functional modification of feature)*
- ***D*** *(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

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 tables describing the Information Elements transported in the various Diameter commands specified in the TS 29.234, there is no description of the meaning of the terms "Mandatory", "Conditional" and "Optional". Moreover, it is not described the correct handling when one of those information elements are missing in received request.
Summary of change:	⌘	It is proposed to add a sub-section in the section 10 explaining the meaning of the terms "Mandatory", "Conditional" and "Optional" in the tables. Moreover, the text states that a missing mandatory information element in a command shall cause an application error and an answer message shall be sent back to the originator of the request with a Result-Code set to DIAMETER_MISSING_AVP and the Failed-AVP AVP containing an example of the expected AVP. The appropriate handling is also detailled for Conditional and Optional information elements
Consequences if not approved:	⌘	Possibility of wrong implementation due to an unclear specification on the meaning as well as on the correct handling of missing IE marked as mandatory, conditional or optional and supported by mandatory/optional Diameter AVPs.

Clauses affected:	⌘	10			
Other specs affected:	⌘	Y	N	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 added section

10.x Handling of Information Elements

In the tables that describe the Information Elements transported by each Diameter command, each Information Element is marked as (M) Mandatory, (C) Conditional or (O) Optional.

- A mandatory Information Element (marked as (M) in the table) shall always be present in the command. If this Information Element is absent, an application error occurs at the receiver and an answer message shall be sent back to the originator of the request with the Result-Code set to DIAMETER_MISSING_AVP. This message shall also include a Failed-AVP AVP containing the missing Information Element i.e. the corresponding Diameter AVP defined by the AVP Code and the other fields set as expected for this Information Element.

- A conditional Information Element (marked as (C) in the table) shall be present in the command if certain conditions are fulfilled.

  - If the receiver detects that those conditions are fulfilled and the Information Element is absent, an application error occurs and an answer message shall be sent back to the originator of the request with the Result-Code set to DIAMETER_MISSING_AVP. This message shall also include a Failed-AVP AVP containing the missing Information Element i.e. the corresponding Diameter AVP defined by the AVP Code and the other fields set as expected for this Information Element.

  - If those conditions are not fulfilled, the Information Element shall be absent. If however this Information Element appears in the message, it shall not cause an application error and it may be ignored by the receiver if this is not explicitly defined as an error case. Otherwise, an application error occurs at the receiver and an answer message with the Result-Code set to DIAMETER_AVP_NOT_ALLOWED shall be sent back to the originator of the request. A Failed-AVP AVP containing a copy of the corresponding Diameter AVP shall be included in this message

- An optional Information Element (marked as (O) in the table) may be present or absent in the command, at the discretion of the application at the sending entity. Absence or presence of this Information Element shall not cause an application error and may be ignored by the receiver.

End of the added section

3GPP TSG-CN WG4 Meeting #25 ***N4-041527***

Seoul, Korea. November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **004** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	3GPP WLAN IP Access parameter rename
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	04/11/2004
Category:	⌘	**D**
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:	⌘	Local Access parameter indicates whether or not the user has Direct access to external IP networks by scenario 2. However, the name of the parameter is confusing, as it was discussed in the last SA2 meeting. WLAN-Tuneling AVP has also been changed toWLAN-3GPP-IP-Access aligned with Stage 2 CR.
Summary of change:	⌘	Replace Local-Access AVP by WLAN-Direct-IP-Access AVP.
Consequences if not approved:	⌘	Misunderstanding of the WLAN 3GPP IP Access functionality.

Clauses affected:	⌘	

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

Other comments:	⌘	There is a similar CR in SA2. that must be approved first before this CR is approved: S2-043606.

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 ******

10.1 AVPs

Table 10.1.1 describes the Diameter AVPs defined for the WLAN reference point, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted. The Vendor-Id header of all AVPs defined in this specification shall be set to 3GPP (10415).

Only those AVPs defined by 3GPP TS 29.234 [2] reference point are listed here.

Table 10.1.1: Diameter Multimedia Application AVPs

				AVP Flag rules				
Attribute Name	**AVP Code**	**Section defined**	**Value Type**	**Shall**	**May**	**Should not**	**Must not**	**May Encr.**
Authentication-Method	X	x.1.5	UTF8String	M, V				No
Authentication-Information-SIM	X	x.1.6	OctetString	M, V				No
Authorization -Information-SIM	X	x.1.7	OctetString	M,V				No
WLAN-User-Data	X	x.1.8	Grouped	M, V				No
WLAN-Access	X	x.1.11	Enumerated	M, V				No
WLAN-Tunnelling3GPP-IP-Access	X	x.1.12	Enumerated	M, V				No
APN-Authorized	X	x.1.14	Grouped	M, V				No
APN-Id	X	x.1.15	OctetString	M, V				No
APN-Authorization	X	x.1.16	Enumerated	M, V				No
WLAN-Direct-IP-AccessLocal-Access	X	x.1.17	Enumerated	M, V				No
EAP payload	X	x.1.20	OctetString	M, V				No
Auth Req Type	X	x.1.21	Enumerated	M,V				No
EAP-Master-Session-Key	X	x.1.22	OctetString	M, V				No
Session-Request-Type	X	x.1.23	Enumerated	M, V				No
Routing-Policy	X	x.1.24	OctetString	M, V				No
Max-Requested-Bandwidth	X	x.1.26	Enumerated	M, V				No
NOTE: The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see RFC 3588 [7].								

****** Second modified section ******

10.1.8 WLAN-User-Data

The WLAN-User-Data AVP (AVP code X) 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>
    [ MSISDN ]
    { WLAN-Access }
    { WLAN-3GPP-IP-AccessTunneling }
    [ Session-Timeout ]
    1* { Charging-Data  }
    *[ APN-Authorized ]
    { WLAN-Direct-IP-Access Local-Access }
    * [AVP]
```

****** Third modified section ******

10.1.12 WLAN-Tunnelling10.1.12 WLAN-3GPP-IP-Access

The WLAN-Tunnelling 3GPP-IP-Access AVP (AVP code xx) is of type Enumerated, and allows operator to disable all W-APNs at one time. If there is a conflict between this item and the "access allowed" flag of any W-APN, the most restrictive will prevail. The following values are defined:

WLAN_ APNS _ENABLE (0)

- Enable all APNs.

WLAN_ APNS _DISABLE (1)

- Disable all APNs.

****** Fourth modified section ******

10.1.17 WLAN Direct IP Local-Access

The WLAN Direct IP Access Local-Access AVP (AVP code xx) is of type Enumerated, and indicate whether the user has direct access to external IP networks, e.g. Internet, from the WLAN Access Network or not.

WLAN_LOCALDIRECT_IP_ACCESS (0)

- The user is allowed to access directly to external IP networks.

WLAN_NO_LOCALDIRECT_IP_ACCESS (1)

- The user is not allowed to access directly to external IP networks.

3GPP TSG-CN WG4 Meeting #25 ***N4-041572***

Seoul, Korea. November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.008** **CR** **142** ⌘ **rev** **1** ⌘ Current version: **6.3.0** ⌘

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

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

Title:	⌘	WLAN-IW data handling: additions to 23.008
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	19/11/2004
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:	⌘	Data Handling at the various nodes in the WLAN-IW system should be defined. These should be added to 23.008
Summary of change:	⌘	Addition of WLAN-IW data handling to 23.008
Consequences if not approved:	⌘	Unclear for implementors which data should be stored in each of the nodes in the WLAN-IW system

Clauses affected:	⌘	0.1, 1.4, new clause added after section 3, 5

	Y	N			
Other specs affected: ⌘	X		Other core specifications	⌘	CR 23.234-???
		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 ****

0 Scope

The present document provides details concerning information to be stored in home subscriber servers, visitor location registers, GPRS Support Nodes and Call Session Control Function (CSCF) concerning mobile subscriber.
Clause 2 contains all details concerning the definition of the parameters, often given by reference to other specifications, and where the parameter is to be stored.
Table 1 in clause 3 gives a summary overview and clause 4 identifies the reference information required for accessing the information.

0.1 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 TS 22.002: "Circuit Bearer Services (BS) supported by a Public Land Mobile Network (PLMN)".

[3] 3GPP TS 22.003: "Circuit Teleservices supported by a Public Land Mobile Network (PLMN)".

[4] 3GPP TS 22.004: "General on supplementary services".

[5] 3GPP TS 23.003: "Numbering, addressing and identification".

[6] 3GPP TS 23.007: "Restoration procedures".

[7] 3GPP TS 23.009: "Handover procedures".

[8] 3GPP TS 23.012: "Location Management Procedures".

[9] 3GPP TS 23.015: "Technical realization of Operator Determined Barring (ODB)".

[10] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[11] 3GPP TS 22.060: "General Packet Radio Service (GPRS); Service description; Stage 1".

[12] 3GPP TS 23.067: "Enhanced Multi-Level Precedence and Preemption service (EMLPP); Stage 2".

[13] 3GPP TS 23.078: "Customised Applications for Mobile network Enhanced Logic (CAMEL); Stage 2".

[14] 3GPP TS 23.081: "Line identification supplementary services; Stage 2".

[15] 3GPP TS 23.082: "Call Forwarding (CF) Supplementary Services; Stage 2".

[16] 3GPP TS 23.083: "Call Waiting (CW) and Call Hold (HOLD) Supplementary Services; Stage 2".

[17] 3GPP TS 23.084: "Multi Party (MPTY) Supplementary Service; Stage 2".

[18] 3GPP TS 23.085: "Closed User Group (CUG) Supplementary Service; Stage 2".

[19] 3GPP TS 23.086: "Advice of Charge (AoC) Supplementary Service; Stage 2".

[20] 3GPP TS 23.088: "Call Barring (CB) Supplementary Service; Stage 2".

[21] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service Description; Stage 2".

[22] 3GPP TS 23.078: "Customised Applications for Mobile network Enhanced Logic (CAMEL); Stage 2".

[23] 3GPP TS 23.090: "Unstructured Supplementary Service Data (USSD); Stage 2".

[24] 3GPP TS 23.116: "Super-Charger Technical Realization; Stage 2."

[25] 3GPP TS 23.135: "Multicall supplementary service; Stage 2"

[26] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[27] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[28] 3GPP TS 29.007: "General requirements on interworking between the Public Land Mobile Network (PLMN) and the Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN)".

[29] 3GPP TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface".

[30] 3GPP TS 42.032: "Digital cellular telecommunications system (Phase 2+); Immediate Service Termination (IST) Service description - Stage 1".

[31] 3GPP TS 43.020: "Digital cellular telecommunications system (Phase 2+); Security-related network functions".

[32] 3GPP TS 43.035: "Digital cellular telecommunications system (Phase 2+); Immediate Service Termination (IST); Stage 2".

[33] 3GPP TS 43.068: "Digital cellular telecommunications system (Phase 2+); Voice Group Call Service (VGCS); Stage 2".

[34] 3GPP TS 43.069: "Digital cellular telecommunications system (Phase 2+); Voice Broadcast Service (VBS); Stage 2".

[35] 3GPP TS 23.071: "Location Services (LCS); Functional Description; Stage 2".

[36] GSM 12.03: "Digital cellular telecommunications system (Phase 2+) (GSM); Security management".

[37] GSM 12.08: "Digital cellular telecommunications system (Phase 2+) (GSM); Subscriber and equipment trace".

[38] ITU-T Recommendation Q.763: "Signalling System No. 7 - ISDN User Part formats and codes".

[39] ANSI T1.113: "Signalling System No7 (SS7); Integrated Services Digital Network (ISDN) User Part"

[40] 3GPP TS 32.005 "Telecommunication Management; Charging and billing; 3G call and event data for the Circuit Switched (CS) domain".

[41] 3GPP TS 32.015: "Telecommunication Management; Charging and billing; 3G call and event data for the Packet Switched (PS) domain".

[42] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[43] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents".

[44] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol; Protocol details".

[45] IETF RFC 3261: "SIP: Session Initiation Protocol".

[46] IETF RFC 2396: "Uniform Resource Identifiers (URI): Generic Syntax".

[47] Void

[48] IETF RFC 2486: "The Network Access Identifier".

[49] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[50] 3GPP TS 23.002: "Network Architecture".

[51] IETF RFC 3588: draft-ietf-aaa-diameter-08.txt: "Diameter Base Protocol", work in progress".

[52] 3GPP TS 33.102: "3G Security; Security Architecture".

[53] 3GPP TS 23.218: "IP Multimedia (IM) session handling; IM call model; Stage 2".

[54] 3GPP TS 29.328: "IP Multimedia Subsystem (IMS) Sh interface signalling flows and message contents (Release 5)".

[55] 3GPP TS 23.278: "Customised Applications for Mobile network Enhanced Logic (CAMEL) - IP Multimedia System (IMS) interworking; Stage 2".

[56] 3GPP TS 23.271: "Location Services (LCS); Functional description; Stage 2".

[57] 3GPP TS 23.221: " Architectural requirements ".

[58] 3GPP TS 33.220: ""Generic Authentication Architecture (GAA);Generic bootstrapping architecture"".

[59] 3GPP TS 29.109 ""Zh and Zn Interfaces based on the Diameter protocol; Protocol details"".

[60] IETF RFC 3548: "The Base16, Base32, and Base64 Data Encodings".

[xx] 3GPP TS 23.234 ""3GPP Systen to WLAN Interworking System Description, Stage 2""

[yy] 3GPP TS 29.234 ""3GPP system to Wireless Local Area Network (WLAN), Stage 3""

****** First modified section ******

1.4 Subscriber data in WLAN-IW functional units

This specification considers subscriber data stored in the following types of functional unit for I-WLAN-IW:

23GPP AAA Server which contains all subscribedsubscriber data necessary to maintain 3GPP WLAN Direct Access and 3GPP WLAN IP Access.

33GPP AAA Proxy which contains subscriber data necessary to perform AAA proxy functionality in the VPLMN and to provide charging inter operator settlement functionality.

4Packet Data Gateway (PDG) which contains all subscriber data necessary to manage 3GPP WLAN IP Access tunnels.

5WLAN Access Gateway (WAG) which contains all subscriber data necessary to manage a per user firewall between the WLAN-AN and PLMN and to perform per tunnel charging.

****** Second modified section **** -- Should be after chapter 3**

X Definition of subscriber data I-WLAN domain

X.1 Data related to subscription, identification and numbering

X.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.

X.1.2 Mobile Subscribertation International 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).

X.1.3 W-APN

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

X.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.

X.1.5 3GPP AAA Proxy Identifier

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

X.1.6 3GPP AAA Server Name

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

AAA Server node.

X.1.7 Serving PDG List

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

X.1.8 Serving WAG

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

X.1.9 WLAN UE Local IP aAddress

The WLAN UE Local IP Address field, specified in 3GPP TS 23.234 [xx], 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.

X.1.10 WLAN UE Remote IP aAddress

The WLAN UE Remote IP Address field, specified in 3GPP TS 23.234 [xx], 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 X.5.4.4.

X.2 Data related to registration

X.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.

X.3 Data related to authentication and ciphering

X.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..

X.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]).

X.3.3 Master Key (MK)

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

X.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.

X.4 Data related to session

X.4.1 Session Identifier

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

X.4.2 Session-Timeout

The Session Timeout field, specified in 3GPP TS 29.234 [yy], 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.

X.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.

.

X.5 Operator Determined Barring general data

X.5.1 WLAN Access

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

- Enable WLAN access ;
- Bar WLAN access ;

X.5.2 WLAN Tunnelling

The WLAN Tunnelling flag is defined in 3GPP TS 29.234 [yy]. 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;

X.5.3 WLAN Direct IP Access

The WLAN Direct IP Access flag is defined in 3GPP TS 29.234 [yy]. 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.

X.5.4 W-APN Authorised

The W-APN Authorised field, is specified in 3GPP TS 29.234 [yy]. 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.

X.5.4.1 W-APN Identifier

See subclause X.1.5.

X.5.4.2 W-APN Barring -Type

The W-APN Barring Type field is specified in 3GPP TS 29.234 [yy]. 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.

X.5.4.3 W-APN Charging Data

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

X.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 X.1.12.

X.5.5 Access Independence Flag

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

2Allow access to WLAN 3GPP IP Access independently of a previous WLAN 3GPP Direct Access

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

X.5.6 I-WLAN Access Type

The I-WLAN Access Type field is defined in 3GPP TS 29.234 [yy]. 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.

X.6 QoS general data

X.6.1 Max Requested Bandwidth

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

X.6.2 Routing Policy

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

X.7 Data related to Charging

X.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.

X.7.1.1 Charging Characteristics

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

X.7.2 Primary OCS Charging Function Name

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

X.7.3 Secondary OCS Charging Function Name

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

X.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 [yy].

X.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 [yy].

**** Third modified section ****

5 Accessing subscriber data

It shall be possible to retrieve or store subscriber data concerning a specific MS from the HSS by use of each of the following references:

- International Mobile Subscriber Identity (IMSI);
- Mobile Subscriber ISDN Number (MSISDN).

It shall be possible to retrieve or store subscriber IP Multimedia service data concerning a specific MS from the HSS by use of each of the following references:

- Private User Identity;
- Public Identity.

It shall be possible to retrieve or store subscriber data concerning a specific MS from the VLR by use of each of the following references:

- International Mobile Subscriber Identity (IMSI);
- Temporary Mobile Subscriber Identity (TMSI).

It shall be possible to retrieve or store subscriber data concerning a specific MS from the SGSN by use of each of the following references:

- International Mobile Subscriber Identity (IMSI);
- Packet Temporary Mobile Subscriber identity (P-TMSI).

It shall be possible to retrieve or store subscriber data concerning a specific MS from the GGSN by use of the following reference:

- International Mobile Subscriber Identity (IMSI).

It shall be possible to retrieve or store subscriber data concerning a specific MS from the 3GPP AAA Server by use of each of the following references:

- International Mobile Subscriber Identity (IMSI);
- Mobile Subscriber ISDN Number (MSISDN).

It shall be possible to retrieve or store subscriber data concerning a specific MS from the 3GPP AAA Proxy by use of the following reference:

- Mobile Subscriber ISDN Number (MSISDN).

It shall be possible to retrieve or store subscriber data concerning a specific MS from the WAG by use of the following reference:

- Mobile Subscriber ISDN Number (MSISDN).

It shall be possible to retrieve or store subscriber data concerning a specific MS from the PDG by use of the following reference:

- Mobile Subscriber ISDN Number (MSISDN).

See clause 4 for explanation of M, C, T and P in table 1, table 2 and table 3.

**** Fourth modified section ****

5.4X I-WLAN Service Data Storage

Table 5.X: Overview of data used for I-WLAN services

PARAMETER	Subclause	HSS	3GPP AAA Server	3GPP AAA Proxy	PDG	WAG	TYPE
IMSI	X.1.1	M	M				P
MSISDN	X.1.2	M	M	M	M	M	P
W-APN	X.1.3	M	M		M		P
List of authorized visited network identifiers	X.1.4	M					P
3GPP AAA Proxy Identifier	X.1.5		M		M	M	T
3GPP AAA Server Name	X.1.6	M		M	M	C	T
Serving PDG List	X.1.7		M	M			P
Serving WAG	X.1.8		M	M	M		P
WLAN UE Local IP address	X.1.9				M	M	T
WLAN UE Remote IP address	X.1.10	C	C		M		P
User Status	X.2.1		M				T
RAND, SRES, Kc	X.3.1	M	M		-		T
RAND, XRES CK, IK, AUTN	X.3.2		M		-		T
Master -Key (MK)	X.3.3		M				T
Transient EAP Keys (TEKs)	X.3.3		M				T
Session Identifier	X.4.1		M				T
Session Timeout	X.4.2		C				P
Quota	X.4.3		C				P
WLAN Access	X.5.1	M					P
WLAN Tunnelling	X.5.2	M					P
WLAN Direct IP aAccess	X.5.3	M					P
W-APN Authorised	X.5.4	M					P
W-APN Identifier	X.5.4.1						P
W-APN Barring Type	X.5.4.2	M					P
W-APN Charging Data	X.5.4.3	C			C		P
WLAN UE Remote IP Address	X.5.4.4	C			P		P
Access Independence Flag	X.5.5	M					P
I-WLAN Access Type	X.5.6	M					P
Max Requested Bandwidth	X.6.1		P		T		P
Routing Policy	X.6.2				C	C	T
Charging Data	X.7.1	M			M		P
Charging Characteristics	X.7.1.1	M	-		M		P
Primary OCS Charging Function Name	X.7.2	M			M		P
Secondary OCS Charging Function Name	X.7.3	M			M		P
Primary Charging Collection Function Name	X.7.4	M			M		P
Secondary Charging Collection Function Name	X.7..5	M			M		P

3GPP TSG-CN1 Meeting #36
Seoul, Korea, 15-19 November 2004

Tdoc N4-041575

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.003** **CR** **093** ⌘ **rev** **1** ⌘ Current version: **6.4.0** ⌘

*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:	⌘	Definition of Alternative NAI
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	15/11/2004
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 order to obtain the list of available PLMNs for manual network selection the definition of an Alternative NAI should be used.
Summary of change:	⌘	In section 1 the reference to IETF document are updated according to the present status. Furthermore the “Alternative NAI” definition is added in order to enable UE to obtain list of available PLMNs for manual network selection
Consequences if not approved:	⌘	The manual network selection will not work

Clauses affected:	⌘	1 and 14

		Y	N			
Other specs affected:	⌘	X		Other core specifications	⌘	24.234-015
			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 Changes

1.1.1 Normative references

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

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

[1] 3GPP TS 21.905: "3G Vocabulary".

[2] 3GPP TS 23.008: "Organization of subscriber data".

[3] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2"

[4] 3GPP TS 23.070: "Routeing of calls to/from Public Data Networks (PDN)".

[5] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[6] 3GPP TS 29.060: "GPRS Tunnelling protocol (GPT) across the Gn and Gp interface".

[7] 3GPP TS 43.020: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[8] void

[9] 3GPP TS 51.011: " Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[10] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[11] ITU-T Recommendation E.212: "The international identification plan for mobile terminals and mobile users".

[12] ITU-T Recommendation E.213: "Telephone and ISDN numbering plan for land Mobile Stations in public land mobile networks (PLMN)".

[13] ITU-T Recommendation X.121: "International numbering plan for public data networks".

[14] IETF RFC 791: "Internet Protocol".

[15] IETF RFC 2373: "IP Version 6 Addressing Architecture".

[16] 3GPP TS 25.401: "UTRAN Overall Description".

[17] 3GPP TS 25.413: "UTRAN Iu Interface RANAP Signalling".

[18] IETF RFC 2181: "Clarifications to the DNS Specification".

[19] IETF RFC 1035: "Domain Names - Implementation and Specification".

[20] IETF RFC 1123: "Requirements for Internet Hosts -- Application and Support".

[21] IETF RFC 2462: "IPv6 Stateless Address Autoconfiguration".

[22] IETF RFC 3041: "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

[23] 3GPP TS 23.236: "Intra Domain Connection of RAN Nodes to Multiple CN Nodes".

[24] 3GPP TS 23.228: "IP Multimedia (IM) Subsystem – Stage 2"

[25] IETF RFC 2486: "The Network Access Identifier"

[26] IETF RFC 3261: "SIP: Session Initiation Protocol"

[27] 3GPP TS 31.102: "Characteristics of the USIM Application."

[28] void

[29] 3GPP TS 44.118: "Radio Resource Control (RRC) Protocol, Iu Mode".

[30] 3GPP TS 23.073: "Support of Localised Service Area (SoLSA); Stage 2"

[31] 3GPP TS 29.002: "Mobile Application Part (MAP) specification"

[32] 3GPP TS 22.016: "International Mobile Equipment Identities (IMEI)"

[33] void

[34] void

[35] 3GPP TS 45.056: "CTS-FP Radio Sub-system"

[36] 3GPP TS 42.009: "Security aspects" [currently not being raised to rel-5 – Pete H. looking into it]

[37] 3GPP TS 25.423: "UTRAN Iur interface RNSAP signalling"

[38] 3GPP TS 25.419: "UTRAN Iu-BC interface: Service Area Broadcast Protocol (SABP)"

[39] 3GPP TS 25.410: "UTRAN Iu Interface: General Aspects and Principles"

[40] ISO/IEC 7812: "Identification cards - Numbering system and registration procedure for issuer identifiers"

[41] 3GPP TS 31.102 "Characteristics of the USIM Application"

[42] 3GPP TS 33.102 "3G security; Security architecture"

[43] 3GPP TS 43.130: "Iur-g interface; Stage 2"

[45] IETF RFC 2806: "URLs for Telephone Calls"

[46] 3GPP TS 44.068: "Group Call Control (GCC) protocol".

[47] 3GPP TS 44.069: "Broadcast Call Control (BCC) Protocol ".

[48] 3GPP TS 24.234: "3GPP System to WLAN Interworking; UE to Network protocols; Stage 3".

[49] void.~~IETF Internet-Draft: "Network Discovery and Selection within the EAP Framework". draft-adrangi-eap-network-discovery-and-selection-00, work in progress~~.

[50] IETF Internet-Draft: "EAP AKA Authentication". draft-arkko-pppext-eap-aka-11, work in progress.

[51] IETF Internet-Draft: "EAP SIM Authentication". draft-haverinen-pppext-eap-sim-12, work in progress.

[52] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architechture and functional description"

[53] IETF Internet-Draft: 'The Network Access Identifier'.~~draft-arkko-roamops-rfc2486bis-00~~ 00draft-ietf-radext-rfc2486bis-01, work in progress.

[54] IETF RFC 2279: "UTF-8, a transformation format of ISO 10646".

[55] 3GPP TS 33.234: "Wireless Local Area Network (WLAN) interworking security".

[56] void.~~IETF Internet-Draft: 'The Network Access Identifier'.draft-arkko-roamops-rfc2486bis-00, work in progress.~~

1.1.2 Informative references

[44] "COMPLEMENT TO ITU-T RECOMMENDATION E.212 (11/98)", Annex to ITU Operational Bulletin No. 741 – 1.VI.200; This is published on the ITU-T website, whose home page is at http://www.itu.int/ITU-T/

[57] GSMA PRD IR.34 "Inter-PLMN Backbone Guidelines"

[58] IETF Internet-Draft: "Identity selection hints for Extensible Authentication Protocol (EAP)". draft-adrangi-eap-network-discovery-05 , work in progress.

End of First Changes

2nd Changes

14.5 Temporary identities

The Temporary identities (Pseudonyms and re-authentication identities) shall take the form of a NAI username as specified in clause 3 of the IETF draft 2486-bis [53~~6~~].

Temporary identity shall be generated as specified in subclause 6.4.1 of 3GPP TS 33.234 [55]. This part of the temporary identity shall follow the UTF-8 transformation format specified in RFC 2279 [54] except for the following reserved hexadecimal octet value:

FF.

When the temporary identity username is coded with FF, this reserved value is used to indicate the special case when no valid temporary identity exists in the WLAN UE (see 3GPP TS 24.234 [48]). The network shall not allocate a temporary identity with the whole username coded with the reserved hexadecimal value FF.

14.6 Alternative NAI

The Alternative NAI shall take the form of a NAI, i.e. 'any_username@REALM' as specified of draft-ietf-radext-rfc2486bis [53]. The Alternative NAI shall not be routable from any AAA server.

The Alternative NAI may contain a username part which is not derived by the IMSI and it may be a ‘dummy’ identity or may be omitted.

The REALM part of the NAI shall be “nonrouteable.3gppnetwork.org”.

The result will be an NAI in the form of:

"<any_string>@nonrouteable.3gppnetwork.org"

~~When the temporary identity username is coded with FF, this reserved value is used to indicate the special case when no valid temporary identity exists in the WLAN UE (see 3GPP TS 24.234 [48]). The network shall not allocate a temporary identity with the whole username coded with the reserved hexadecimal value FF.~~

15 Identification of Multimedia Broadcast/Multicast Service

3GPP TSG-CN WG4 Meeting #25 ***N4-041577***

Seoul, KOREA. 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **005** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Static Remote IP address
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	17/11/2004
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:	⌘	According to approved S2-042931 CR, the HSS shall be able to download an static remote IP Address for the WLAN UE to the 3GPP AAA Server and the 3GPP AAA Server shall download such a value to the PDG when the WLAN UE has been authorised.
Summary of change:	⌘	Static remote IP address is added to the profile being downloaded from the HSS to the 3GPP AAA Server. Static remote IP address is downloaded from the 3GPP AAA Server to the HSS when the WLAN UE is successfully authorised.
Consequences if not approved:	⌘	Static remote IP address is not implemented. Misalignment Stage 2 – Stage 3.

Clauses affected:	⌘	8.4, 10

		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 ******

8.4 Procedures Description

8.4.1 Authorization Procedures

According to the requirements stated in Chapter 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 tunneling 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.

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

Table 8.4.1.1 Wm Authorization 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.
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 8.4.1.2: 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.
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.

8.4.1.1.1 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:

    1 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.

        2 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.

        3 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.

        4 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.

        5 The 3GPP AAA Server 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. The Result-Code shall be set to DIAMETER_SUCCESS.

    6 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 authorisation information shall be returned.

8.4.1.1.2 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:

b. 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.

****** Second modified section ******

10 Information Elements Contents

10.1 AVPs

The following table describes the Diameter AVPs defined for the WLAN reference point, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted. The Vendor-Id header of all AVPs defined in this specification shall be set to 3GPP (10415).

Only those AVPs defined by 3GPP TS 29.234 reference point are listed here.

Table 10.1.1: Diameter Multimedia Application AVPs

				AVP Flag rules				
Attribute Name	**AVP Code**	**Section defined**	**Value Type**	**Shall**	**May**	**Should not**	**Must not**	**May Encr.**
Authentication-Method	X	x.1.5	UTF8String	M, V				No
Authentication-Information-SIM	X	x.1.6	OctetString	M, V				No
Authorization –Information-SIM	X	x.1.7	OctetString	M,V				No
WLAN-User-Data	X	x.1.8	Grouped	M, V				No
WLAN-Access	X	x.1.11	Enumerated	M, V				No
WLAN-Tunneling	X	x.1.12	Enumerated	M, V				No
APN-Authorised	X	x.1.14	Grouped	M, V				No
APN-Id	X	x.1.15	OctetString	M, V				No

APN-Authorisation	X	x.1.16	Enumerated	M, V				No
Local-Access	X	x.1.17	Enumerated	M, V				No
EAP payload	X	x.1.20	OctetString	M, V				No
Auth Req Type	X	x.1.21	Enumerated	M,V				No
EAP-Master-Session-Key	X	x.1.22	OctetString	M, V				No
Session-Request-Type	X	x.1.23	Enumerated	M, V				No
Routing-Policy	X	x.1.24	OctetString	M, V				No
Max-Requested-Bandwidth	X	x.1.26	Enumerated	M, V				No

NOTE 1: The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see IETF RFC 3588 [7].

10.1.1 Auth-Session-State

Between the 3GPP AAA server and the HSS, Diameter sessions are implicitly terminated. An implicitly terminated session is one for which the server does not maintain state information. The client does not need to send any re-authorization or session termination requests to the server.

The Diameter base protocol includes the Auth-Session-State AVP as the mechanism for the implementation of implicitly terminated sessions.

The client (server) shall include in its requests (responses) the Auth-Session-State AVP set to the value NO_STATE_MAINTAINED (1), as described in IETF RFC 3588 [7]. As a consequence, the server does not maintain any state information about this session and the client does not need to send any session termination request. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP shall be present in requests or responses.

10.1.2 User-Name

The User-Name AVP is defined in the IETF RFC 3588 [7] and contains the user identity.

For the WLAN Wx referende point, the User-Name AVP contains the IMSI of the subscriber.

10.1.3 Visited-Network-Identifier

The Visited-Network-Identifier AVP is defined in 3GPP TS 29.229[6] and indicates the 3GPP VPLMN where the user is roaming.

10.1.4 SIP-Auth-Data-Item

The SIP-Auth-Data-Item AVP is defined in 3GPP TS 29.229[6]. However three new more conditional AVPs are needed for WLAN Wx reference point.

AVP format

SIP-Auth-Data-Item :: = < AVP Header : TBD >

[SIP-Item-Number]

[SIP-Authentication-Scheme]

[SIP-Authenticate]

[SIP-Authorization]

[SIP-Authentication-Context]

[Confidentiality-Key]

[Integrity-Key]

[Authentication-Method]

[Authentication-Information-SIM]

[Authorization-Information-SIM]

* [AVP]

10.1.5 Authentication-Method

The Authentication-Method AVP (AVP code X) is of type UTF8String and indicates the authentication method required for the user. The following values are defined:

WLAN_EAP_SIM (0)

The UE indicates to the HSS that the required authentication method is EAP/SIM.

WLAN_EAP_AKA (1)

The UE indicates to the HSS that the required authentication method is EAP/AKA.

10.1.6 Authentication-Information-SIM

The Authentication-Information-SIM AVP (AVP code X) is of type OctetString and contains the concatenation of authentication challenge RAND and the ciphering key Kc.

10.1.7 Authorization –Information-SIM

The Authentication-Information-SIM AVP (AVP code X) is of type OctetString and contains the response SRES.

10.1.8 WLAN-User-Data

The WLAN-User-Data AVP (AVP code X) 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>

[MSISDN]

{ WLAN-Access }

{ WLAN-Tunneling }

[Session-Timeout]

1* { Charging-Data }

*[APN-Authorised]

{ Local-Access }

* [AVP]

10.1.9 MSISDN

The MSISDN AVP (AVP code 101) is defined in 3GPP TS 29.329 [x]. This identification could be used for example used for charging purposes.

Editor's Note: The optionality/presence could be modified by the SA1 and SA5 decision.

10.1.10 Charging-Information

The Charging-Mode AVP (AVP code 19) is of type is of type Grouped, and contains the addresses of the charging functions. It is defined in 3GPP TS 29.229 [6].

10.1.11 WLAN-Access

The WLAN-Access AVP (AVP code xx) is of type Enumerated, and allows operators to determine barring of 3GPP -WLAN interworking subscription. The following values are defined:

WLAN_SUBSCRIPTION_ALLOWED (0)

The subscriber has WLAN subscription.

WLAN_SUBSCRIPTION_BARRED (1)

The subscriber has no WLAN subscription.

10.1.12 WLAN-Tunneling

The WLAN-Tunneling AVP (AVP code xx) is of type Enumerated, and allows operator to disable all W-APNs at one time. If there is a conflict between this item and the "access allowed" flag of any W-APN, the most restrictive will prevail. The following values are defined:

WLAN_ APNS _ENABLE (0)

Enable all APNs.

WLAN_ APNS _DISABLE (1)

Disable all APNs

10.1.13 Session-Timeout

The Session-TimeOut AVP (AVP code 27) is defined in IETF RFC 3588 [7] and indicates the maximum period for a session measured in seconds.

This AVP is used for re-authentication purposes. If this field is not used, the WLAN AN will apply default

time intervals.

10.1.14 APN-Authorised

The APN-Authorised AVP (AVP code xx) is of type Grouped and contains authorization information for the APNs. This AVP indicates the list of allowed APNs and the environment where the access is allowed (visited or home PLMN). Also information is provided about the WLAN UE remote IP address when it has been statically assigned by the operator.

AVP format

APN-Authorised::= <AVP header: TBD>

{ APN-Id }

{ APN-Authorisation }

[Framed-IP-Address]

* [Framed-IPv6-Prefix]

* [AVP]

10.1.15 APN-Id

The APN-Id AVP (AVP code xx) 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.

10.1.16 APN-Authorisation

The APN-Authorisation AVP (AVP code xx) is of type Enumerated, and contains a flag indicating whether access is allowed in visited PLMNs or in the home PLMN.

WLAN_ APN_HOME (0)

Access is allowed in home PLMN only.

WLAN_ APN_VISITED (1)

Access is allowed in visited PLMNs and home PLMN.

10.1.17 Local-Access

The Local-Access AVP (AVP code xx) is of type Enumerated, and indicate whether the user has direct access to external IP networks, e.g. Internet, from the WLAN Access Network or not.

WLAN_ LOCAL_ACCESS (0)

The user is allowed to access directly to external IP networks.

WLAN_ NO_LOCAL_ACCESS (1)

The user is not allowed to access directly to external IP networks.

10.1.18 Server-Assignment-Type

The Server-Assignment-Type AVP (AVP code 15) 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.

10.1.19 Deregistration-Reason

The Deregistration-Reason AVP (AVP code 16) is defined in 3GPP TS 29.229 [6] and indicates reason for a de-registration operation.

This grouped AVP contains a Reason-Code AVP to indicate the reason for the de-registration. Reasons are listed in 3GPP TS 29.229 [6]. Wx reference point defines as valid only PERMANENT_TERMINATION value.

10.1.20 EAP-Payload

The EAP-Payload AVP (AVP code xx) is defined in the IETF draft-ietf-aaa-eap-08.txt [8] and contains the encapsulated EAP packet that is being exchanged between the EAP client and the home Diameter server.

10.1.21 Auth Req Type

The Auth Req Type AVP (AVP code xx) is of type Enumerated and indicates the action that the PDG is asking to the 3GPP AAA Server to perform (Authentication, authorization or both). Wm interface only makes use of the AUTHENTICATION_ONLY value. It is defined in the IETF draft-ietf-aaa-eap-08.txt [8]

10.1.22 EAP-Master-Session-Key

The EAP-Master-Session-Key AVP (AVP code xx) is of type OctetString and contains keying material for protecting the communications between the user and the NAS. It is defined in the IETF draft-ietf-aaa-eap-08.txt [8]

10.1.23 Session-Request-Type

The Session-Request-Type AVP (AVP code xx) is of type Enumerated and indicates the action that the PDG is asking to the 3GPP AAA Server to perform (authorization or routing policy). The following values are defined:

AUTHORIZATION REQUEST (0)

The PDG is requesting authorization for a user for a given W-APN.

ROUTING POLICY (1)

The PDG is indicating that routing policy information is present.

10.1.24 Routing-Policy

The Routing-Policy AVP (AVP code xx) is of type OctetString and indicates routing policies of the tunnel set-up.

Editor's Note: Its exact format is ffs.

10.1.25 Subscription-ID

The Subscription-ID AVP (AVP code xx) is of type Enumerated and indicates the user identity to be used for charging purposes. It is defined in the IETF Diameter Credit-Control Application draft [19].

WLAN shall make use only of the value MSISDN.

10.1.26 Max-Requested-Bandwidth

The Max-Requested-Bandwidth AVP (AVP code xx) is of type OctetString and indicates the Max requested bandwidth. If present, shall be sent from the 3GPP AAA Server to the PDG.

10.1.27 Routing Policy

The Routing Policy AVP (AVP code tbd) is of type IPFilterRule, and defines a packet filter for an IP flow with the following information:

7 Direction (in or out)

8 Source and destination IP address (possibly masked)

9 Protocol

10 Source and destination port (list or ranges)

Where the protocol type shall be set to ESP (50).

The IPFilterRule type shall be used with the following restrictions:

7 Only the Action "permit" shall be used.

8 No "options" shall be used.

9 The invert modifier "!" for addresses shall not be used.

10 The keyword "assigned" shall not be used.

11 For direction "out", an IPv4 destination IP address shall not be wildcarded. For direction "out", the 64 bits network prefix of an IPv6 destination IP address shall not be wildcarded.

The Flow description AVP shall be used to describe a single IP flow.

The direction "in" refers to uplink IP flows, and the direction "out" refers to downlink IP flows.

10.1.xx Framed-IP-Address

The Framed-IP-Address AVP is of type OctetString, and defines the remote IPv4 address that the operator has statically assigned to the WLAN UE.

When none of the Framed-IP-Address AVP and Framed-IPv6-Address AVP is present, the PDG shall dynamically assign, or ask some other node, e.g. a DHCP server, to assign, a remoten IP address to the WLAN UE.

~~The occurrence of this AVP is as per described in section 10.1 of NASREQ [12]:~~

~~Framed-IP-Address~~	~~0-1~~	~~0-1~~	

10.1.yy Framed-IPv6-Prefix

The Framed-IPv6-Address AVP is of type OctetString, and defines the remote IPv6 prefix that the operator has statically assigned to the WLAN UE.

When none of the Framed-IP-Address AVP and Framed-IPv6-Address AVP is present, the PDG shall dynamically assign, or ask some other node, e.g. a DHCP server, to assign, an remote IP address to the WLAN UE.

The occurrence of this AVP is as per described in section 10.1 of NASREQ [12]:

Framed-IPv6-Prefix	0+	0+

3GPP TSG-CN WG4 Meeting #25 ***N4-041578***

Seoul, KOREA. 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **008** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Online charging failure report
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	17/11/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:
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: ⌘ According to the following statements from LS S2-042830:

"Hence, the online charging system only needs to inform that 3GPP AAA Server that the user ran out of credit, and this information does not need to be forwarded to the HSS", and

"It is the understanding of the group that the only time the 3GPP AAA Server needs to inform the HSS is when the last tunnel is disconnected".

These statements indicate that the HSS has not to be informed of the reason for de-registering the user but a general deregistration code is enough and such a notification is only needed to be forwarded to the HSS when the last tunnel is disconnected.

Current TS 29.234 includes a reason code named ONLINE_CHARGING_FAILURE to inform the HSS about such on-line charging failure. This should be removed.

Summary of change: ⌘ This paper proposes to add the following changes to be compliant with the SA2 LS:

- Existing ONLINE_CHARGING_FAILURE code is removed from TS 29.234,
- 3GPP AAA Server notifies to the HSS about a user de-registration (ADMINISTRATIVE_REASON) when an on-line charging failure occurred

		only in the case that the 3GPP AAA Server disconnects all tunnels for that user.
Consequences if not approved:	⌘	Misalignment between Stage 2 and 3 for the Online charging failure

Clauses affected:	⌘	Table 6.3.2.1, 6.3.2.1.1, A.1.12			
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.

****** First modified section ******

Table 6.3.2.1: WLAN Registration 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 requests in the HSS. When this IE contains REGISTRATION value, the HSS performs a registration of the WLAN user. When this IE contains USER_DEREGISTRATION / ADMINISTRATIVE_DEREGISTRATION / REAUTHENTICATION_FAILURE ~~/ ONLINE_CHARGING_FAILURE~~ the HSS performs a de-registration of the WLAN user. When this IE contains NO_ASSIGNMENT value, the HSS initiates the download of the subscriber user profile towards the 3GPP AAA Server, but no registration is performed. Any other value is considered as an error case.
Routing Information (See 7.13)	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 the HSS, e.g. included in the MAA command. 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.

****** Second modified section ******

6.3.2.1.1 Detailed behaviour

When a new 3GPP subscriber has been authenticated and authorised by the 3GPP AAA Server, the 3GPP AAA Server initiates the registration towards the HSS. The HSS 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 HSS indicating the registration procedure. The subscriber is identified by the User-Name AVP.

At reception of Server-Assignment-Request command, the HSS 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, the HSS shall store the 3GPP AAA Server name for the authenticated and authorised 3GPP subscriber.

   - If it indicates USER_DEREGISTRATION / ADMINISTRATIVE_DEREGISTRATION / REAUTHENTICATION_FAILURE ~~/ ONLINE_CHARGING_FAILURE~~, the HSS shall remove the 3GPP AAA Server name previously assigned for the 3GPP subscriber.

   - If it indicates NO_ASSIGNMENT, the HSS shall download the relevant user identity information.

   - If it indicates any other value, the Result-Code shall be set to DIAMETER_UNABLE_TO COMPLY, and no registration/de-registration or profile download procedure shall be performed.

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

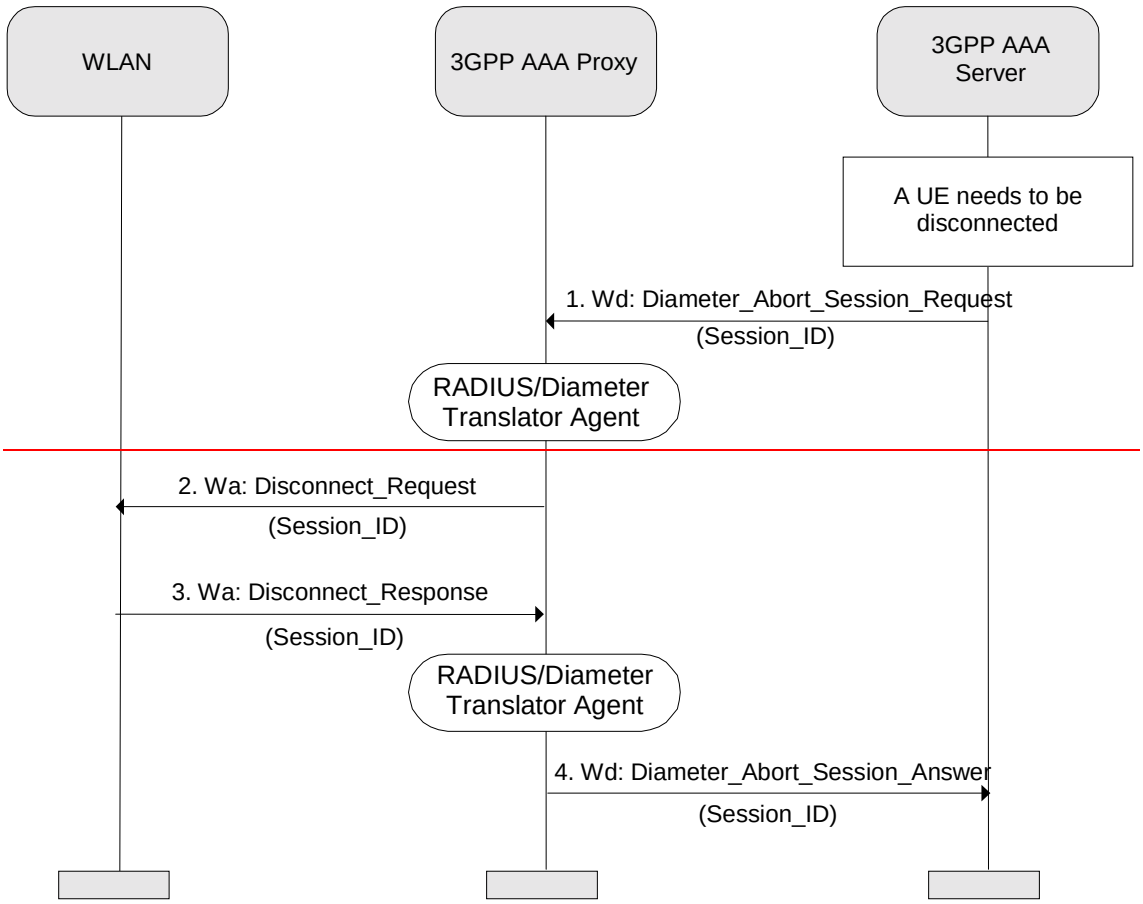
****** Second modified section ******

A.1.2. Immediate Purging of a WLAN User from the WLAN Access Network

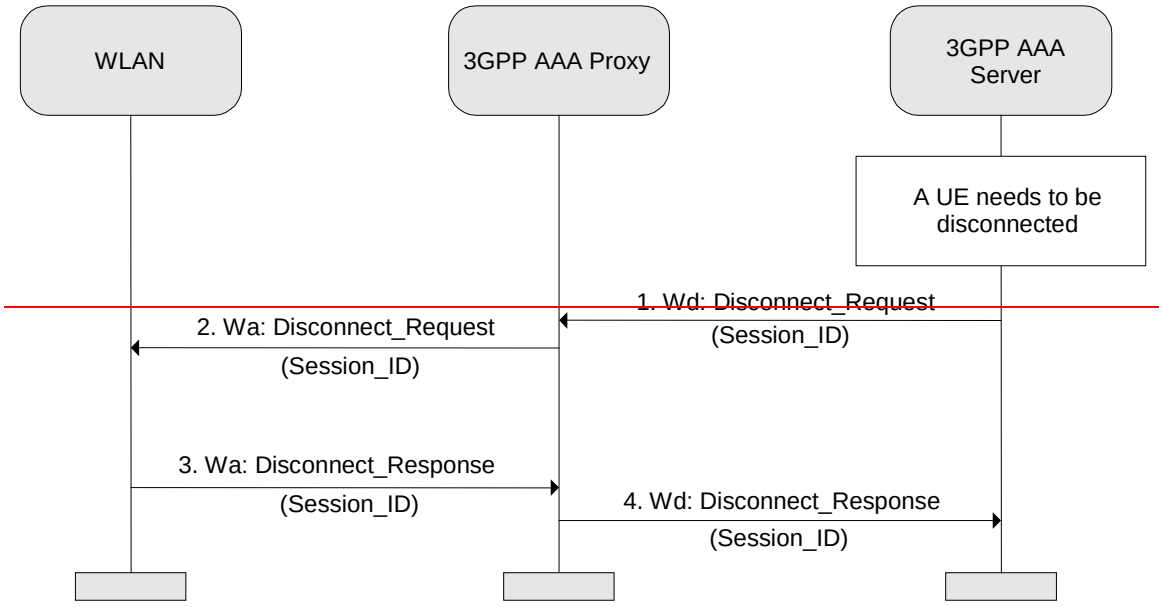
The purpose of this signalling sequence is to indicate to the WLAN AN that a specific WLAN-UE needs to be disconnected from accessing the WLAN interworking service.

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

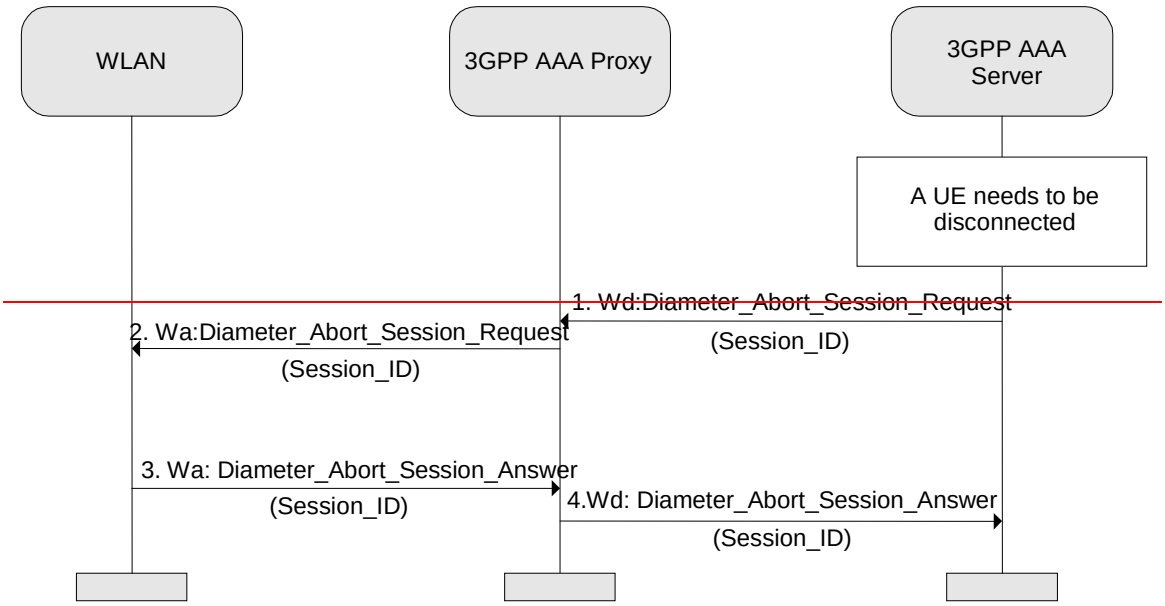
The signalling sequences shown are based on RADIUS and Diameter, as specified in sub-clauses 4 and 5. For more information on proxying and protocol translation associated with RADIUS and Diameter between the Wa and Wd reference points see sub-clause 5.3.



~~Figure A.4: Wa and Wd message flow for User Purging Case a) Wa using RADIUS and Wd using Diameter~~



~~Figure A.5: Wa and Wd message flow for User Purging Case b) Wa and Wd using RADIUS~~



~~Figure A.6: Wa and Wd message flow for User Purging Case c) Wa and Wd using Diameter~~

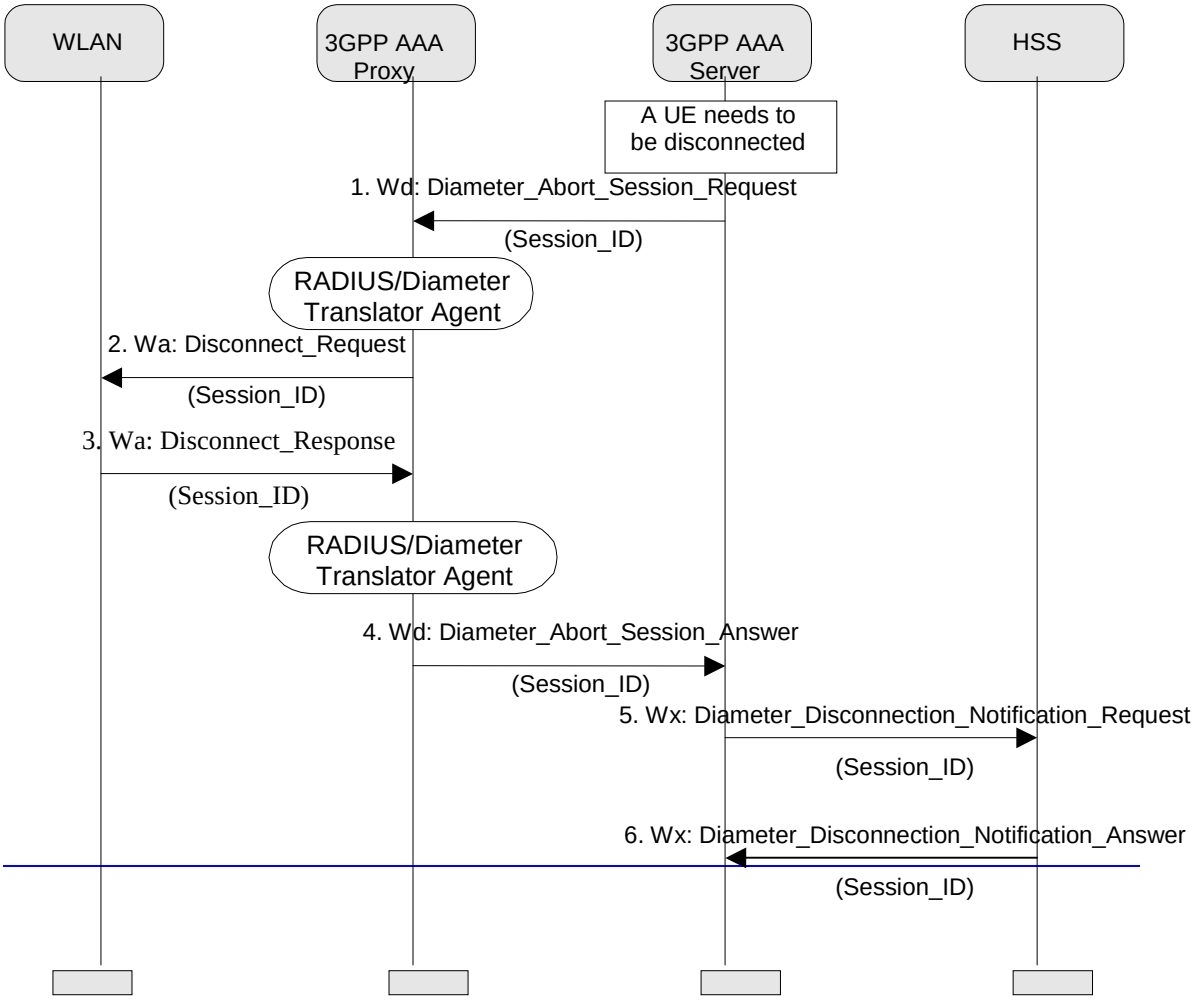


Figure A.4: Wa and Wd message flow for User Purging. Case a) Wa using RADIUS and Wd using Diameter

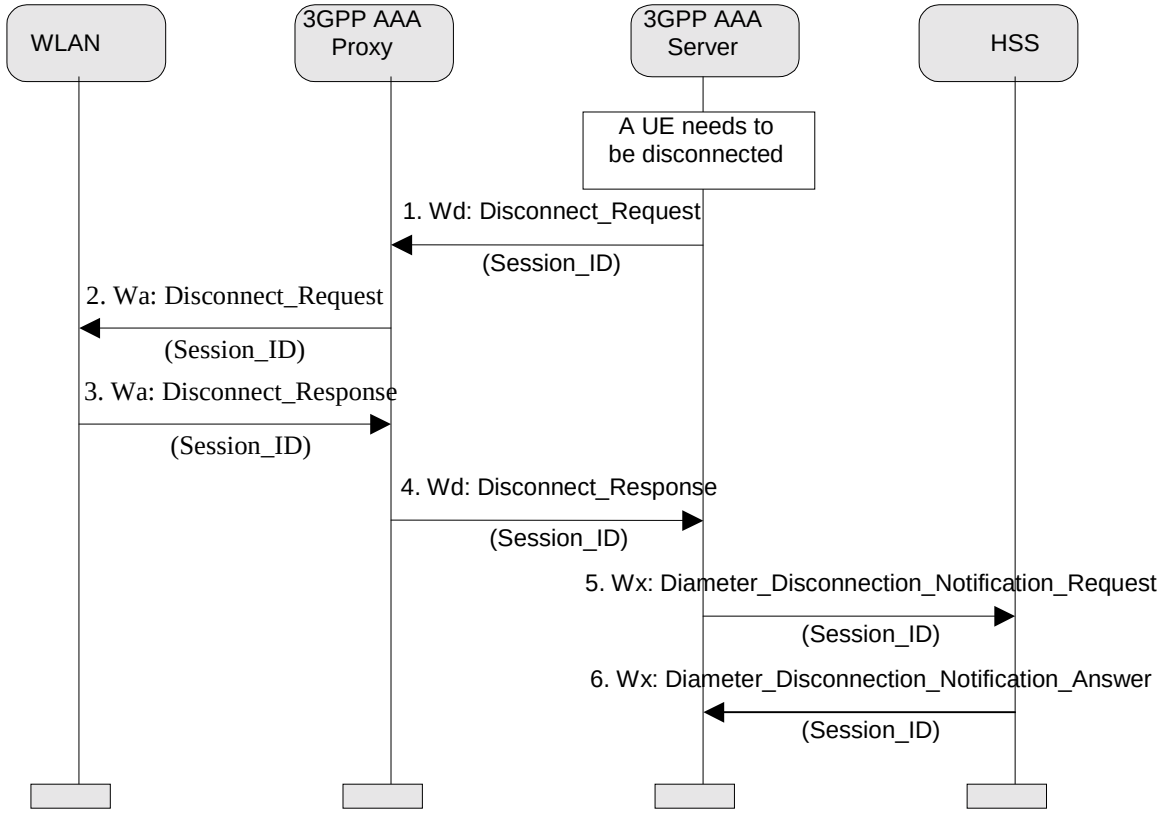


Figure A.5: Wa and Wd message flow for User Purging. Case b) Wa and Wd using RADIUS

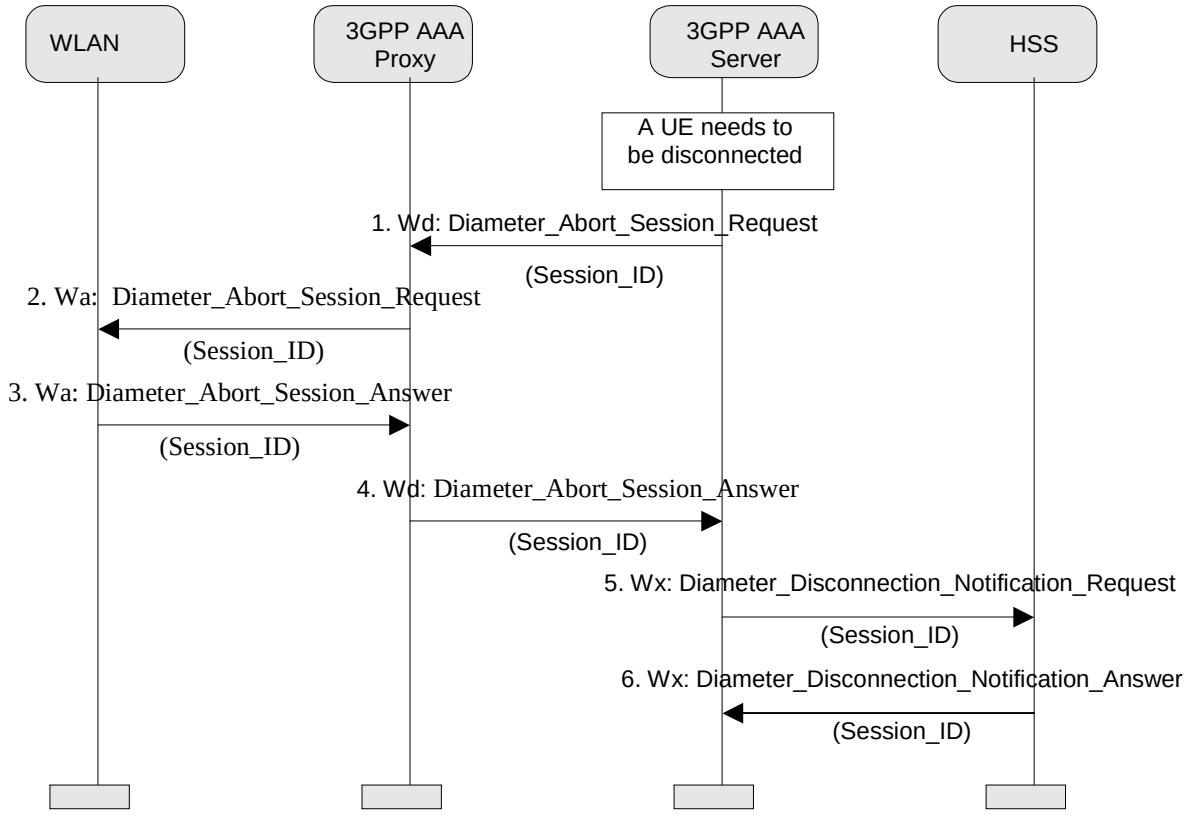


Figure A.6: Wa and Wd message flow for User Purging. Case c) Wa and Wd using Diameter

1. When the 3GPP AAA Server needs to disconnect (e.g. after receiving an external trigger) a 3GPP subscriber from the WLANAN, the 3GPP AAA Server sends to the 3GPP AAA Proxy either:

   a) "Disconnect_Request" message

   b) "Diameter_Abort_Session_Request" message

   Both messages carry a Session-ID used to identify the session within the WLAN AN.

2. The 3GPP AAA Proxy then performs one of the following two procedures:

   a) Converts the "Diameter_Abort_Session_Request" message to "Disconnect_Request" by use of the "RADIUS/Diameter Translator Agent" and sends this "Disconnect_Request" message to the WLAN AN;

b) Proxies the "Disconnect_Request" or "Diameter_Abort_Session_Request" message to the WLAN AN.

3. The WLAN AN responds to the 3GPP AAA Server via the 3GPP AAA Proxy with either:

   a) "Disconnect_Response" message;

   b) "Diameter_Abort_Session_Answer" message.

   Both messages carry the Session-ID received in the request message.

4. The 3GPP AAA Proxy then performs one of the following two procedures:

   a) Converts the "Disconnect_Response" message to a "Diameter_Abort_Session_Answer" message by use of the " RADIUS/Diameter Translator Agent" and sends this "Diameter_Abort_Session_Answer" message to the 3GPP AAA Server;

b) Proxies the "Disconnect_Response" or "Diameter_Abort_Session_Answer" message to the 3GPP AAA Server.

5. The 3GPP AAA Proxy then informs the HSS about a user de-registration (ADMINISTRATIVE_REASON) when an on-line charging failure occurred, only in the case that the 3GPP AAA Server disconnects all tunnels for that user.

3GPP TSG-CN WG4 Meeting #25 ***N4-041585***

Seoul, Korea. November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **015** ⌘**rev** **1** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Addition of ABNF definitions missing onWa, Wd Wm, Wg interfaces
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	15.11.2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
- ***F*** *(correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(addition of feature),*
- ***C*** *(functional modification of feature)*
- ***D*** *(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

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:	⌘	ABNF definitions are missing from the Wm & Wg interfaces
Summary of change:	⌘	Addition of ABNF to Wa, Wd, Wm and Wg interfaces
Consequences if not approved:	⌘	Unclear for implementors which fields are necessary in Wa, Wd, Wm & Wg Diameter messages
Clauses affected:	⌘	4.5.2.2.1, 5.5.1, 5.5.2, 5.5.3, 8, 9

		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 ****

4.5.2.2.1 Information Element Contents

The ABNF for the Accounting Request and Accouting Response messages over the Wa interface are given below:

<AC-Request> ::= < Diameter Header: 271, REQ, PXY >
< Session-Id >
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Accounting-Record-Type }
{ Accounting-Record-Number }
[Acct-Application-Id]
[Vendor-Specific-Application-Id]
[User-Name]
[Accounting-Sub-Session-Id]
[Acct-Session-Id]
[Acct-Multi-Session-Id]
[Origin-State-Id]
[Destination-Host]
[Event-Timestamp]
[Acct-Delay-Time]
[NAS-Identifier]
[NAS-IP-Address]
[NAS-IPv6-Address]
[Acc-Terminate-Cause]
[Accounting-Session-Time]
[NAS-Port]
[NAS-Port-Id]
[NAS-Port-Type]

<AC-Answer> ::= < Diameter Header: 271, PXY >
< Session-Id >
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
{ Accounting-Record-Type }
{ Accounting-Record-Number }
[Acct-Application-Id]
[Vendor-Specific-Application-Id]
[User-Name]
[Accounting-Sub-Session-Id]
[Acct-Session-Id]
[Acct-Multi-Session-Id]

[Event-Timestamp]
[Error-Message]
[Error-Reporting-Host]
* [Failed-AVP]
[Origin-State-Id]
[NAS-Identifier]
[NAS-IP-Address]
[NAS-IPv6-Address]
[NAS-Port]
[NAS-Port-Id]
[NAS-Port-Type]
[Service-Type]
[Termination-Cause]
[Accounting-Realtime-Required]
[Acct-Interim-Interval]
* [Class]
* [Proxy-Info]
* [Route-Record]
* [AVP]

**** Second modified section ****

5.5 Information Elements Contents

~~FFS~~

~~5.5.1 Authentication Procedures~~

~~ABNF for the Wd Diameter EAP Request/Answer 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

**** Third modified section ****

8.x Information Element Contents

8.x.1 Authentication Request/Response Messages

ABNF for the Wm Authentication Request and Authentication Answer 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 ]
            [ Visited-Network-Identifier ]
            [ 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 }
            { Auth-Request-Type }
            { Result-Code }
            { Origin-Host }
            { Origin-Realm }
            [ User-Name ]
            [ Master-Session-Key ]
            [ EAP-Payload ]
            * [ Proxy-Info ]
            * [ AVP ]
```

8.x.2 Authorization Procedures

The authorization request and response messages are mapped onto the NASREQ AAR/AAA messages. The ABNF are indicated below:

```
<AA-Request> ::= < Diameter Header: 265, REQ, PXY >
            < Session-Id >
            { Auth-Application-Id }
            { Origin-Host }
```

{ Origin-Realm }
{ Destination-Realm }
{ Auth-Request-Type }
[Destination-Host]
[Session-Request-Type]
[Visited-Network-Identifier]
[APN-ID]
[Routing-Policy]
[NAS-Identifier]
[NAS-IP-Address]
[NAS-IPv6-Address]
[NAS-Port]
[NAS-Port-Id]
[NAS-Port-Type]
[Origin-State-Id]
[Port-Limit]
[User-Name]
[User-Password]
[Service-Type]
[State]
[Authorization-Lifetime]
[Auth-Grace-Period]
[Auth-Session-State]
[Callback-Number]
[Called-Station-Id]
[Calling-Station-Id]
[Originating-Line-Info]
[Connect-Info]
[CHAP-Auth]
[CHAP-Challenge]
* [Framed-Compression]
[Framed-Interface-Id]
[Framed-IP-Address]
[Framed-IP-Netmask]
[Framed-MTU]
[Framed-Protocol]
[ARAP-Password]
[ARAP-Security]
* [ARAP-Security-Data]
* [Login-IP-Host]
* [Login-IPv6-Host]
[Login-LAT-Group]
[Login-LAT-Node]
[Login-LAT-Port]
[Login-LAT-Service]
* [Tunneling]
* [Proxy-Info]
* [Route-Record]
* [AVP]

The ABNF for the AAA is 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]
[Max-Subscribed-Bandwidth]
[Framed-IP-Address]
[Framed-IP-Prefix]
[Charging-Data]
[Service-Type]
* [Class]
* [Configuration-Token]
[Acct-Interim-Interval]
[Error-Message]
[Error-Reporting-Host]
* [Failed-AVP]
[Idle-Timeout]

[Authorization-Lifetime]
[Auth-Grace-Period]
[Auth-Session-State]
[Re-Auth-Request-Type]
[Session-Timeout]
[State]
* [Reply-Message]
[Origin-State-Id]
* [Filter-Id]
[Password-Retry]
[Port-Limit]
[Prompt]
[ARAP-Challenge-Response]
[ARAP-Features]
[ARAP-Security]
* [ARAP-Security-Data]
[ARAP-Zone-Access]
[Callback-Id]
[Callback-Number]
[Framed-Appletalk-Link]
* [Framed-Appletalk-Network]
[Framed-Appletalk-Zone]
* [Framed-Compression]
[Framed-Interface-Id]
[Framed-IP-Address]
* [Framed-IPv6-Prefix]
[Framed-IPv6-Pool]
* [Framed-IPv6-Route]
[Framed-IP-Netmask]
* [Framed-Route]
[Framed-Pool]
[Framed-IPX-Network]
[Framed-MTU]
[Framed-Protocol]
[Framed-Routing]
* [Login-IP-Host]
* [Login-IPv6-Host]
[Login-LAT-Group]
[Login-LAT-Node]
[Login-LAT-Port]
[Login-LAT-Service]
[Login-Service]
[Login-TCP-Port]
* [NAS-Filter-Rule]
* [QoS-Filter-Rule]
* [Tunneling]
* [Redirect-Host]
[Redirect-Host-Usage]
[Redirect-Max-Cache-Time]
* [Proxy-Info]
* [AVP]

8.x.3 PDG Initiated Session Termination Procedure

This procedure is mapped onto the STR/STA procedures. The ABNF are as follows:

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

For the response:

```
<STA>  ::= < Diameter Header: 275, PXY >
            < Session-Id >
            { Result-Code }
            { Origin-Host }
            { Origin-Realm }
            [ User-Name ]
            * [ Class ]
            [ Error-Message ]
            [ Error-Reporting-Host ]
            * [ Failed-AVP ]
            [ Origin-State-Id ]
            * [ Redirect-Host ]
            [ Redirect-Host-Usage ]
            [ Redirect-Max-Cache-Time ]
            * [ Proxy-Info ]
            * [ AVP ]
```

8.x.4 3GPP AAA Server Initiated Tunnel Disconnect Procedure

ABNF for the 3GPP AAA Server Initiated Tunnel Disconnect Procedure are mapped onto 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 ]
            [ 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 ]
```

**** FourthSecond modified section ****

9.x Information Element Contents

9.x.1 Policy Download Procedures

The Wg Policy Download Request/Response are mapped onto the NASREQ AAR/AAA messages. The ABNF are indicated below:

```
<AA-Request> ::= < Diameter Header: 265, REQ, PXY >
             < Session-Id >
             { Auth-Application-Id }
             { Origin-Host }
             { Origin-Realm }
             { Destination-Realm }
             { Auth-Request-Type }
             [Destination-Host]
             [ Routing Policy ]
             [ Subscription-ID ]
             [ NAS-Identifier ]
             [ NAS-IP-Address ]
             [ NAS-IPv6-Address ]
             [ NAS-Port ]
             [ NAS-Port-Id ]
             [ NAS-Port-Type ]
             [ Origin-State-Id ]
             [ Port-Limit ]
             [ User-Name ]
             [ User-Password ]
             [ Service-Type ]
             [ State ]
             [ Authorization-Lifetime ]
             [ Auth-Grace-Period ]
             [ Auth-Session-State ]
             [ Callback-Number ]
             [ Called-Station-Id ]
             [ Calling-Station-Id ]
             [ Originating-Line-Info ]
             [ Connect-Info ]
             [ CHAP-Auth ]
             [ CHAP-Challenge ]
          *  [ Framed-Compression ]
             [ Framed-Interface-Id ]
             [ Framed-IP-Address ]
             [ Framed-IP-Netmask ]
             [ Framed-MTU ]
             [ Framed-Protocol ]
             [ ARAP-Password ]
             [ ARAP-Security ]
          *  [ ARAP-Security-Data ]
          *  [ Login-IP-Host ]
          *  [ Login-IPv6-Host ]
             [ Login-LAT-Group ]
             [ Login-LAT-Node ]
             [ Login-LAT-Port ]
             [ Login-LAT-Service ]
          *  [ Tunneling ]
          *  [ Proxy-Info ]
          *  [ Route-Record ]
          *  [ AVP ]
```

The ABNF for the AAA is as follows:

```
<AA-Answer> ::= < Diameter Header: 265, PXY >
             < Session-Id >
             { Auth-Application-Id }
             { Auth-Request-Type }
             { Result-Code }
             { Origin-Host }
             { Origin-Realm }
             [ User-Name ]
             [ Service-Type ]
          *  [ Class ]
          *  [ Configuration-Token ]
```

[Acct-Interim-Interval]
[Error-Message]
[Error-Reporting-Host]
* [Failed-AVP]
[Idle-Timeout]
[Authorization-Lifetime]
[Auth-Grace-Period]
[Auth-Session-State]
[Re-Auth-Request-Type]
[Session-Timeout]
[State]
* [Reply-Message]
[Origin-State-Id]
* [Filter-Id]
[Password-Retry]
[Port-Limit]
[Prompt]
[ARAP-Challenge-Response]
[ARAP-Features]
[ARAP-Security]
* [ARAP-Security-Data]
[ARAP-Zone-Access]
[Callback-Id]
[Callback-Number]
[Framed-Appletalk-Link]
* [Framed-Appletalk-Network]
[Framed-Appletalk-Zone]
* [Framed-Compression]
[Framed-Interface-Id]
[Framed-IP-Address]
* [Framed-IPv6-Prefix]
[Framed-IPv6-Pool]
* [Framed-IPv6-Route]
[Framed-IP-Netmask]
* [Framed-Route]
[Framed-Pool]
[Framed-IPX-Network]
[Framed-MTU]
[Framed-Protocol]
[Framed-Routing]
* [Login-IP-Host]
* [Login-IPv6-Host]
[Login-LAT-Group]
[Login-LAT-Node]
[Login-LAT-Port]
[Login-LAT-Service]
[Login-Service]
[Login-TCP-Port]
* [NAS-Filter-Rule]
* [QoS-Filter-Rule]
* [Tunneling]
* [Redirect-Host]
[Redirect-Host-Usage]
[Redirect-Max-Cache-Time]
* [Proxy-Info]
* [AVP]

9.x.2 Routing Policy Cancellation Procedure

The Policy Cancellation Request/Response messages are mapped onto ASR/ASA messages. The ABNF are given 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]

9.x.3 WAG Initiated Routing Policy Cancellation Procedure

The WAG initiated Routing Policy Cancellation Procedure is mapped onto the STR/STA messages. The ABNF are given below:

<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]

For the response:

<STA> ::= < Diameter Header: 275, PXY >
< Session-Id >
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
[User-Name]
*[Class]
[Error-Message]
[Error-Reporting-Host]
*[Failed-AVP]
[Origin-State-Id]
*[Redirect-Host]
[Redirect-Host-Usage]
[Redirect-Max-Cache-Time]
*[Proxy-Info]
*[AVP]

3GPP TSG-CN WG4 Meeting #25 ***N4-041586***

Seoul, Korea. November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **016** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Access Independence for WLAN 3GPP IP access
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	18/11/2004
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:	SA2 recently agreed a CR, S2-042503, which states that WLAN 3GPP IP access (Scenario 3) can be provided independently of WLAN Direct Access (Scenario 2). 29.234 should therefore be updated to provide this functionality, since at present this is not possible in the spec. Further, this functionality shall be per user subscription decision.
Summary of change:	Build in the access independence to the spec
Consequences if not approved:	Feature required by SA2 not supported in Cn4 spec

Clauses affected:	2, 6, 8, 10

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.

**** First modified section ****

2 References

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

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

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

[2] 3GPP TR 22.934: "Feasibility Study on 3GPP system to WLAN interworking"

[3] 3GPP TR 23.934: "3GPP system to WLAN Interworking; Functional and architectural definition"

[4] 3GPP TS 23.234: "3GPP system to 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, TS 29.229, Protocol details"

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

[8] IETF Draft: "Diameter Extensible Authentication Protocol (EAP) Application", draft-ietf-aaa-eap-06.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, "Attributes for Access Network Location and Ownership Information", http://www.ietf.org/internet-drafts/draft-tschofenig-geopriv-radius-lo-00.txt, work in progress

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

[18] 3GPP TS 33.234: "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"

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

**** Second modified section ****

6 Wx Description

Wx is the reference point between 3GPP AAA Server and HSS. The prime purpose of the protocols crossing this reference point to communicate 3GPP AAA Server and HSS

6.1 Functionality

The functionality of the reference point is to enable:

- Retrieval of authentication vectors (triplets and quintuplets) from HSS
- Retrieval of WLAN subscriber profile retrieval from HSS
- Indication to 3GPP AAA Server of change of WLAN subscriber profile within HSS
- Registration of the 3GPP AAA Server of an authorised WLAN user in the HSS
- Purge procedure between the 3GPP AAA server and the HSS
- Retrieval of online charging / offline charging function addresses from HSS

~~7- Fault recovery procedure between the HSS and the 3GPP AAA server~~

~~8authorization of a WLAN user via checking of user subscription information at the HSS~~

~~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.

6.3 Procedures Description

6.3.1 Authentication Procedures

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

9- Retrieval of authentication vectors (triplets and quintuplets) from HSS.

10checking 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 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. A further possibility is for WLAN 3GPP IP access only i.e. where the UE is setting up a tunnel to the PDG without previously being authenticated for WLAN direct access 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	M	Identifier that allows the home network to identify the Visited Network. 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 the HSS, e.g. included in the

				MAA command. 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 [XX]

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
Private 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.
	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
Authotization 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 3. Check that the user is allowed to roam in the visited network. If 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 whether the user has dependence permissions that the user has with regard to the access type.

2If 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.

3If 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.

4If 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.

45. Check that the authentication method indicated in the request is supported. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_AUTH_METHOD_UNSUPPORTED.

56. 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.

67. 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.

**** Second modified section ****

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 IETF 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]

6.5 Result-Code AVP values

This section defines new result code values that shall be supported by all Diameter implementations that conform to this specification. When one of the result codes defined here is included in a response, it shall be inside an Experimental-Result AVP and Result-Code AVP shall be absent.

6.5.1 Permanent Failures

Errors that fall within the Permanent Failures category are used to inform the peer that the request failed, and should not be attempted again.

6.5.1.1 DIAMETER_ERROR_USER_NO_SERVICE_SUBSCRIPTON (500x)

A message was received for a user with no WLAN-subscription.

6.5.1.2 DIAMETER_ERROR_AUTH_METHOD_UNSUPPORTED (500x)

The authentication method indicated in an authentication request (Authentication-Method AVP) is not supported.

Editor's Note: It is FFS whether this Error Code can be replaced by the general DIAMETER_ERROR_AUTH_SCHEME_NOT_SUPPORTED (5006) error code defined in 3GPP TS 29.229 [6].

6.5.1.3 DIAMETER_ERROR_W-APN_UNUSED_BY_USER

A message was received for a user who has no subscription for a specified W-APN.

6.5.1.4 6.5.1.4 DIAMETER_ERROR_NO_ACCESS_INDEPENDENT_SUBSCRIPTION

A message was received requesting WLAN 3GPP IP access for a user whose subscription does not allow it if it was not previously authenticated by WLAN 3GPP direct access.

**** Third modified section ****

8 Wm Description

8.1 Functionality

This clause specifies a Diameter application that allows the following messaging to take place between the 3GPP AAA Server and the PDG :

- *The 3GPP AAA Server/Proxy retrieves tunneling attributes and WLAN UE's IP configuration parameters from the Packet Data Gateway.*
- *Messaging for service authentication between WLAN UE and 3GPP AAA Server/Proxy.*
- *Messaging for service authorization between PDG and 3GPP AAA Server/Proxy.*
- *Messaging for carrying authentication data for the purpose of tunnel establishment, tunnel data authentication and encryption.*

In the roaming case, the 3GPP AAA Proxy shall act as a stateful proxy between the PDG and 3GPP AAA Server.

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 [18].For authorization and other Wm functionalities, NASREQ and base protocol procedures are used.

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 [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[18].

Table 8.3.1.1 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.
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 [XX]

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 [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:

2.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 Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

3.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).

**** Fourth modified section ****

1110 Information Elements Contents

10.1 10.1 AVPs

The following table describes the Diameter AVPs defined for the WLAN reference point, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted. The Vendor-Id header of all AVPs defined in this specification shall be set to 3GPP (10415).
Only those AVPs defined by 3GPP TS 29.234 reference point are listed here.

Table 10.1.1: Diameter Multimedia Application AVPs

					AVP Flag rules				
	Attribute Name	AVP Code	Section defined	Value Type	Shall	May	Should not	Must not	May Encr.
	Authentication-Method	X	X10.1.5	UTF8String	M, V				No
	Authentication-Information-SIM	X	10x.1.6	OctetString	M, V				No
	Authorization-Information-SIM	X	10x.1.7	OctetString	M,V				No
	WLAN-User-Data	X	10x.1.8	Grouped	M, V				No
	WLAN-Access	X	10x.1.11	Enumerated	M, V				No
	WLAN-Tunneling	X	10x.1.12	Enumerated	M, V				No
	APN-Authorised	X	10x.1.14	Grouped	M, V				No
	APN-Id	X	10x.1.15	OctetString	M, V				No
	APN-Authorisation	X	10x.1.16	Enumerated	M, V				No

	Local-Access	X	10x.1.17	Enumerated	M, V				No
	EAP-payload	X	10x.1.20	OctetString	M, V				No
	Auth-Req-Type	X	10x.1.21	Enumerated	M,V				No
	EAP-Master-Session-Key	X	10x.1.22	OctetString	M, V				No
	Session-Request_Type	X	10x.1.23	Enumerated	M, V				No
	Routing-Policy	X	10x.1.24	OctetString	M, V				No
	Max-Requested-Bandwidth	X	10x.1.26	Enumerated	M, V				No
	NOTE 1: The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see IETF RFC 3588 [7].								

10.1.1 Auth-Session-State

Between the 3GPP AAA server and the HSS, Diameter sessions are implicitly terminated. An implicitly terminated session is one for which the server does not maintain state information. The client does not need to send any re-authorization or session termination requests to the server.

The Diameter base protocol includes the Auth-Session-State AVP as the mechanism for the implementation of implicitly terminated sessions.

The client (server) shall include in its requests (responses) the Auth-Session-State AVP set to the value NO_STATE_MAINTAINED (1), as described in IETF RFC 3588 [7]. As a consequence, the server does not maintain any state information about this session and the client does not need to send any session termination request. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP shall be present in requests or responses.

10.1.2 User-Name

The User-Name AVP is defined in the IETF RFC 3588 [7] and contains the user identity.

For the WLAN Wx referende point, the User-Name AVP contains the IMSI of the subscriber.

10.1.3 Visited-Network-Identifier

The Visited-Network-Identifier AVP is defined in 3GPP TS 29.229[6] and indicates the 3GPP VPLMN where the user is roaming.

10.1.4 SIP-Auth-Data-Item

The SIP-Auth-Data-Item AVP is defined in 3GPP TS 29.229[6]. However three new more conditional AVPs are needed for WLAN Wx reference point.

AVP format

SIP-Auth-Data-Item :: = < AVP Header : TBD >

[SIP-Item-Number]

[SIP-Authentication-Scheme]

[SIP-Authenticate]

[SIP-Authorization]

[SIP-Authentication-Context]

[Confidentiality-Key]

[Integrity-Key]

~~**[Authentication-Method]**~~

~~**[Authentication-Information-SIM]**~~

~~**[Authorization-Information-SIM]**~~

~~* [AVP]~~

~~10.1.5 Authentication-Method~~

~~The Authentication-Method AVP (AVP code X) is of type UTF8String and indicates the authentication method required for the user. The following values are defined:~~

~~WLAN_EAP_SIM (0)~~

~~The UE indicates to the HSS that the required authentication method is EAP/SIM.~~

~~WLAN_EAP_AKA (1)~~

~~The UE indicates to the HSS that the required authentication method is EAP/AKA.~~

~~10.1.6 Authentication-Information-SIM~~

~~The Authentication-Information-SIM AVP (AVP code X) is of type OctetString and contains the concatenation of authentication challenge RAND and the ciphering key Kc.~~

~~10.1.7 Authorization - Information-SIM~~

~~The Authentication-Information-SIM AVP (AVP code X) is of type OctetString and contains the response SRES.~~

~~10.1.8 WLAN-User-Data~~

~~The WLAN-User-Data AVP (AVP code X) 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>~~

~~[MSISDN]~~

~~{ WLAN-Access }~~

~~{ WLAN-Tunneling }~~

~~[Session-Timeout]~~

~~1* { Charging-Data }~~

~~*[APN-Authorised]~~

~~{ Local-Access }~~

~~* [AVP]~~

~~10.1.9 MSISDN~~

~~The MSISDN AVP (AVP code 101) is defined in 3GPP TS 29.329 [x]. This identification could be used for example used for charging purposes.~~

~~Editor's Note: The optionality/presence could be modified by the SA1 and SA5 decision.~~

10.1.10 Charging-Information

The Charging-Mode AVP (AVP code 19) is of type is of type Grouped, and contains the addresses of the charging functions. It is defined in 3GPP TS 29.229 [6].

10.1.11 WLAN-Access

The WLAN-Access AVP (AVP code xx) is of type Enumerated, and allows operators to determine barring of 3GPP -WLAN interworking subscription. The following values are defined:

WLAN_SUBSCRIPTION_ALLOWED (0)

The subscriber has WLAN subscription.

WLAN_SUBSCRIPTION_BARRED (1)

The subscriber has no WLAN subscription.

10.1.12 WLAN-Tunneling

The WLAN-Tunneling AVP (AVP code xx) is of type Enumerated, and allows operator to disable all W-APNs at one time. If there is a conflict between this item and the "access allowed" flag of any W-APN, the most restrictive will prevail. The following values are defined:

WLAN_ APNS _ENABLE (0)

Enable all APNs.

WLAN_ APNS _DISABLE (1)

Disable all APNs

10.1.13 Session-Timeout

The Session-TimeOut AVP (AVP code 27) is defined in IETF RFC 3588 [7] and indicates the maximum period for a session measured in seconds.

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

10.1.14 APN-Authorised

The APN-Authorised AVP (AVP code xx) is of type Grouped and contains authorization information for the APNs. This AVP indicates the list of allowed APNs and the environment where the access is allowed (visited or home PLMN).

AVP format

APN-Authorised::= <AVP header: TBD>

{ APN-Id }

{ APN-Authorisation }

* [AVP]

10.1.15 APN-Id

The APN-Id AVP (AVP code xx) 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.

10.1.16 APN-Authorisation

The APN-Authorisation AVP (AVP code xx) is of type Enumerated, and contains a flag indicating whether access is allowed in visited PLMNs or in the home PLMN.

WLAN_APN_HOME (0)

Access is allowed in home PLMN only.

WLAN_APN_VISITED (1)

Access is allowed in visited PLMNs and home PLMN.

10.1.17 Local-Access

The Local-Access AVP (AVP code xx) is of type Enumerated, and indicate whether the user has direct access to external IP networks, e.g. Internet, from the WLAN Access Network or not.

WLAN_LOCAL_ACCESS (0)

The user is allowed to access directly to external IP networks.

WLAN_NO_LOCAL_ACCESS (1)

The user is not allowed to access directly to external IP networks.

10.1.18 Server-Assignment-Type

The Server-Assignment-Type AVP (AVP code 15) 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.

10.1.19 Deregistration-Reason

The Deregistration Reason AVP (AVP code 16) is defined in 3GPP TS 29.229 [6] and indicates reason for a de-registration operation.

This grouped AVP contains a Reason-Code AVP to indicate the reason for the de-registration. Reasons are listed in 3GPP TS 29.229 [6]. Wx reference point defines as valid only PERMANENT_TERMINATION value.

10.1.20 EAP-Payload

The EAP-Payload AVP (AVP code xx) is defined in the IETF draft ietf-aaa-eap-08.txt [8] and contains the encapsulated EAP packet that is being exchanged between the EAP client and the home Diameter server.

10.1.21 Auth-Req-Type

The Auth-Req-Type AVP (AVP code xx) is of type Enumerated and indicates the action that the PDG is asking to the 3GPP AAA Server to perform (Authentication, authorization or both). Wm interface only makes use of the AUTHENTICATION_ONLY value. It is defined in the IETF draft ietf-aaa-eap-08.txt [8]

10.1.22 EAP-Master-Session-Key

The EAP-Master-Session-Key AVP (AVP code xx) is of type OctetString and contains keying material for protecting the communications between the user and the NAS. It is defined in the IETF draft ietf-aaa-eap-08.txt [8]

10.1.23 Session-Request-Type

The Session-Request-Type AVP (AVP code xx) is of type Enumerated and indicates the action that the PDG is asking to the 3GPP AAA Server to perform (authorization or routing policy). The following values are defined:

AUTHORIZATION REQUEST (0)

The PDG is requesting authorization for a user for a given W-APN.

ROUTING POLICY (1)

The PDG is indicating that routing policy information is present.

10.1.24 Routing-Policy

The Routing-Policy AVP (AVP code xx) is of type OctetString and indicates routing policies of the tunnel set up.

Editor's Note: Its exact format is ffs.

10.1.25 Subscription-ID

The Subscription-ID AVP (AVP code xx) is of type Enumerated and indicates the user identity to be used for charging purposes. It is defined in the IETF Diameter Credit-Control Application draft [19].

WLAN shall make use only of the value MSISDN.

10.1.26 Max-Requested-Bandwidth

The Max-Requested-Bandwidth AVP (AVP code xx) is of type OctetString and indicates the Max requested bandwidth. If present, shall be sent from the 3GPP AAA Server to the PDG.

10.1.27 Routing Policy

The Routing Policy AVP (AVP code tbd) is of type IPFilterRule, and defines a packet filter for an IP flow with the following information:

8Direction (in or out)

9Source and destination IP address (possibly masked)

10Protocol

11Source and destination port (list or ranges)

Where the protocol type shall be set to ESP (50).

The IPFilterRule type shall be used with the following restrictions:

8Only the Action "permit" shall be used.

9No "options" shall be used.

10The invert modifier "!" for addresses shall not be used.

11The keyword "assigned" shall not be used.

12For direction "out", an IPv4 destination IP address shall not be wildcarded. For direction "out", the 64 bits network prefix of an IPv6 destination IP address shall not be wildcarded.

The Flow description AVP shall be used to describe a single IP flow.

The direction "in" refers to uplink IP flows, and the direction "out" refers to downlink IP flows.

10.1.x EAP-Lower-Layer AVP

The EAP-Lower-Layer AVP indicates the layer 2 protocol which has been used to carry EAP messages. It is defined in the IETFdraft-mariblanca-aaa-eap-lla-01[xx].
For I-WLAN, only 802.1X value for WLAN 3GPP Direct access and IKEv2 value for WLAN 3GPP IP access are valid.

3GPP TSG-CN WG4 Meeting #25 ***N4-041591***

Seoul, Korea. November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **019** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Editorial Modifications
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	29/11/2004
Category:	⌘	**D**
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:	Improves readability of the document
Summary of change:	Wf interface description changed in the symbols Superfluous sentence removed from top of chapter 6 Chapters 8 and 9 sections renumbered Removed duplicated Routing policy AVP section in 10.1
Consequences if not approved:	Unclear spec

Clauses affected:	3.2, 6, 8.4, 9.4, 10.1.24, 20.1.27

	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 ****

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

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 ~~CGw/CCF~~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

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
RADIUS	Remote Authentication Dial-In User Service
WAG	WLAN Access Gateway
WLAN AN	WLAN Access Network
WLAN	Wireless Local Access Network
WLAN-UE	WLAN User Equipment

**** Second modified section ****

6 Wx Description

Wx is the reference point between 3GPP AAA Server and HSS.

~~The prime purpose of the protocols crossing this reference point to communicate 3GPP AAA Server and HSS.~~

**** Third modified section ****

8 Wm Description

8.1 Functionality

This clause specifies a Diameter application that allows the following messaging to take place between the 3GPP AAA Server and the PDG:

- The 3GPP AAA Server/Proxy retrieves tunnelling attributes and WLAN UE's IP configuration parameters from the Packet Data Gateway.
- Messaging for service authentication between WLAN UE and 3GPP AAA Server/Proxy.
- Messaging for service authorization between PDG and 3GPP AAA Server/Proxy.
- Messaging for carrying authentication data for the purpose of tunnel establishment, tunnel data authentication and encryption.

In the roaming case, the 3GPP AAA Proxy shall act as a stateful proxy between the PDG and 3GPP AAA Server.

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.

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
Permanent User Identity	User-Name	M	This information element contains the permanent identity of the user, i.e. the IMSI.
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.

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 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.

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).

~~8.4 Procedures Description~~

8.34.21 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.

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

Table 8.34.21.1 Wm Authorization 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.
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 8.34.21.2: 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.

8.34.21.1 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 APN-User-Data AVP. 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.

8.34.21.2 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.

8.3.35 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 8.35..3.1: Session Termination 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.
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 8.3.3.5.2: 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.

8.3.15.1 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.

8.3.25.2 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.

8.3.46 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 8.3.46.1: 3GPP AAA Server Initiated Tunnel Disconnection - 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.
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 8.3.46.2: 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.

8.3.16.1 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~~6.2~~ 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.

9 Wg Description

Wg is the reference point that connects the 3GPP AAA Server/Proxy to the WAG. The prime purpose of this reference point is to transfer Policy Enforcement rules to the WAG, which would enable WAG to allow only authorized packets to/from the WLAN AN. This interface is applicable only when a WLAN UE is allowed to access the 3GPP PS services from the 3G-WLAN interworking network.

9.1 Functionality

This clause specifies a Diameter application that allows the following messaging to take place between the 3GPP AAA Server and the WAG for the case where the PDG is in the HPLMN, and between the 3GPP AAA Proxy and the WAG for the case where the PDG is in the VPLMN:

- data carrying policy Enforcement rules to be applied to packets to/from WLAN AN.
- transport per-tunnel based charging information from the WAG to the AAA Proxy/Server.

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 scenario 3 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 shall act as the NAS client and the WAG as the Diameter Server

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.

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.**

9.3.1.1 WAG Detailed Behaviour

On receipt of the Policy Download Request, the WAG shall check whether or not the user has already routing policies stored:

- If it has, the WAG shall modify the routing policy accordingly.
- Otherwise, the WAG shall take necessary steps to provision the new routing policy indicated in the routing policy AVP for the user in order to allow data plane packet flows across the Wn interface.

The Result-Code shall be set to DIAMETER_SUCCESS and the WAG shall reply with the Policy Download Response message.

Exceptions to the cases specified here shall be treated by WAG as error situations, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY.

9.3.24 Routing Policy Cancellation Procedure

This procedure is used between the 3GPP AAA Server and the WAG. It is invoked by the 3GPP AAA Server when the session specific routing policy should be removed from the WAG (i.e. users tunnel has been disconnected and the tunnel specific routing policy configured at the WAG - the firewall "pinhole"- must be removed).

The Wg reference point performs the routing policy cancellation procedure based on the use of RFC 3588 [7] Abort-Session-Request / Answer (ASR/ASA) commands.

In the roaming case where the PDG is in the VPLMN, the 3GPP AAA Proxy shall perform the functions described below for the 3GPP AAA Server.

Table 9.3.24.1: Policy Cancellation - 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 Information	Destination-Host	M	The WAG name is obtained from the Origin-Host AVP of a previous message received from the WAG.

Table 9.3.24.2: Policy Cancellation- 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 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.

9.3.2.14.1 Detailed Behaviour

The 3GPP AAA Server shall make use of this procedure to instruct the WAG to remove a routing policy W-APN for a specific user. On receipt of the message, the WAG shall:

- Check that the user is known in the WAG. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.
- If the User is known, the WAG shall remove all routing policies configured for that session. The WAG shall further remove any stored user information pertaining to that W-APN.
- The WAG shall set the Result-Code to DIAMETER_SUCCESS and send back the ASA command to the 3GPP AAA Server.

Exceptions to the cases specified here shall be treated by the WAG as error situations, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY and no Wn flows shall be disabled.

9.3.35 WAG Initiated Routing Policy Cancellation Procedure

This procedure is used between the WAG and the 3GPP AAA Server. It is invoked by the WAG in the case whereby the session specific routing policy has been removed from the WAG and this action has not been preceded by any "Routing policy Cancellation Procedure" being sent from the 3GPP AAA Server to the WAG to instruct it to do so.

The trigger for removal of the routing policy is implementation dependent, but it may e.g. result from a security attack on the PLMN using a corrupted WLAN-UE - PDG tunnel.

The Wg reference point performs the routing policy cancellation procedure based on the use of RFC 3588 [7] Session Termination Request/ Answer (STR/STA) commands.

In the roaming case where the PDG is in the VPLMN, the 3GPP AAA Proxy shall perform the functions described below for the 3GPP AAA Server.

Table 9.3.35.1: WAG Initiated Policy Cancellation - Notification

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 Information	Destination-Host	M	This information element contains the 3GPP AAA Server/Proxy name obtained from previous messages.

Table 9.3.35.2: WAG Initiated Policy Cancellation- 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 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.

9.3.3.15.1 Detailed Behaviour

The WAG shall make use of this procedure to instruct the 3GPP AAA Server of the fact that it has removed routing policy firewall pinhole at a specific W-APN for a specific user. On receipt of the message, the 3GPP AAA Server shall:

- Check the user is known in the 3GPP AAA Server. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.
- If the User is known the 3GPP AAA Server behaviour is implementation dependent. The 3GPP AAA Server may:

  (i) try to reconfigure a routing policy at the WAG by initiating a new session using AA-R to the WAG; or

  (ii) take steps to remove the users session at the 3GPP AAA Server and the PDG.
- The 3GPP AAA Server shall set the Result-Code to DIAMETER_SUCCESS and send back the ASA command to the WAG.

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.

10 Information Elements Contents

10.1 AVPs

Table 10.1.1 describes the Diameter AVPs defined for the WLAN reference point, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted. The Vendor-Id header of all AVPs defined in this specification shall be set to 3GPP (10415).

Only those AVPs defined by 3GPP TS 29.234 [2] reference point are listed here.

Table 10.1.1: Diameter Multimedia Application AVPs

				AVP Flag rules				
Attribute Name	**AVP Code**	**Section defined**	**Value Type**	**Shall**	**May**	**Should not**	**Must not**	**May Encr.**
Authentication-Method	X	x.1.5	UTF8String	M, V				No
Authentication-Information-SIM	X	x.1.6	OctetString	M, V				No
Authorization -Information-SIM	X	x.1.7	OctetString	M,V				No
WLAN-User-Data	X	x.1.8	Grouped	M, V				No
WLAN-Access	X	x.1.11	Enumerated	M, V				No
WLAN-Tunnelling	X	x.1.12	Enumerated	M, V				No
APN-Authorized	X	x.1.14	Grouped	M, V				No
APN-Id	X	x.1.15	OctetString	M, V				No
APN-Authorization	X	x.1.16	Enumerated	M, V				No
Local-Access	X	x.1.17	Enumerated	M, V				No
EAP payload	X	x.1.20	OctetString	M, V				No
Auth Req Type	X	x.1.21	Enumerated	M,V				No
EAP-Master-Session-Key	X	x.1.22	OctetString	M, V				No
Session-Request-Type	X	x.1.23	Enumerated	M, V				No
Routing-Policy	X	x.1.24	OctetString	M, V				No
Max-Requested-Bandwidth	X	x.1.26	Enumerated	M, V				No
NOTE: The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see RFC 3588 [7].								

10.1.1 Auth-Session-State

Between the 3GPP AAA server and the HSS, Diameter sessions are implicitly terminated. An implicitly terminated session is one for which the server does not maintain state information. The client does not need to send any re-authorization or session termination requests to the server.

The Diameter base protocol includes the Auth-Session-State AVP as the mechanism for the implementation of implicitly terminated sessions.

The client (server) shall include in its requests (responses) the Auth-Session-State AVP set to the value NO_STATE_MAINTAINED (1), as described in RFC 3588 [7]. As a consequence, the server does not maintain any state information about this session and the client does not need to send any session termination request. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP shall be present in requests or responses.

10.1.2 User-Name

The User-Name AVP is defined in the RFC 3588 [7] and contains the user identity.

For the WLAN Wx reference point, the User-Name AVP contains the IMSI of the subscriber.

10.1.3 Visited-Network-Identifier

The Visited-Network-Identifier AVP is defined in 3GPP TS 29.229 [6] and indicates the 3GPP VPLMN where the user is roaming.

10.1.4 SIP-Auth-Data-Item

The SIP-Auth-Data-Item AVP is defined in 3GPP TS 29.229 [6]. However three new more conditional AVPs are needed for WLAN Wx reference point.

AVP format

```
SIP-Auth-Data-Item :: = < AVP Header : TBD >
    [ SIP-Item-Number ]
    [ SIP-Authentication-Scheme ]
    [ SIP-Authenticate ]
    [ SIP-Authorization ]
    [ SIP-Authentication-Context ]
    [Confidentiality-Key]
    [Integrity-Key]
    [Authentication-Method]
    [Authentication-Information-SIM]
    [Authorization-Information-SIM]
    * [AVP]
```

10.1.5 Authentication-Method

The Authentication-Method AVP (AVP code X) is of type UTF8String and indicates the authentication method required for the user. The following values are defined:

WLAN_EAP_SIM (0)

- The UE indicates to the HSS that the required authentication method is EAP/SIM.

WLAN_EAP_AKA (1)

- The UE indicates to the HSS that the required authentication method is EAP/AKA.

10.1.6 Authentication-Information-SIM

The Authentication-Information-SIM AVP (AVP code X) is of type OctetString and contains the concatenation of authentication challenge RAND and the ciphering key Kc.

10.1.7 Authorization -Information-SIM

The Authentication-Information-SIM AVP (AVP code X) is of type OctetString and contains the response SRES.

10.1.8 WLAN-User-Data

The WLAN-User-Data AVP (AVP code X) 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>
    [ MSISDN ]
    { WLAN-Access }
    { WLAN-Tunneling }
    [ Session-Timeout ]
    1* { Charging-Data  }
    *[ APN-Authorized ]
    { Local-Access }
    * [AVP]
```

10.1.9 MSISDN

The MSISDN AVP (AVP code 101) is defined in 3GPP TS 29.329 [21]. This identification could be used for example used for charging purposes.

Editor's Note: The optionality/presence could be modified by the SA1 and SA5 decision.

10.1.10 Charging-Information

The Charging-Mode AVP (AVP code 19) is of type is of type Grouped, and contains the addresses of the charging functions. It is defined in 3GPP TS 29.229 [6].

10.1.11 WLAN-Access

The WLAN-Access AVP (AVP code xx) is of type Enumerated, and allows operators to determine barring of 3GPP - WLAN interworking subscription. The following values are defined:

WLAN_SUBSCRIPTION_ALLOWED (0)

- The subscriber has WLAN subscription.

WLAN_SUBSCRIPTION_BARRED (1)

- The subscriber has no WLAN subscription.

10.1.12 WLAN-Tunnelling

The WLAN-Tunnelling AVP (AVP code xx) is of type Enumerated, and allows operator to disable all W-APNs at one time. If there is a conflict between this item and the "access allowed" flag of any W-APN, the most restrictive will prevail. The following values are defined:

WLAN_ APNS _ENABLE (0)

- Enable all APNs.

WLAN_ APNS _DISABLE (1)

- Disable all APNs.

10.1.13 Session-Timeout

The Session-TimeOut AVP (AVP code 27) is defined in RFC 3588 [7] and indicates the maximum period for a session measured in seconds.

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

10.1.14 APN-Authorized

The APN-Authorized AVP (AVP code xx) is of type Grouped and contains authorization information for the APNs. This AVP indicates the list of allowed APNs and the environment where the access is allowed (visited or home PLMN).

AVP format

```
APN-Authorized::= <AVP header: TBD>
    { APN-Id }
    { APN-Authorization }
    * [AVP]
```

10.1.15 APN-Id

The APN-Id AVP (AVP code xx) 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.

10.1.16 APN-Authorization

The APN-Authorization AVP (AVP code xx) is of type Enumerated, and contains a flag indicating whether access is allowed in visited PLMNs or in the home PLMN.

WLAN_ APN_HOME (0)

- Access is allowed in home PLMN only.

WLAN_ APN_VISITED (1)

- Access is allowed in visited PLMNs and home PLMN.

10.1.17 Local-Access

The Local-Access AVP (AVP code xx) is of type Enumerated, and indicate whether the user has direct access to external IP networks, e.g. Internet, from the WLAN Access Network or not.

WLAN_LOCAL_ACCESS (0)

- The user is allowed to access directly to external IP networks.

WLAN_NO_LOCAL_ACCESS (1)

- The user is not allowed to access directly to external IP networks.

10.1.18 Server-Assignment-Type

The Server-Assignment-Type AVP (AVP code 15) 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.

10.1.19 Deregistration-Reason

The Deregistration-Reason AVP (AVP code 16) is defined in 3GPP TS 29.229 [6] and indicates reason for a de-registration operation.

This grouped AVP contains a Reason-Code AVP to indicate the reason for the de-registration. Reasons are listed in 3GPP TS 29.229 [6]. Wx reference point defines as valid only PERMANENT_TERMINATION value.

10.1.20 EAP-Payload

The EAP-Payload AVP (AVP code xx) is defined in the draft-ietf-aaa-eap-08.txt [8] and contains the encapsulated EAP packet that is being exchanged between the EAP client and the home Diameter server.

10.1.21 Auth Req Type

The Auth Req Type AVP (AVP code xx) is of type Enumerated and indicates the action that the PDG is asking to the 3GPP AAA Server to perform (Authentication, authorization or both). Wm interface only makes use of the AUTHENTICATION_ONLY value. It is defined in the draft-ietf-aaa-eap-08.txt [8].

10.1.22 EAP-Master-Session-Key

The EAP-Master-Session-Key AVP (AVP code xx) is of type OctetString and contains keying material for protecting the communications between the user and the NAS. It is defined in the draft-ietf-aaa-eap-08.txt [8].

10.1.23 Session-Request-Type

The Session-Request-Type AVP (AVP code xx) is of type Enumerated and indicates the action that the PDG is asking to the 3GPP AAA Server to perform (authorization or routing policy). The following values are defined:

AUTHORIZATION REQUEST (0)

- The PDG is requesting authorization for a user for a given W-APN.

ROUTING POLICY (1)

- The PDG is indicating that routing policy information is present.

10.1.24 Routing-Policy

~~The Routing-Policy AVP (AVP code xx) is of type OctetString and indicates routing policies of the tunnel set-up.~~

~~Editor's Note: Its exact format is ffs.~~

The Routing Policy AVP (AVP code tbd) is of type IPFilterRule, and defines a packet filter for an IP flow with the following information:

- Direction (in or out).
- Source and destination IP address (possibly masked).
- Protocol.
- Source and destination port (list or ranges).

Where the protocol type shall be set to ESP (50).

The IPFilterRule type shall be used with the following restrictions:

- Only the Action "permit" shall be used.
- No "options" shall be used.

- The invert modifier "!" for addresses shall not be used.
- The keyword "assigned" shall not be used.
- For direction "out", an IPv4 destination IP address shall not be wildcarded. For direction "out", the 64 bits network prefix of an IPv6 destination IP address shall not be wildcarded.

The Flow description AVP shall be used to describe a single IP flow.

The direction "in" refers to uplink IP flows, and the direction "out" refers to downlink IP flows.

10.1.25 Subscription-ID

The Subscription-ID AVP (AVP code xx) is of type Enumerated and indicates the user identity to be used for charging purposes. It is defined in the IETF Diameter Credit-Control Application draft [19].

WLAN shall make use only of the value MSISDN.

10.1.26 Max-Requested-Bandwidth

The Max-Requested-Bandwidth AVP (AVP code xx) is of type OctetString and indicates the Max requested bandwidth. If present, shall be sent from the 3GPP AAA Server to the PDG.

~~10.1.27 Routing Policy~~

~~The Routing Policy AVP (AVP code tbd) is of type IPFilterRule, and defines a packet filter for an IP flow with the following information:~~

- ~~Direction (in or out).~~
- ~~Source and destination IP address (possibly masked).~~
- ~~Protocol.~~
- ~~Source and destination port (list or ranges).~~

~~Where the protocol type shall be set to ESP (50).~~

~~The IPFilterRule type shall be used with the following restrictions:~~

- ~~Only the Action "permit" shall be used.~~
- ~~No "options" shall be used.~~
- ~~The invert modifier "!" for addresses shall not be used.~~
- ~~The keyword "assigned" shall not be used.~~
- ~~For direction "out", an IPv4 destination IP address shall not be wildcarded. For direction "out", the 64 bits network prefix of an IPv6 destination IP address shall not be wildcarded.~~

~~The Flow description AVP shall be used to describe a single IP flow.~~

~~The direction "in" refers to uplink IP flows, and the direction "out" refers to downlink IP flows.~~

3GPP TSG-CN WG4 Meeting #25 ***N4-041592***

Seoul, Korea. November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **041382** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Clarification on the reauthorization and reauthentication procedures in Wa chapter
Source:	⌘	Nokia
Work item code:	⌘	WLAN
Date:	⌘	15.11.04
Category:	⌘	**D**
Release:	⌘	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:	⌘	Clarifies the reauthentication procedure on the Wa interface
Summary of change:	⌘	Clarifications in sections 4.1 & 4.3 on reauthentication
Consequences if not approved:	⌘	Unclear spec

Clauses affected:	⌘	4.1 & 4.3

	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 ****

4 Wa Description

The Wa reference point connects the WLAN AN, possibly via intermediate networks, to a 3GPP Network i.e. the 3GPP AAA Server when the WLAN AN in which the subscriber is currently located is directly connected to the home 3GPP network (also known as "the non-roaming case"), and the 3GPP AAA Proxy) when the WLAN AN is connected to the home 3GPP network through another 3GPP network (also known as "the roaming case"). The reference accommodates both legacy WLAN ANs of which use the RADIUS protocol, as well as future WLAN ANs which are expected to support Diameter.

4.1 Functionality

The functionality of the reference point is to transport:

- data for WLAN session authentication and reauthentication signalling between WLAN-UE and 3GPP Network;
- data for WLAN session authorization signalling between WLAN AN and 3GPP Network;
- keying data for the purpose of radio interface integrity protection and encryption;
- data for purging a user from the WLAN access for immediate service termination, when such functionality is supported by the WLAN AN;
- data to enable the identification of the operator networks within which roaming occurs;
- 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 RFC 2865 [17], including the following extensions:
   - RFC 2869 [9], which provides RADIUS extensions to support the transport of EAP frames over RADIUS.
   - IETF Draft "Attributes for Access Network Location and Ownership Information" [16], which provides RADIUS Extensions for Public WLAN [16] are also used in order to identify uniquely the owner and location of the WLAN.
   - 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 RFC 3588 [7], as well as IETF Draft " Diameter EAP Application", which [8] provides a Diameter application to support the transport of EAP (RFC 2284 [10] and IETF Draft "EAP" [11]) 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

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.

Editors Note: AVPs such as User Name defined on the Wa interface and VPLMN-ID defined on the Wd interface are parameters additional to those carried by the Diameter_EAP application. As defined below there parameters are defined as mandatory on the interface. It is an open point whether this implies that a new Diameter application is required, or whether these AVPs should be defined as conditional in order that the use of the Diameter_EAP application can be preserved.

Table 4.3.1.1: Authentication request

Information element name	Mapping to Diameter AVP	Cat.	Description
Username NAI	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 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.

The Diameter-EAP response message shall contain the following.

Table 4.3.1.2: Authentication response

Information element name	Mapping to Diameter AVP	Cat.	Description
Username NAI	User-Name	M	This information element contains the permanent identity of the user, i.e. the IMSI.
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.

<I think the specification is a little bit ambiguous whether the support of RFC3576 is mandaroty. My understanding of 4.3.1 bullet 1) was that it is mandatory, but according to this text it is optional. I think it would be better if it was mandatory. Have you decided not to mandate it due to the legacy WLAN ANs?>

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
Username NAI	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
Username NAI	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 [8]. 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.

What is the reason that these procedures are not in the Appendix as the others?

What about reauthenitcation? Is it totally the same as 4.3.1?

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 to be authenticated. More detailed description of the IE can be found in RFC 3580 [15] and 3GPP TS 23.234 [4].	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 RFC 3580 [15].	Mandatory	NA	NA	NA	NAS-IP Address
Operator Name	Hot Spot Operator Name as defined in [16].	Mandatory	NA	NA	NA	Operator Name
Location Name	Location Name of the hot spot operator as defined in [16].	Mandatory	NA	NA	NA	Location Name
Location Information	Location information regarding the hotspot operator as defined in [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 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
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 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 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 RFC 3580 [15].	NA	Optional	NA	Optional	Termination-Action
Cryption Key	This Attribute is available to allow vendors to support their own extended Attributes not suitable for general usage. More detailed description of the IE can be found in RFC 3580 [15].	NA	Mandatory	NA	NA	Vendor-Specific (MS-MPPE-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

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).

3GPP TSG-CN WG4 Meeting #25 ***N4-041593***

was N4-041411

Seoul, KOREA. 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **023** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	To replace 'Permanent User ID' by 'User Id'
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	03/11/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
- ***F*** *(correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(addition of feature),*
- ***C*** *(functional modification of feature)*
- ***D*** *(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

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 numerous places, the User ID to be specified in the Diameter message has been mentioned as the Permanent User ID. However, in many cases the permanant user id is not available to the corresponding always using Permanent User ID is against the User Identity Privacy.
Summary of change:	⌘	The 'Permenent User ID' needs to be replaced by User ID'
Consequences if not approved:	⌘	It will affect the User Identity Privacy of the User. The entities need to know 'Permanant User ID' which is not the case now.

Clauses affected:	⌘	4.3.1, 4.5.2.1, 5.4.1, 8.3.1, 8.4.1, 8.6, 8.5

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.

*** First modified section ***

4.3.1 WLAN Access Authentication and Authorization

This procedure is used to transport over RADIUS or Diameter, the WLAN Access 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.

Editors Note: AVPs such as User Name defined on the Wa interface and VPLMN-ID defined on the Wd interface are parameters additional to those carried by the Diameter_EAP application. As defined below there parameters are defined as mandatory on the interface. It is an open point whether this implies that a new Diameter application is required, or whether these AVPs should be defined as conditional in order that the use of the Diameter_EAP application can be preserved.

Table 4.3.1.1: Authentication request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity~~Username NAI~~	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 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~~Username NAI~~	User-Name	M	This information element contains the ~~permanent~~ identity of the user~~, i.e. the IMSI~~.
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~~Username NAI~~	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~~Username NAI~~	User-Name	M	This information element contains the identity of the user.
Result-Code	Result-Code	M	Informs of success of procedure

*** Next modified section ***

4.5.2.1 Procedures Description

4.5.2.1 Procedures Description

This procedure is used to transport over Diameter, the WLAN accounting specific information between the WLAN AN and the 3GPP AAA Proxy/Server.

Diameter usage in Wa:

- This procedure is mapped to the Diameter-Accounting Request and Accounting Response (ACR/ACA) command codes as defined in NASREQ [12]. The Diameter-ACR Message shall contain the following information elements.

Table 4.5.2.1: Accounting request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity~~Username NAI~~	User-Name	M	This information element contains the identity of the user.
NAS-IP address	NAS-IP Address	C	IPv4 address of the hot-spot
NAS-Ipv6 address	NAS-Ipv6 address	C	IPv6 address of the hot-spot
Accounting Record type	Accounting Record type	M	2= Start, 4= Stop, 3= Interim Record
Accounting Session-ID	Accounting Session-ID	M	Uniquely Identifies the accounting session. May be the same Session-ID as for the authentication signalling over the Wa
Accounting-Input-Octets	Accounting-Input-Octets	O	Number of octets sent by the WLAN UE
Accounting-Output-Octets	Accounting-Output-Octets	O	Number of octets received by the WLAN UE
Accounting-Input-Packets	Accounting-Input-Packets	O	Number of packets sent by the WLAN UE
Accounting-Output-Packets	Accounting-Output-Packets	O	Number of packets received by the WLAN UE
Accounting-Session-Time	Accounting-Session-Time	C	Indicates the length of the current session in seconds. Shall only be present if Accounting-Record-Type is set to Stop or Interim
Termination-Cause	Termination-Cause	C	Shall be present only if Accounting-Record-Type is set to Stop.

The Diameter-Accounting response message shall contain the following.

Table 4.5.2.2: Accounting response

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity~~Username NAI~~	User-Name	M	This information element contains the ~~permanent~~ identity of the user~~, i.e. the IMSI~~.
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.

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

5.4.1 WLAN Access Authentication and Authorization

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.

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.

Editors Note: AVPs such as User Name defined on the Wa interface and VPLMN-ID defined on the Wd interface are parameters additional to those carried by the Diameter_EAP application. As defined below there parameters are defined as mandatory on the interface. It is an open point whether this implies that a new Diameter application is required, or whether these AVPs should be defined as conditional in order that the use of the Diameter_EAP application can be preserved.

Table 5.4.1.1: Diameter EAP Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity~~Username NAI~~	User Name	M	This information element shall contain 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 or authentication procedure is requested. 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
Visited-Network-Identifier	Visited-Network-Identifier	M	Identifies the VPLMN

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~~Username NAI~~	User Name	M	This information element contains the ~~permanent~~ identity of the user~~, i.e. the IMSI~~.
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 Alive Time	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.
WLAN UE MAC address	Calling Station-ID	M	Carries the MAC address of the WLAN-UE.

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

8.3.1 Authentication Procedures

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
~~Permanent~~ User Identity	User-Name	M	This information element contains the ~~permanent~~ identity of the user~~, i.e. the IMSI~~.
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.

*** Next modified section ***

8.4.1 Authorization Procedures

8.4.1 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.

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

*** Table 8.4.1.1 Wm Authorization Request**

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the ~~permanent~~ identity of the user~~, i.e. the IMSI~~.
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.

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

8.5 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 8.5.1: Session Termination 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~~.
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 8.5.2: 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.

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

8.6 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 8.6.1: 3GPP AAA Server Initiated Tunnel Disconnection - 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~~.
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 8.6.2: 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.

***** End of document *****

3GPP TSG-CN WG4 Meeting #25 ***N4-041596***

was N4-041416

Seoul, KOREA. 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **028** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Editorial Changes
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	05/11/2004
Category:	⌘	**D**
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 is an essential change, since these can mis-guide the reader.
Summary of change:	⌘	1. WLAN expansion is Wireless Local Area Network instead of Wireless Local Access Network. 2. There is a reference to wrong document. This has been corrected. 3. There is a self reference. This has been deleted. 4. Scope mentions a reference point which has not been explained in this specification. This has been deleted
Consequences if not approved:	⌘	These mistakes will continue and can misguide readers.

Clauses affected:	⌘	1, 3.3, 4.3.3, 10.1

	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.

***** First modified section *****

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 Wp reference point between the 3GPP WAG and the PDG.~~
- The Wg reference point between the 3GPP AAA Server/Proxy and the WAG.

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

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
RADIUS	Remote Authentication Dial-In User Service
WAG	WLAN Access Gateway
WLAN AN	WLAN Access Network
WLAN	Wireless Local ~~Access~~Area Network
WLAN-UE	WLAN User Equipment

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

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~~8~~]. Information elements to be carried in the STR, STA messages are shown in tables 4.4.3.1 and 4.4.3.2.

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

10 Information Elements Contents

10.1 AVPs

Table 10.1.1 describes the Diameter AVPs defined for the WLAN reference point, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted. The Vendor-Id header of all AVPs defined in this specification shall be set to 3GPP (10415).

Only those AVPs ~~defined~~ which belong to the ~~by 3GPP TS 29.234 [2]~~ reference points mentioned within the scope of this specification are listed here.

***** End of document *****

3GPP TSG-CN WG4 Meeting #25 ***N4-041693***

Seoul, KOREA. 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.003** **CR** **092** ⌘ **rev** **2** ⌘ Current version: **6.4.0** ⌘

*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:	⌘	'otherrealm' format of Decorated NAI
Source:	⌘	CN4
Work item code:	⌘	7.1
Date:	⌘	21/10/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:

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 'otherrealm' of Decorated NAI shall be in the same format than 'Homerealm' but with the PLMN ID (visitedMCC and visitedMNC) of the selected PLMN.
Summary of change:	⌘	The 'otherrealm' format is changed to wlan.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org
Consequences if not approved:	⌘	The 'otherrealm' can't be resolved and the format is not aligned with domain name assigned by GSMA for PLMN identity defined for WLAN-I.

Clauses affected:	⌘				
		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.

14.4 Decorated NAI

The Decorated NAI shall take the form of a NAI and shall have the form 'homerealm!username@otherrealm' as specified in clause 3 of the IETF draft 2486-bis [53].

The realm part of Decorated NAI consists of 'otherrealm', see the IETF draft 2486-bis [53]. 'Homerealm' is the realm as specified in clause 14.2, using the HPLMN ID ('homeMCC' + 'homeMNC)'. 'Otherrealm' is the realm built using the PLMN ID (visitedMCC + visited MNC) of the PLMN selected as a result of WLAN PLMN selection (see 3GPP TS 24.234 [48]).

The username part format of the Root NAI shall comply with draft-arkko-pppext-eap-aka [50] when EAP AKA authentication is used and with draft-haverinen-pppext-eap-sim [51], when EAP SIM authentication is used.

When the username part of Decorated NAI includes the IMSI, it shall be built following the same steps specified for Root NAI in clause 14.3.

The result will be a decorated NAI of the form:

"wlan.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org
!0<IMSI>@wlan.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org", for EAP AKA authentication and "
wlan.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org
!1<IMSI>@wlan.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org ", for EAP SIM authentication

For example, for EAP AKA authentication: If the IMSI is 234150999999999 (MCC = 234, MNC = 15) and the PLMN ID of the Selected PLMN is MCC = 610, MNC = 71 then the Decorated NAI takes the form wlan.mnc015.mcc234.3gppnetwork.org!0234150999999999@wlan.mnc071.mcc610.3gppnetwork.org.

NOTE: the 'otherrealm' specified in the present document is resolved by the WLAN AN. If the WLAN AN does not have access to the GRX, then the WLAN AN should resolve the realm by other means e.g. static look-up table, private local DNS server acting as an authoritative name server for that sub-domain.

3GPP TSG-CN1 Meeting #36
Seoul, Korea, 15-19 November 2004

Tdoc N4-041694
revision of N4-041661

CR-Form-v7.1

CHANGE REQUEST

29.234 **CR** **001** ⌘ **rev** **2** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	PLMN advertising and selection
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	19/11/2004
Category:	⌘	**D**
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:	⌘	Necessity to obtain the list of available PLMNs to enable network selection.
Summary of change:	⌘	In the reference section and in section 4.2 the references to IETF RFCs has been revised in order to refer to the most updated documents. In section 4.4 the username Information Element field has been updated to point to the TS 23.003. In section A.1 a clarification to operation made by the 3GPP AAA Proxy/Server is made.
Consequences if not approved:	⌘	The PLMN selection procedure not corretly implemented.

Clauses affected:	⌘	Reference, 4.2, 4.4 , A.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.

First Changes

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~~6~~.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, "Attributes for Access Network Location and Ownership Information"., 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".

End of 1st Changes

2nd Changes

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 RFC 2865 [17], including the following extensions:

   - RFC 3579~~2869~~ [14~~9~~], which provides RADIUS extensions to support the transport of EAP frames over RADIUS.
   - IETF Draft "Attributes for Access Network Location and Ownership Information" [16], which provides RADIUS Extensions for Public WLAN [16] are also used in order to identify uniquely the owner and location of the WLAN.
   - 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 RFC 3588 [7], as well as IETF Draft " Diameter ~~EAP~~ Extensible Authentication Protocol (EAP) Application"[8], which ~~[8]~~ provides a Diameter application to support the transport of EAP (RFC ~~2284~~ 3748 [~~10~~21]~~ and IETF Draft "EAP" [11]~~) 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

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 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.

Editors Note: AVPs such as User Name defined on the Wa interface and VPLMN-ID defined on the Wd interface are parameters additional to those carried by the Diameter_EAP application. As defined below there parameters are defined as mandatory on the interface. It is an open point whether this implies that a new Diameter application is required, or whether these AVPs should be defined as conditional in order that the use of the Diameter_EAP application can be preserved.

Table 4.3.1.1: Authentication request

Information element name	Mapping to Diameter AVP	Cat.	Description
Username NAI	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 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.

The Diameter-EAP response message shall contain the following.

Table 4.3.1.2: Authentication response

Information element name	Mapping to Diameter AVP	Cat.	Description
Username NAI	User-Name	M	This information element contains the permanent identity of the user, i.e. the IMSI.
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.

End of 2nd Changes

3th Changes

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 [22] ~~to be authenticated. More detailed description of the IE can be found in RFC 3580 [15] and 3GPP TS 23.234 [4].~~	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 RFC 3580 [15].	Mandatory	NA	NA	NA	NAS-IP Address
Operator Name	Hot Spot Operator Name as defined in [16].	Mandatory	NA	NA	NA	Operator Name
Location Name	Location Name of the hot spot operator as defined in [16].	Mandatory	NA	NA	NA	Location Name
Location Information	Location information regarding the hotspot operator as defined in [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 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
Session Alive Time	This Attribute sets the maximum number of seconds of service to be	NA	Optional	NA	Optional	Session-Time-Out

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
	provided to the user before termination of the session or prompt. A more detailed description of the IE can be found in 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 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 RFC 3580 [15].	NA	Optional	NA	Optional	Termination-Action
Cryption Key	This Attribute is available to allow vendors to support their own extended Attributes not suitable for general usage. More detailed description of the IE can be found in RFC 3580 [15].	NA	Mandatory	NA	NA	Vendor-Specific (MS-MPPE-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

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 3rd Changes

4th Changes

A.1 Authentication, Authorization and Key Delivery

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

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

The signalling sequences shown are based on RADIUS and Diameter, as specified in clauses 4 and 5. For more information on proxying and protocol translation associated with using RADIUS and Diameter between the Wa and Wd reference points see subclause 5.3.

The 3GPP AAA Proxy/Server manipulates the Root/Decorated/Alternative NAI as defined in 3GPP TS 23.003 [22].

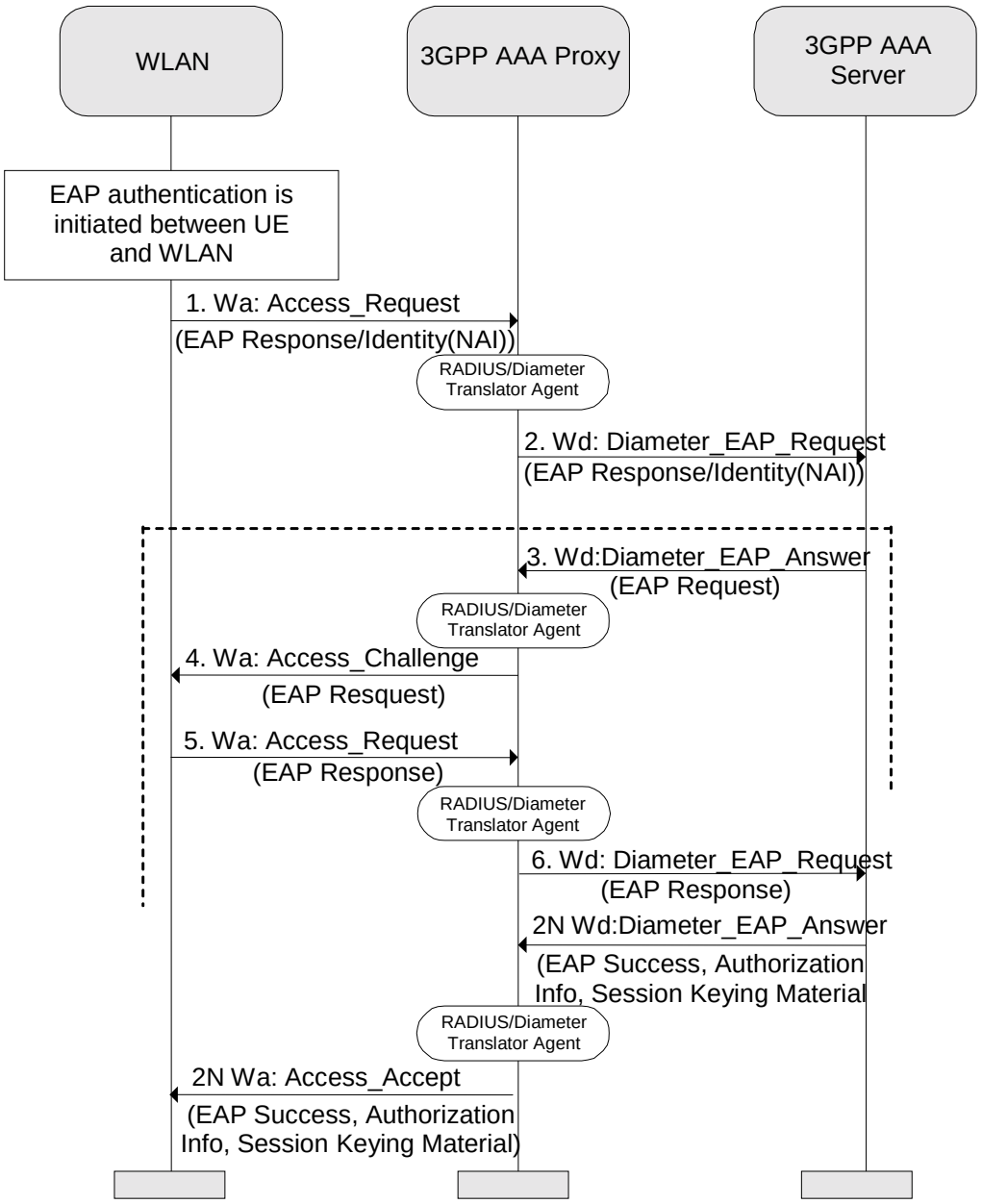


Figure A.1: Wa and Wd message flow for WLAN Session Authentication and Authorization Case a) Wa using RADIUS and Wd using Diameter

End of 4th Changes

3GPP TSG CN WG4 Meeting #25 **N4-041695**
Seoul, KOREA, 15th – 19th November 2004

CR-Form-v7

CHANGE REQUEST

⌘ **29.234** **CR** **012** ⌘ **rev** **2** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Wd Interface RADIUS profile clarifications
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	19/11/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

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

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

Reason for change:	⌘	To add Charging and Location information RADIUS attributes to Wa/Wd interfaces with proper references to IETF Drafts. Also a missing VPLMN identity attribute needs to be added to Wa/Wd RADIUS profiles.
Summary of change:	⌘	This contribution updates Location Information and Chargebale User Identity references to IETF Drafts and adds a reference to required VPLMN identity GSMA PRD IR.61 defined Vendor Specific Attribute. This contribution also clarifies the general RADIUS profile for the Wd interface. This addition concerns only RADIUS based Wa/Wd interfaces.
Consequences if not approved:	⌘	Inproper references to IETF Drafts and a missing VPLMN identity attribute in Wa/Wd RADIUS profile.

Clauses affected:	⌘	2, 4.2, 4.4.1, 4.5.1.1, 5.2

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-06.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~~Attributes for Access Network Location and Ownership Information~~"~~.~~, 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".

[xx] GSMA PRD IR.61, “WLAN Roaming Guidelines”

[yy] IETF Draft, “Chargeable User Identity”, draft-adrangi-radius-chargeable-user-identity-02.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 2869 [9], which provides RADIUS extensions to support the transport of EAP frames over RADIUS.

   - IETF Draft "Carrying Location Objects in RADIUS~~Attributes for Access Network Location and Ownership Information~~", draft-ietf-geopriv-radius-lo-01 [16], which provides RADIUS Extensions for Public WLAN ~~[16]~~ 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], as well as IETF Draft " Diameter EAP Application", which IETF Draf draft-ietf-aaa-eap-06 [8] provides a Diameter application to support the transport of EAP (IETF RFC 2284 [10] and IETF Draft "EAP" [11]) 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

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

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

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 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
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~~Type	Location ~~Name~~ Type of the hot spot operator as defined in IETF Draft draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	NA	NA	Location-~~Name~~Type
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
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	NA	Optional	NA	Optional	Session-Time-Out

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
	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
Cryption Key	This Attribute is available to allow vendors to support their own extended Attributes not suitable for general usage. More detailed description of the IE can be found in IETF RFC 3580 [15].	NA	Mandatory	NA	NA	Vendor-Specific (MS-MPPE-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 [yy].	Optional	Mandatory	NA	NA	Chargeable-User-Id
Visited Operator Identity	Identifies the VPLMN as specified in GSMA PRD IR.61 [xx]	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 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 ****

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 IETF Draft draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	Operator-Name
Location ~~Name~~Type	Location Name of the hot spot operator as defined in IETF Draft draft-ietf-geopriv-radius-lo-01 -[16].	Mandatory	NA	Location-~~Name~~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

IE NAME	IE description	Accounting Request	Accounting Response	Attribute
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
Chargeable User Identity	This Attribute shall contain the MSISDN of the user as specified in IETF Draft draft-adrangi-radius-chargeable-user-identity-02 [yy].	Mandatory	NA	Chargeable-User-Id
Visited Operator Identity	Identifies the VPLMN as specified in GSMA PRD IR.61 [xx]	Mandatory	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 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 #4 ****

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

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~~Attributes for Access Network Location and Ownership Information~~" 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.

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

3GPP TSG CN WG4 Meeting #25 **N4-041696**
Seoul, KOREA, 15th – 19th November 2004

CR-Form-v7

CHANGE REQUEST

⌘ **29.234** **CR** **014** ⌘ **rev** **2** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	RADIUS Profile for Wa and Wd
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	19/11/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:

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

Reason for change:	⌘	Currently 29.234 lacks a proper RADIUS profile for Wa and Wd interfaces
Summary of change:	⌘	This CR add a RADIUS profile for Wd interface and updates the RADIUS profile for Wa. The RADIUS profile is based on the IR.61 RADIUS profile for EAP-SIM based WLAN roaming.
Consequences if not approved:	⌘	There won't be properly defined RADIUS profile for Wa and Wd interfaces.

Clauses affected:	⌘	2, 4.5.1.1, 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-06.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 ~~Attributes for Access Network Location and Ownership Information~~"., 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".

[xx] GSMA PRD IR.61, “WLAN Roaming Guidelines”.

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

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

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

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 IETF draft-ietf-geopriv-radius-lo-01.txt [16].	Mandatory	NA	Operator Name
Location ~~Name~~TYPE	Location Name of the hot spot operator as defined in IETF draft-ietf-geopriv-radius-lo-01.txt [16].	Mandatory	NA	Location-Type ~~Name~~
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-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.	Conditional. Shall	N/A	Acc-Terminate-

IE NAME	IE description	Accounting Request	Accounting Response	Attribute
	Cause values are as per specified in IETF RFC 3580 [15].	be present if Acct-Status-Type set to "Accounting Stop".		Cause
Event Time Stamp	Number of second elapsed since January 1st 1970. UTC time.	Mandatory	NA	Event-Time-Stamp

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 ******

5.5 Information Elements Contents

5.5.1 RADIUS based Information Elements Contents for Authentication and Authorization

Table 5.5.1: 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
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
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
Cryption Key	This Attribute is available to allow vendors to support their own extended Attributes not suitable for general usage. More detailed description of the IE can be found in IETF RFC 3580 [15].	NA	Mandatory	NA	NA	Vendor-Specific (MS-MPPE-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 [yy].	Optional	Mandatory	NA	NA	Chargeable-User-Id
Visited Operator Identity	Identifies the VPLMN as specified in GSMA PRD IR.61 [xx]	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 #3 ****

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

5.5.2 RADIUS based Information Elements Contents for Accounting

Table 5.5.2: 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 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.	Conditional. Shall	N/A	Acc-Terminate-

IE NAME	IE description	Accounting Request	Accounting Response	Attribute
	Cause values are as per specified in IETF RFC 3580 [15].	be present if Acct-Status-Type set to "Accounting Stop".		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 the user as specified in IETF Draft draft-adrangi-radius-chargeable-user-identity-02 [yy].	Mandatory	NA	Chargeable-User-Id
Visited Operator Identity	Identifies the VPLMN as specified in GSMA PRD IR.61 [xx]	Mandatory	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 #4 ****

3GPP TSG-CN WG4 Meeting #25

N4-041697

was N4-041595

was N4-041413

Seoul, KOREA. 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **025** ⌘ **rev** **2** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	To make VPLMN-Id Conditional in Wd interface
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	05/11/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:
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 is regarding Wd interface Authentication Request message. After the first diameter message, in a diameter session, all subsequent messages follow the same route, making the VPLMN id mandatory redundant.
Summary of change:	⌘	To make the VPLMN id "Conditional" in Diameter EAP Request in Wd interdace.
Consequences if not approved:	⌘	There will be redundancy in the message. Also it might not allign to the Diameter EAP application.

Clauses affected:	⌘	4.3.1, 5.4.1			
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.

*** First modified section ***

4.3.1 WLAN Access Authentication and Authorization

This procedure is used to transport over RADIUS or Diameter, the WLAN Access 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.

Editors Note: AVPs such as User Name defined on the Wa interface and ~~VPLMN-ID defined on the Wd interface~~ are parameters additional to those carried by the Diameter_EAP application. As defined below there parameters are defined as mandatory on the interface. It is an open point whether this implies that a new Diameter application is required, or whether these AVPs should be defined as conditional in order that the use of the Diameter_EAP application can be preserved.

Table 4.3.1.1: Authentication request

Information element name	Mapping to Diameter AVP	Cat.	Description
Username NAI	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 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.

*** Next modified section ***

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.

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.

Editors Note: AVPs such as User Name defined on the Wa interface ~~and VPLMN-ID defined on the Wd interface~~ are parameters additional to those carried by the Diameter_EAP application. As defined below there parameters are defined as mandatory on the interface. It is an open point whether this implies that a new Diameter application is required, or whether these AVPs should be defined as conditional in order that the use of the Diameter_EAP application can be preserved.

Table 5.4.1.1: Diameter EAP Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Username NAI	User Name	M	This information element shall contain 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 or authentication procedure is requested. 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
Visited-Network-Identifier	Visited-Network-Identifier	C~~M~~	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.

***** End of document *****