3GPP TSG CN Plenary Meeting #27 **NP-050047**
9th – 11th March 2005 Tokyo, JAPAN.

Source: TSG CN WG4

Title: Corrections on WLAN

Agenda item: 9.17

Document for: APPROVAL

Doc-2nd-Level	Spec	CR	Rev	Phase	Subject	Cat	Ver_C
N4-050123	29.234	31		Rel-6	Removal of Wn reference point Definition from the Stage 3	F	6.1.0
N4-050124	29.234	32		Rel-6	Wa Interface RADIUS profile corrections	F	6.1.0
N4-050125	29.234	33		Rel-6	Wd Interface RADIUS profile corrections	F	6.1.0
N4-050127	29.234	35		Rel-6	Information Element corrections on Wd	F	6.1.0
N4-050166	29.234	43		Rel-6	Editorial corrections	F	6.1.0
N4-050279	29.230	40	1	Rel-6	WLAN Diameter AVP and result codes	F	6.2.0
N4-050339	23.003	93	3	Rel-6	CR on WLAN Alternative NAI	B	6.5.0
N4-050345	29.234	30	1	Rel-6	Removal of material duplicating 23.234 in 29.234	F	6.1.0
N4-050347	29.234	34	1	Rel-6	Removal of unnecessary attributes on Wa	F	6.1.0
N4-050349	29.234	37	1	Rel-6	Editorial corrections	F	6.1.0
N4-050351	29.234	38	1	Rel-6	Description of the RADIUS session termination procedure	F	6.1.0
N4-050352	29.234	39	1	Rel-6	WLAN Diameter AVP and result codes	F	6.1.0
N4-050353	29.234	41	1	Rel-6	WLAN Diameter AVP table and chapters coherence revision	F	6.1.0
N4-050354	29.234	42	2	Rel-6	PDG behaviour on Wm interface	F	6.1.0
N4-050357	29.234	47	1	Rel-6	Wa Interface RADIUS profile Information Element corrections	F	6.1.0

3GPP TSG-CN WG4 Meeting #26 **N4-050123**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **31** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

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

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

Title:	⌘	Removal of Wn reference point Definition from the Stage 3
Source:	⌘	Lucent Technologies
Work item code:	⌘	WLAN
Date:	⌘	31/01/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:

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

Reason for change:	⌘	The Wn reference point is currently included in the scope of 29.234, and clause 7 purports to be a description of this reference point. However, the text in clause 7 merely indicates that the protocol for the interface at this reference point is implementation dependent, and contains no additional information over and above that already specified in 23.234.
Summary of change:	⌘	The Wn reference point is removed from the scope, and all material in the document relating to the Wn reference point deleted.
Consequences if not approved:	⌘	Retention of duplicate material to that specified in 23.234, with possible deviation of that material in the future.
Clauses affected:	⌘	1, 7

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

Other comments: ⌘

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

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

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

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

1 Scope

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

The present document is applicable to:

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

7 ~~Wn Description~~Void

~~Wn interface is a user plane interface whose purpose is to route packets to/from the WLAN AN via the WAG into the PLMN for WLAN 3GPP IP access functionality.~~

~~Several methods exist for implementing this functionality, some examples are presented in annex C of 3GPP TS 23.234 [4]. The specific method to implement this interface is subject to local agreement between the WLAN AN and the PLMN and it is out of the scope of 3GPP specifications.~~

3GPP TSG CN WG4 Meeting #26 **N4-050124**
Sydney, AUSTRALIA, 14th – 18th February 2005

CR-Form-v7

CHANGE REQUEST

⌘ **29.234** **CR** **032** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

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

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

Title:	⌘	Wa Interface RADIUS profile corrections
Source:	⌘	CN4
Work item code:	⌘	WLAN-IW
Date:	⌘	04/02/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

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

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

Reason for change:	⌘	Correction of incorrect RADIUS attributes in Wa
Summary of change:	⌘	This contribution corrects the RADIUS Wa profile to be compliant with the requirements of the 33.234-6.3.0. The correction concerns only the MS-MPP-Send-key attribute in the RADIUS Wa interface.
Consequences if not approved:	⌘	The 29.234 is not compliant with the 33.234 requirements for RADIUS Wa.

Clauses affected:	⌘	2, 4.4.1			
Other specs affected:	⌘	Y	N		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

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

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

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

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

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

2 References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.4.1 RADIUS based Information Elements Contents

Table 4.4.1: RADIUS based Information Elements Contents

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

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

The parameters listed above as 'mandatory' are only optional in the particular RADIUS (extension) specification in which they are originally defined. However, in order for 3GPP WLAN-IW to function, these attributes shall be passed in messaging over the 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 ****

3GPP TSG CN WG4 Meeting #26 **N4-050125**
Sydney, AUSTRALIA, 14th – 18th February 2005

CR-Form-v7

CHANGE REQUEST

⌘ **29.234** **CR** **033** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

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

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

Title:	⌘	Wd Interface RADIUS profile corrections
Source:	⌘	CN4
Work item code:	⌘	WLAN-IW
Date:	⌘	04/02/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

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

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

Reason for change:	⌘	Correction of incorrect RADIUS attributes in Wd
Summary of change:	⌘	This contribution corrects the RADIUS Wd profile to be compliant with the requirements of the 33.234-6.3.0. Also the WLAN 3GPP IP Access requires both MS-MPP-Send-Key and MS-MPP-Recv-Key in order to provide enough key seed to authenticate the IKEv2 key exchange. The correction concerns only the MS-MPP-Send-key and MS-MPP-Recv-Key attributes in the RADIUS Wd interface.
Consequences if not approved:	⌘	The 29.234 is not compliant with the 33.234 requirements and cannot provide key seed for authenticating the IKEv2 key exchange.

Clauses affected:	⌘	2, 5.5.4

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

⌘

Other comments: ⌘

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

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

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

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

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

2 References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.5.4 RADIUS based Information Elements Contents for Authentication and Authorization

Table 5.5.4.1: RADIUS based Information Elements Contents

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
RADIUS Client Address	This Attribute indicates the identifying IP Address of the RADIUS Client. It should be unique to the RADIUS Client within the scope of the RADIUS server. More detailed description of the IE can be found in IETF RFC 3580 [15].	Mandatory	NA	NA	NA	NAS-IP Address
USER ID	This Attribute indicates the identity of the user to be authenticated. More detailed description of the IE can be found in IETF RFC 3580 [15] and 3GPP TS 23.234 [4].	Mandatory	Mandatory	Mandatory	Mandatory	User-Name
Operator Name	Hot Spot Operator Name as defined in IETF draft-ietf-geopriv-radius-lo-01.txt [16].	Mandatory	NA	NA	NA	Operator-Name
Location Type	Location Name of the hot spot operator as defined in IETF draft-ietf-geopriv-radius-lo-01.txt [16].	Mandatory	NA	NA	NA	Location-Type
Location Information	Location information regarding the hotspot operator as defined in IETF draft-ietf-geopriv-radius-lo-01.txt [16].	Mandatory	NA	NA	NA	Location-information
EAP Message	This attribute encapsulates Extensible Authentication Protocol packets so as to allow the NAS to authenticate users via EAP without having to understand the EAP protocol. More detailed description of the IE can be found in IETF RFC 3580 [15].	Mandatory	Mandatory	Mandatory	Mandatory	EAP-Message
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 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~~ Pairwise Master Key (PMK)	This IE is used to carry the Pairwise Master 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]~~ Draft draft-haverinen-pppext-eap-sim-16 [xx] and IETF Draft draft-arkko-pppext-eap-aka-15 [yy].	NA	Mandatory	NA	NA	Vendor-Specific (MS-MPPE-Recv~~Send~~-Key)
Master Session Key (MSK)	This IE is used to carry the Master Session Key for WLAN 3GPP IP Access. More detailed description of the IE can be found in IETF Draft draft-haverinen-pppext-eap-sim-16 [xx] and IETF Draft draft-arkko-pppext-eap-aka-15 [yy].	NA	Mandatory	NA	NA	Vendor-Specific (MS-MPP-Recv-Key) and Vendor-Specific (MS-MPP-Send-Key)
Message Authenticator	Message Authenticator.	Mandatory	Mandatory	Mandatory	Mandatory	Message-Authenticator
WLAN-UE MAC address	Carries the MAC address of the WLAN-UE for verification at the 3GPP AAA Server.	Mandatory	NA	NA	NA	Calling-Station-ID
Chargeable User Identity	This Attribute shall contain the MSISDN of the user as specified in IETF Draft draft-adrangi-radius-chargeable-user-identity-02 [26].	Optional	Mandatory	NA	NA	Chargeable-User-Id
Visited Operator Identity	Identifies the VPLMN as specified in GSMA PRD IR.61 [25]	Mandatory	NA	NA	NA	Vendor-Specific (Visited-Operator-Id)

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

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

3GPP TSG CN WG4 Meeting #26 **N4-050127**
Sydney, AUSTRALIA, 14th – 18th February 2005

CR-Form-v7

CHANGE REQUEST

⌘ **29.234** **CR** **035** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

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

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

Title:	⌘	Information Element corrections on Wd
Source:	⌘	CN4
Work item code:	⌘	WLAN-IW
Date:	⌘	04/02/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

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

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

Reason for change:	⌘	Correction of incorrect and removal of unnecessary Information Element descriptions on the RADIUS Wd profile
Summary of change:	⌘	This contribution corrects and removes Information Element descriptions on the RADIUS Wd profile related to Class and State attributes.
Consequences if not approved:	⌘	Unclear and possibly misleading descriptions on RADIUS Wd profile's Information Element descriptions.

Clauses affected:	⌘	5.5.4, 5.5.5

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

Other comments:	⌘	

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

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

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

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

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

5.5.4 RADIUS based Information Elements Contents for Authentication and Authorization

Table 5.5.4.1: RADIUS based Information Elements Contents

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
RADIUS Client Address	This Attribute indicates the identifying IP Address of the RADIUS Client. It should be unique to the RADIUS Client within the scope of the RADIUS server. More detailed description of the IE can be found in IETF RFC 3580 [15].	Mandatory	NA	NA	NA	NAS-IP Address
USER ID	This Attribute indicates the identity of the user to be authenticated. More detailed description of the IE can be found in IETF RFC 3580 [15] and 3GPP TS 23.234 [4].	Mandatory	Mandatory	Mandatory	Mandatory	User-Name
Operator Name	Hot Spot Operator Name as defined in IETF draft-ietf-geopriv-radius-lo-01.txt [16].	Mandatory	NA	NA	NA	Operator-Name
Location Type	Location Name of the hot spot operator as defined in IETF draft-ietf-geopriv-radius-lo-01.txt [16].	Mandatory	NA	NA	NA	Location-Type
Location Information	Location information regarding the hotspot operator as defined in IETF draft-ietf-geopriv-radius-lo-01.txt [16].	Mandatory	NA	NA	NA	Location-information
EAP Message	This attribute encapsulates Extensible Authentication Protocol packets so as to allow the NAS to authenticate users via EAP without having to understand the EAP protocol. More detailed description of the IE can be found in IETF RFC 3580 [15].	Mandatory	Mandatory	Mandatory	Mandatory	EAP-Message
~~Diameter Session ID + 3GPP AAA Server Host AVP + prefix "Diameter"~~State information	This attribute ~~is~~may be ~~relayed~~ sent ~~from~~ by the 3GPP AAA server to the WLAN-AN~~3GPP AAA Proxy to the WLAN-AN when the 3GPP AAA Proxy acts as translation agent~~. If the RADIUS client in the WLAN-AN receives such an attribute, it ~~MUST~~ shall be included ~~it~~ in subsequent Access Requests.	Conditional	NA	NA	~~Conditional~~Optional	State
~~Diameter Session ID + prefix "Diameter"~~Session ID	This attribute is sent by 3GPP AAA ~~Proxy~~ server to the visited network~~when acting as a translation agent~~. If the RADIUS client in the WLAN-An receives it, ~~is~~ it should be included ~~it~~ in subsequent accounting	NA	~~Conditional~~ Mandatory	NA	NA	Class

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
	messages.					
Session Alive Time	This Attribute sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt. A more detailed description of the IE can be found in IETF RFC 3580 [15].	NA	Optional	NA	Optional	Session-Time-Out
Charging Duration	This attribute indicates the time between each interim update in seconds for this specific session. A more detailed description of the IE can be found in IETF RFC 2869 [9].	NA	Optional	NA	NA	Acct-Interim-Interval
Termination Action	This Attribute indicates what action the NAS should take when the specified service is completed. More detailed description of the IE can be found in IETF RFC 3580 [15].	NA	Optional	NA	Optional	Termination-Action
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 [26].	Optional	Mandatory	NA	NA	Chargeable-User-Id
Visited Operator Identity	Identifies the VPLMN as specified in GSMA PRD IR.61 [25]	Mandatory	NA	NA	NA	Vendor-Specific (Visited-Operator-Id)

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

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

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

5.5.5 RADIUS based Information Elements Contents for Accounting

Table 5.5.5.1: RADIUS based Information Elements Contents

IE NAME	IE description	Accounting Request	Accounting Response	Attribute
USER ID	This Attribute indicates the identity of the user. More detailed description of the IE can be found in IETF RFC 3580 [15] and 3GPP TS 23.234 [4].	Mandatory	Mandatory	User-Name
RADIUS Client Address	This Attribute indicates the identifying IP Address of the RADIUS Client. It should be unique to the RADIUS Client within the scope of the RADIUS server. More detailed description of the IE can be found in IETF RFC 3580 [15].	Mandatory	NA	NAS-IP Address
Acc-Session-ID	According to IETF RFC 2866 [20], this attribute is an accounting ID which uniquely identifies the user's session. ~~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. Cause values are as per specified in IETF RFC 3580 [15].	Conditional. Shall be present if Acct-Status-Type set to "Accounting Stop".	N/A	Acc-Terminate-Cause
Event Time Stamp	Number of second elapsed since January 1st 1970. UTC time.	Mandatory	NA	Event-Time-Stamp

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

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

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

3GPP TSG-CN WG4 Meeting #26 **N4-050166**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **43** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

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

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

Title:	⌘	Editorial corrections
Source:	⌘	CN4
Work item code:	⌘	WLAN-IW
Date:	⌘	29/01/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:

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

Reason for change:	⌘	In the clause 4.4.2.2, according to the context, it should describe the AVPs of ASR/ASA. But the title is the STR/STS', and the STR/STA AVPs have been described in the clause 4.4.2.3.
Summary of change:	⌘	Correct the title and corresponding contents of the clause 4.4.2.2.
Consequences if not approved:	⌘	It is not coincidental between the title and the contents and will confuse implementing.

Clauses affected:	⌘	4.4.2.2

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

Other comments: ⌘

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

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

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

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

********the part of change**********

4.4.2.2 Abort Session ~~Termination~~ Request and Answer AVPs

ABNF for the ~~STR~~ ASR and ~~STA~~ ASA commands are as follows:

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

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

********the part of change**********

3GPP TSG-CN WG4 Meeting #26 **N4-050279**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.230** **CR** **040** ⌘ **rev** **1** ⌘ Current version: **6.2.0** ⌘

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

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

Title:	⌘	WLAN Diameter AVP and result codes
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	09/02/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:

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

Reason for change:	⌘	Complete the TS with the AVP and result codes from TS 29.234.
Summary of change:	⌘	Table 7.1 updated with the WLAN AVP codes. Also a reference to the WLAN 3GPP TS 29.234 TS has been added in those grouped Cx AVPs that WLAN modifies slightly the ABNF: • SIP-Auth-Data-Item AVP for WLAN adds three new optional sub-AVPs to the ABNF described in TS 29.229 Table 8.1.4 updated with new result codes
Consequences if not approved:	⌘	TS will not be complete and misinterpretation of the Grouped AVPs.

Clauses affected:	⌘	7.1, 8.1.4

Other specs affected: ⌘	Y	N		⌘
	X		Other core specifications	29.234-39
		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 <<<<<<<<<<<

7.1 3GPP specific AVP codes

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

Table 7.1: 3GPP specific AVP codes

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

601	Public-Identity	UTF8String	
602	Server-Name	UTF8String	
603	Server-Capabilities	Grouped	
604	Mandatory-Capability	Unsigned32	
605	Optional-Capability	Unsigned32	
606	User-Data	OctetString	
607	SIP-Number-Auth-Items	Unsigned32	
608	SIP-Authentication-Scheme	UTF8String	
609	SIP-Authenticate	OctetString	
610	SIP-Authorization	OctetString	
611	SIP-Authentication-Context	OctetString	
612	SIP-Auth-Data-Item	Grouped	29.229 [2], 29.234 [6]
613	SIP-Item-Number	Unsigned32	
614	Server-Assignment-Type	Enumerated	
615	Deregistration-Reason	Grouped	
616	Reason-Code	Enumerated	
617	Reason-Info	UTF8String	
618	Charging-Information	Grouped	
619	Primary-Event-Charging-Function-Name	DiameterURI	
620	Secondary-Event-Charging-Function-Name	DiameterURI	
621	Primary-Charging-Collection-Function-Name	DiameterURI	
622	Secondary-Charging-Collection-Function-Name	DiameterURI	29.229 [2]
623	User-Authorization-Type	Enumerated	
624	User-Data-Already-Available	Enumerated	
625	Confidentiality-Key	OctetString	
626	Integrity-Key	OctetString	
627	User-Data-Request-Type	Enumerated	
628	Supported-Features	Grouped	
629	Feature-List-ID	Unsigned32	
630	Feature-List	Unsigned32	
631	Supported-Applications	Grouped	
Note: The AVP codes from 632 to 699 are reserved for TS 29.229.			
700	User-Identity	Grouped	
701	MSISDN	OctetString	
702	User-Data	OctetString	
703	Data-Reference	Enumerated	
704	Service-Indication	OctetString	29.329 [4]
705	Subs-Req-Type	Enumerated	
706	Requested-Domain	Enumerated	
707	Current-Location	Enumerated	
708	Identity-Set	Enumerated	
Note: The AVP codes from 709 to799 are reserved for TS 29.329.			
			32.299 [5]
Note: The AVP codes from 800 to 899 are reserved for TS 32.299			
			29.061 [13]
Note: The AVP codes from 900 to 999 are reserved for TS 29.061			
			29.210 [15]
Note: The AVP codes from 1000 to 1099 are reserved for TS 29.210			

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

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

8.1.4 Permanent Failures

The Permanent Failure result codes shall use the values from 5001 to 5999 in the Experimental-Result-Code AVP. The reserved 3GPP specific Permanent Failure result codes are presented in the following table.

Table 8.1.4: 3GPP specific Permanent Failure result codes

Experimental Result Code	Result text	Specified in the TS
5001	DIAMETER_ERROR_USER_UNKNOWN	29.229 [2]
5002	DIAMETER_ERROR_IDENTITIES_DONT_MATCH	
5003	DIAMETER_ERROR_IDENTITY_NOT_REGISTERED	
5004	DIAMETER_ERROR_ROAMING_NOT_ALLOWED	
5005	DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED	
5006	DIAMETER_ERROR_AUTH_SCHEME_NOT_SUPPORTED	
5007	DIAMETER_ERROR_IN_ASSIGNMENT_TYPE	
5008	DIAMETER_ERROR_TOO_MUCH_DATA	
5009	DIAMETER_ERROR_NOT_SUPPORTED_USER_DATA	
5010	DIAMETER_MISSING_USER_ID	
Note: The Experimental Result Codes from 5011 to 5020 are reserved for the TS 29.229.		
		32.299 [5]
Note: The Experimental Result Codes from 5021 to 5040 are reserved for the TS 32.299.		
5041	DIAMETER_ERROR_USER_NO_WLAN_SUBSCRIPTION	29.234 [6]
5042	DIAMETER_ERROR_W-APN_UNUSED_BY_USER	
5043	DIAMETER_ERROR_NO_ACCESS_INDEPENDENT_SUBSCRIPTION	
5044	DIAMETER_ERROR_USER_NO_W-APN_SUBSCRIPTION	
Note: The Experimental Result Codes from ~~5041~~ 5045 to 5060 are reserved for the TS 29.234.		
5061	GQ_INVALID_SERVICE_INFORMATION	29.209 [8]
5062	GQ_FILTER_RESTRICTIONS	
Note: The Experimental Result Codes from 5063 to 5080 are reserved for the TS 29.209.		
5100	DIAMETER_ERROR_USER_DATA_NOT_RECOGNIZED	29.329 [4]
5101	DIAMETER_ERROR_OPERATION_NOT_ALLOWED	
5102	DIAMETER_ERROR_USER_DATA_CANNOT_BE_READ	
5103	DIAMETER_ERROR_USER_DATA_CANNOT_BE_MODIFIED	
5104	DIAMETER_ERROR_USER_DATA_CANNOT_BE_NOTIFIED	
5105	DIAMETER_ERROR_TRANSPARENT_DATA_OUT_OF_SYNC	
Note: The Experimental Result Codes from 5106 to 5119 are reserved for the TS 29.329.		
		29.061 [13]
Note: The Experimental Result Codes from 5120 to 5139 are reserved for the TS 29.061		
		29.210 [15]
Note: The Experimental Result Codes from 5140 to 5159 are reserved for the TS 29.210.		
		29.109 [7]
Note: The Experimental Result Codes from 5400 to 5419 are reserved for the TS 29.109.		

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

3GPP TSG-CN1 Meeting #37 **Tdoc N4-050339**
Sydney, Australia, 14-18 February 2005

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.003** **CR** **93** ⌘ **rev** **3** ⌘ Current version: **6.5.0** ⌘

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

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

Title:	⌘	Definition of Alternative NAI
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	15/2/2005
Category:	⌘	**B**
Release:	⌘	Rel-6

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

Use one of the following releases:

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

Reason for change:	⌘	In 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	⌘	23.234-019
			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] ~~IETF Internet-Draft: "Network Discovery and Selection within the EAP Framework". draft-adrangi-eap-network-discovery-and-selection-00, work in progress~~void.

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

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.

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 shall contain a username part which is not derived from the IMSI. The username part shall not be a null string.

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

The result shall be an NAI in the form of:

"<any_non_null_string>@unreachable.3gppnetwork.org"

15 Identification of Multimedia Broadcast/Multicast Service

3GPP TSG-CN WG4 Meeting #26 **N4-050345**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **030** ⌘ **rev** **1** ⌘ Current version: **6.1.0** ⌘

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

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

Title:	⌘	Removal of material duplicating 23.234 in 29.234
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	15/02/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:

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

Reason for change:	⌘	For the clause dealing with each reference point, material is duplicated within 29.234 from 23.234 that describes that reference point. Such duplication should be replaced by a reference, where such a reference does not already exist.
Summary of change:	⌘	In all cases a brief introductory sentence describing what functional entities the reference point exists between has been retained, but all other duplicate material has been removed. Material suitable for retention existing between clause x, and subclause x.1 has been moved to subclause x.1, sometimes with some minor editorial modifications.
Consequences if not approved:	⌘	Retention of duplicate material to that specified in 23.234 within 29.234 will leave open possible deviation of that material in the future.

Clauses affected:	⌘	4, 4.1, 5, 5.1, 6, 6.1, 8, 8.1, 9, 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.

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

~~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.~~

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 Wd reference point is defined between the 3GPP AAA Proxy and the 3GPP AAA Server. The description of the reference point and its functionality is given in 3GPP TS 23.234 [4].

Therefore, this reference point is used in the roaming case only.

~~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.~~

6 Wx Description

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

6.1 Functionality

The Wx reference point is defined between the 3GPP AAA Server and the HSS. The description of the reference point and its functionality is given in 3GPP TS 23.234 [4].

~~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 authorized 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.~~
- ~~Fault recovery procedure between the HSS and the 3GPP AAA server.~~
- ~~authorization of a WLAN user via checking of user subscription information at the HSS~~

8 Wm Description

8.1 Functionality

The Wm reference point is defined between the 3GPP AAA Server and the PDG. The description of the reference point and its functionality is given in 3GPP TS 23.234 [4].

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

~~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.

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

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

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

~~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.~~

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

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

3GPP TSG CN WG4 Meeting #26 **N4-050347**
Sydney, AUSTRALIA, 14th – 18th February 2005

CR-Form-v7

CHANGE REQUEST

⌘ **29.234** **CR** **034** ⌘ **rev** **1** ⌘ Current version: **6.1.0** ⌘

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

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

Title:	⌘	Removal of unnecessary attributes on Wa
Source:	⌘	CN4
Work item code:	⌘	WLAN-IW
Date:	⌘	17/02/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:

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

Reason for change:	⌘	Removal of unnecessary attributes on Wa.
Summary of change:	⌘	This contribution removes unnecessary RADIUS attributes on the RADIUS Wa profile. The correction concerns only the Visited-Operator-Id attribute on the RADIUS Wa profile. The Visited-Operator-Id attribute gets added to RADIUS messages by the 3GPP AAA-Proxy only when the RADIUS messages traverse via the 3GPP AAA-Proxy, which does not happen on the Wa interface. Furthemore, there is no equivalent AVP defined on the Diameter Wa profile.
Consequences if not approved:	⌘	The Visited-Operator-Id attribute remains on the RADIUS Wa profile although it never gets added to RADIUS messages on the Wa interface. Also inconsistency remains between the RADIUS and the Diameter Wa profiles.

Clauses affected:	⌘	4.4.1, 4.5.1.1

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.

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

4.4.1 RADIUS based Information Elements Contents

Table 4.4.1: RADIUS based Information Elements Contents

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
USER ID	This Attribute indicates the identity of the user as defined in 3GPP TS 23.003 [22].	Mandatory	Mandatory	Mandatory	Mandatory	User-Name
RADIUS Client Address	This Attribute indicates the identifying IP Address of the RADIUS Client. It should be unique to the RADIUS Client within the scope of the RADIUS server. More detailed description of the IE can be found in IETF RFC 3580 [15].	Mandatory	NA	NA	NA	NAS-IP Address
Operator Name	Hot Spot Operator Name as defined in IETF Draft draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	NA	NA	Operator Name
Location Name	Location Type of the hot spot operator as defined in IETF Draft draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	NA	NA	Location Name
Location Information	Location information regarding the hotspot operator as defined in IETF Draft draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	NA	NA	Location information
EAP Message	This attribute encapsulates Extensible Authentication Protocol packets so as to allow the NAS to authenticate users via EAP without having to understand the EAP protocol. More detailed description of the IE can be found in IETF RFC 3580 [15].	Mandatory	Mandatory	Mandatory	Mandatory	EAP-Message
Diameter Session ID + 3GPP AAA Server Host AVP + prefix "Diameter"	This attribute is relayed from the 3GPP AAA Proxy to the WLAN-AN when the 3GPP AAA Proxy acts as translation agent. If the WLAN-AN receives such an attribute, it MUST include it in Access Requests.	Conditional	NA	NA	Conditional	State
Diameter Session ID + prefix "Diameter"	This attribute is sent by 3GPP AAA Proxy when acting as a translation agent. If WLAN-AN receives it, is should include it in subsequent accounting messages.	NA	Conditional	NA	NA	Class
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 [26].	Optional	Mandatory	NA	NA	Chargeable-User-Id
~~Visited Operator Identity~~	~~Identifies the VPLMN as specified in GSMA PRD IR.61 [25]~~	~~Mandatory~~	~~NA~~	~~NA~~	~~NA~~	~~Vendor-Specific (Visited-Operator-Id)~~

The parameters listed above as 'mandatory' are only optional in the particular RADIUS (extension) specification in which they are originally defined. However, in order for 3GPP WLAN-IW to function, these attributes shall be passed in messaging over the 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 #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	Mandatory	Mandatory	User-Name

IE NAME	IE description	Accounting Request	Accounting Response	Attribute
	3GPP TS 23.234 [4].			
RADIUS Client Address	This Attribute indicates the identifying IP Address of the RADIUS Client. It should be unique to the RADIUS Client within the scope of the RADIUS server. More detailed description of the IE can be found in IETF RFC 3580 [15].	Mandatory	NA	NAS-IP Address
Acc-Session-ID	According to IETF RFC 2866 [20], this attribute is an accounting ID which uniquely identifies the user's session. If the WLAN AN receives an Access Accept containing a Class attribute with prefix "Diameter", then the Session-ID contained therein is used as the Acc-Session-ID.	Mandatory	Mandatory	Acc-Session-ID
Operator Name	Hot Spot Operator Name as defined in [16].	Mandatory	NA	Operator Name
Location Type	Location Name of the hot spot operator as defined in IETF Draft draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	Location Type
Location Information	Location information regarding the hotspot operator as defined in IETF Draft draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	Location information
Acct.Status Type	Indicates whether this is: (i) Accounting Start. (ii) Stop. (iii) Interim Report. Accounting start indicates that this is the beginning of the user service, Account stop the end.	Mandatory	N/A	Acct.Status Type
Acc-Input-octets	Indicates the number of octets sent by the WLAN UE over the course of the session. According to IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop".	Optional	N/A	Acc-Input-octets
Acc-Output Octets	Indicates the number of octets received by the WLAN-UE. According to IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop".	Optional	N/A	
Acc-Session-Time	This attribute indicates how many seconds the user has received service for.	Conditional. Shall be present if Acct-Status-Type set to Accounting Stop	N/A	Acc-Session-Time
Acc-Input-Packets	Indicates the number of packets sent by the WLAN UE over the course of the session. According to IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop"	Optional	N/A	Acc-Input-Packets
Acc-Output-Packets	Indicates the number of packets received by the WLAN-UE over the course of the session. According to IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop".	Optional	N/A	Acc-Output-Packets
Acc-Terminate-Cause	Indicates how the session was stopped. Cause values are as per specified in IETF 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 [26].	Mandatory	NA	Chargeable-User-Id
~~Visited Operator Identity~~	~~Identifies the VPLMN as specified in GSMA PRD IR.61 [25]~~	~~Mandatory~~	~~NA~~	~~Vendor-Specific (Visited-Operator-Id)~~
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 ****

3GPP TSG-CN WG4 Meeting #26 **N4-050349**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **37** ⌘ **rev** **1** ⌘ Current version: **6.1.0** ⌘

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

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

Title:	⌘	Editorial corrections
Source:	⌘	Ericsson
Work item code:	⌘	CN4
Date:	⌘	16/12/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:

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

Reason for change:	⌘	Some corrections are needed to keep coherence.
Summary of change:	⌘	Editorial corrections and clarifications throughout the document.
Consequences if not approved:	⌘	TS will be confussing.

Clauses affected:	⌘	3.2,4,5.4.1,5.5.1,6.3,10.1.2			
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 <<<<<<<<<<<

3.2 Symbols

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

Dw	Reference point between the 3GPP AAA Server and an SLF
Wa	Reference point between a WLAN Access Network and a 3GPP AAA Proxy in the roaming case and a 3GPP AAA Server in the Non-Roaming case (charging and control signalling)
Wd	reference point between a 3GPP AAA Proxy and a 3GPP AAA Server (charging and control signalling)
~~Wf~~	~~Reference point between a Offline Charging System and a 3GPP AAA Server/Proxy~~
Wg	Reference point between a 3GPP AAA Server/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

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

>>>>>>>>>>> Second 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 IETF RFC 2865 [17], including the following extensions:
   - IETF RFC 3579 [14], which provides RADIUS extensions to support the transport of EAP frames over RADIUS.
   - IETF Draft "Carrying Location Objects in RADIUS", draft-ietf-geopriv-radius-lo-01 [16], which provides RADIUS Extensions for Public WLAN are also used in order to identify uniquely the owner and location of the WLAN.
   - IETF RFC 3576 [13], which provides RADIUS extensions to supports, amongst other capabilities, the capability to immediately disconnect a user from the WLAN AN.
2) Diameter Base, as defined in IETF RFC 3588 [7], as well as IETF Draft " Diameter Extensible Authentication Protocol (EAP) Application" [8], which provides a Diameter application to support the transport of EAP (IETF RFC 3748 [21] frames over Diameter.

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

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

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

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 (re)authentication procedures, the messaging described below is reused.

Table 4.3.1.1: Authentication request

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

~~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
User Identity	User-Name	M	This information element contains the identity of the user.
EAP payload	EAP payload	M	Encapsulated EAP payload used for UE- 3GPP AAA Server mutual authentication
Result code	~~Result~~ 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~~-Timeout	O	Max no of seconds the user session should remain active
Accounting Interim - Interval	Accounting Interim ~~-~~-Interval	O	Charging duration
Encryption-Key	EAP-Master-Session-Key	C	Shall be sent if Result Code is set to "Success". ~~This is defined in Diameter EAP specification [8]~~

RADIUS usage in Wa:

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

See Annex A.1~~.1~~ for signalling flow reference.

4.3.2 Immediate Purging of a User from WLAN access

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

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

Diameter usage in Wa:

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

Table 4.3.2.1: Information Elements passed in ASR message

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

Table 4.3.2.2: Information Elements passed in ASA message

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

See Annex A~~.1~~.2 for signalling flow reference.

RADIUS usage in Wa:

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

4.3.3 Ending a Session

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

Table 4.3.3.1: Information Elements passed in STR message

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

4.4 Information Element Contents

4.4.1 RADIUS based Information Elements Contents

Table 4.4.1: RADIUS based Information Elements Contents

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
USER ID	This Attribute indicates the identity of the user as defined in 3GPP TS 23.003 [22].	Mandatory	Mandatory	Mandatory	Mandatory	User-Name
RADIUS Client Address	This Attribute indicates the identifying IP Address of the RADIUS Client. It should be unique to the RADIUS Client within the scope of the RADIUS server. More detailed description of the IE can be found in IETF RFC 3580 [15].	Mandatory	NA	NA	NA	NAS-IP Address
Operator Name	Hot Spot Operator Name as defined in IETF Draft ~~draft-ietf-geopriv-radius-lo-01~~ draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	NA	NA	Operator Name
Location Name	Location Type of the hot spot operator as defined in IETF Draft ~~draft-ietf-geopriv-radius-lo-01~~ draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	NA	NA	Location Name
Location Information	Location information regarding the hotspot operator as defined in IETF Draft ~~draft-ietf-geopriv-radius-lo-01~~ 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	NA	Optional	NA	Optional	Session-Time-Out

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
	termination of the session or prompt. A more detailed description of the IE can be found in IETF RFC 3580 [15].					
Charging Duration	This attribute indicates the time between each interim update in seconds for this specific session. A more detailed description of the IE can be found in IETF RFC 2869 [9].	NA	Optional	NA	NA	Acct-Interim-Interval
Termination Action	This Attribute indicates what action the NAS should take when the specified service is completed. More detailed description of the IE can be found in IETF RFC 3580 [15].	NA	Optional	NA	Optional	Termination-Action
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 [26].	Optional	Mandatory	NA	NA	Chargeable-User-Id
Visited Operator Identity	Identifies the VPLMN as specified in GSMA PRD IR.61 [25]	Mandatory	NA	NA	NA	Vendor-Specific (Visited-Operator-Id)

The parameters listed above as 'mandatory' are only optional in the particular RADIUS (extension) specification in which they are originally defined. However, in order for 3GPP WLAN-IW to function, these attributes shall be passed in messaging over the 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).

4.4.2 Diameter based Information Elements Contents

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

4.4.2.1 DER and DEA Commands

ABNF for the DER and DEA messages are given below:

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

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

For the DEA, the following are necessary:

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

4.4.2.2 Session Termination Request and Answer AVPs

ABNF for the STR and STA commands are as follows:

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

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

4.4.2.3 Session Termination Request and Answer AVPs

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

```
* [ Route-Record ]
* [ AVP ]
```

4.5 Accounting Signalling Across the Wa interface

The Wa interface carries accounting signalling per WLAN user. This is implemented as described in the subclauses below either using RFC 2866 [20] or RFC 3588 [7].

4.5.1 RADIUS

If the Wa interface is implemented using RADIUS, the WLAN-AN sends a RADIUS Accounting-Request message (start) on receipt of a RADIUS Access Accept Message successfully authenticating the user.

The WLAN-AN sends a RADIUS Accounting-Request (stop) message when the WLAN session is terminated.

If the Access Accept Message contained an Acc-Interim-Interval attribute, the WLAN-AN sends interim accounting records at intervals in accordance with the value of this attribute.

During the lifetime of a WLAN session, the WLAN System may generate additional RADIUS Accounting-Request starts and stops messages.

4.5.1.1 RADIUS Attributes in accounting messages

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

Table 4.5.1: RADIUS based Information Elements Contents

IE NAME	IE description	Accounting Request	Accounting Response	Attribute
USER ID	This Attribute indicates the identity of the user. More detailed description of the IE can be found in IETF RFC 3580 [15] and 3GPP TS 23.234 [4].	Mandatory	Mandatory	User-Name
RADIUS Client Address	This Attribute indicates the identifying IP Address of the RADIUS Client. It should be unique to the RADIUS Client within the scope of the RADIUS server. More detailed description of the IE can be found in IETF RFC 3580 [15].	Mandatory	NA	NAS-IP Address
Acc-Session-ID	According to IETF RFC 2866 [20], this attribute is an accounting ID which uniquely identifies the user's session. If the WLAN AN receives an Access Accept containing a Class attribute with prefix "Diameter", then the Session-ID contained therein is used as the Acc-Session-ID.	Mandatory	Mandatory	Acc-Session-ID
Operator Name	Hot Spot Operator Name as defined in [16].	Mandatory	NA	Operator Name
Location Type	Location Name of the hot spot operator as defined in IETF Draft ~~draft-ietf-geopriv-radius-lo-01~~ draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	Location Type
Location Information	Location information regarding the hotspot operator as defined in IETF Draft ~~draft-ietf-geopriv-radius-lo-01~~ 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	Optional	N/A	Acc-Input-octets

IE NAME	IE description	Accounting Request	Accounting Response	Attribute
	only be present if ACC Status Type is set to "Stop".			
Acc-Output Octets	Indicates the number of octets received by the WLAN-UE. According to IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop".	Optional	N/A	
Acc-Session-Time	This attribute indicates how many seconds the user has received service for.	Conditional. Shall be present if Acct-Status-Type set to Accounting Stop	N/A	Acc-Session-Time
Acc-Input-Packets	Indicates the number of packets sent by the WLAN UE over the course of the session. According to IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop"	Optional	N/A	Acc-Input-Packets
Acc-Output-Packets	Indicates the number of packets received by the WLAN-UE over the course of the session. According to IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop".	Optional	N/A	Acc-Output-Packets
Acc-Terminate-Cause	Indicates how the session was stopped. Cause values are as per specified in IETF 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 [26].	Mandatory	NA	Chargeable-User-Id
Visited Operator Identity	Identifies the VPLMN as specified in GSMA PRD IR.61 [25]	Mandatory	NA	Vendor-Specific (Visited-Operator-Id)
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).

4.5.2 Diameter

When Diameter is used on the Wa interface, the accounting messaging is as per defined in NASREQ [12] i.e. Accounting Request Message (ACR) is sent by the WLAN-AN after any authentication transaction and at the end of the session.

In addition, the WLAN-AN may send Interim accounting records.

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	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	User-Name	M	This information element contains the identity of the user.
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.

4.5.2.2 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]

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

>>>>>>>>>>> Third 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.

Table 5.4.1.1: Diameter EAP Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User Name	M	This information element shall contain the identity of the user
EAP payload	EAP payload	M	Encapsulated EAP payload used for 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	C	Identifies the VPLMN and shall be present during the first DER message of either authentication or reauthentication sent by the 3GPP AAA Proxy to 3GPP AAA Server.
WLAN UE MAC address	Calling Station-ID		Carries the MAC address of the WLAN-UE.

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

Table 5.4.1.2: Diameter EAP answer message

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

>>>>>>>>>>> End of third modified section <<<<<<<<<<<

>>>>>>>>>>> Fourth modified section <<<<<<<<<<<

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]

>>>>>>>>>>> End of fourth modified section <<<<<<<<<<<

>>>>>>>>>>> Fifth modified section <<<<<<<<<<<

6.3 Procedures Description

6.3.1 Authentication Procedures

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

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

This procedure is used between the 3GPP AAA Server and the HSS. The procedure is invoked by the 3GPP AAA Server when a new set of authentication information for a given subscriber is to be retrieved from an HSS. This can happen for example, when a new 3GPP subscriber has accessed the 3GPP AAA Server for authentication or when a new set of authentication information is required for one of the 3GPP subscribers already registered in the 3GPP AAA server. ~~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~~a previous command from the HSS or from the SLF. Otherwise only the Destination-Realm is included so that it is resolved to an HSS address in an SLF-like function. Once resolved the Destination-Host AVP is included with the suitable HSS address and it is stored in the 3GPP AAA Server for further usage.
EAP Lower Layer	EAP Lower Layer	M	This AVP shall contain the value "2" to indicate the user accessed the I-WLAN network by WLAN 3GPP Direct access and shall contain value “3” to indicate the user accessed the I-WLAN network by WLAN 3GPP IP access, according to IETFdraft-mariblanca-aaa-eap-lla-01 [27].

Table 6.3.1.2: Authentication Data content - request

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

Table 6.3.1.3: Authentication Data content - request, synchronization failure

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

Table 6.3.1.4: Authentication answer

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

Table 6.3.1.5: Authentication Data content - response

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

6.3.1.1 Detailed behaviour

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

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

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

3. 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.

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

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

message with Experimental-Result-Code set to DIAMETER_ERROR_NO_ACCESS_INDEPENDENT_SUBSCRIPTION.

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

5. 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.

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

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

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

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

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

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

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

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

6.3.2 Location Management Procedures

6.3.2.1 WLAN Registration/DeRegistration Notification

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

- Registration of the 3GPP AAA Server of an authorized 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 authorized~~ 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 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 clause 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-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.
User Profile	WLAN-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 authorized 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 authorized 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, 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.

6.3.2.2 Network Initiated De-Registration by HSS, Administrative

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

- Purge procedure between the 3GPP AAA Server and the HSS.

This procedure is used between the 3GPP AAA Server and the HSS. When the purge procedure is initiated by the HSS, indicates that a subscription has to be removed from the 3GPP AAA Server, when the purge procedure is initiated by the 3GPP AAA Server see clause 6.3.2.1.

The Wx interface performs the cancellation of a registration initiated by the HSS based on the reuse of the existing Cx registration termination command code set (RTR/RTA), see 3GPP TS 29.228 [5] and 3GPP TS 29.229[6]. It corresponds to the combination of the operations CANCEL_WLAN_REGISTRATION and CANCEL_WLAN_REGISTRATION_ACK (see 3GPP TS 23.234 [4]).

Table 6.3.2.3: Network Initiated Deregistration by HSS 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.
Reason for de-registration	Deregistration-Reason	M	The HSS shall send to the 3GPP AAA server a reason for the de-registration. The de-registration reason is composed of two parts: one textual message (if available) that is intended to be forwarded to the user that is de-registered, and one reason code (see 3GPP TS 29.229 [6]) that determines the behaviour of the 3GPP AAA Server.
Routing Information	Destination-Host	M	The 3GPP AAA server name is obtained from the Origin-Host AVP, which is received from the 3GPP AAA Server, e.g. included in the MAR command.

Table 6.3.2.4: Network Initiated Deregistration by HSS 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 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.

6.3.2.2.1 Detailed behaviour

The HSS shall de-register the affected identity and invoke this procedure to inform the 3GPP AAA server to remove the subscribed user from the 3GPP AAA Server.

The HSS shall send in the Deregistration-Reason AVP the reason for the de-registration, composed by a textual message (if available) aimed for the user and a reason code that determines the action the 3GPP AAA server has to perform. The possible reason codes are:

- PERMANENT_TERMINATION: The WLAN subscription or service profile(s) has been permanently terminated. The 3GPP AAA Server should start the network initiated de-registration towards the user.

6.3.3 User Data Handling

~~FFS~~

6.3.3.1 ~~User Profile Download~~Void

~~FFS~~

6.3.3.2 HSS Initiated Update of User Profile

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

- Indication to 3GPP AAA Server of change of WLAN subscriber profile within HSS.

This procedure is used between the 3GPP AAA Server and the HSS. The procedure is invoked by the HSS when the subscriber profile has been modified and needs to be sent to the 3GPP AAA Server. This may happen due to a modification in the HSS.

The Wx reference point performs the download of the subscriber profile initiated by the HSS based on the reuse of the existing Cx profile download command code set (PPR/PPA), see 3GPP TS 29.228 [5] and 3GPP TS 29.229[6]. It corresponds to the combination of the operations SUBSCRIBER_PROFILE and PROFILE_ACK (see 3GPP TS 23.234 [4]).

Table 6.3.3.1: User Profile Update 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.
User profile	WLAN-User-Data	M	Updated user profile. ~~Editor's note: The format of the user profile is for further study.~~
Routing Information	Destination-Host	M	The 3GPP AAA Server name is obtained from the Origin-Host AVP, which is received from the 3GPP AAA Server, e.g. included in the MAR command.

Table 6.3.3.2: User Profile Update response

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

6.3.3.2.1 Detailed behaviour

The HSS shall make use of this procedure to update relevant user profile information in the 3GPP AAA server.

The 3GPP AAA server shall overwrite, for the subscriber identity indicated in the request, current information with the information received from the HSS, except in the error situations detailed in table 6.3.3.3.

Table 6.3.3.3 details the valid result codes that the 3GPP AAA server can return in the response.

Table 6.3.3.3: User profile response valid result codes

Result-Code AVP value	Condition
DIAMETER_SUCCESS	The request succeeded.
DIAMETER_ERROR_USER_UNKNOWN	The request failed because the user is not found in 3GPP AAA Server.
DIAMETER_UNABLE_TO_COMPLY	The request failed.

>>>>>>>>>>> End of fifth modified section <<<<<<<<<<<

>>>>>>>>>>> Sixth modified section <<<<<<<<<<<

10.1.2 User-Name

The User-Name AVP is defined in the RFC 3588 [7] and contains the NAI format ~~u~~User ~~i~~Identity as described in 3GPP TS 23.234 [4].

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

>>>>>>>>>>> End of sixth modified section <<<<<<<<<<<

3GPP TSG-CN WG4 Meeting #26 **N4-050351**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **38** ⌘ **rev** **1** ⌘ Current version: **6.1.0** ⌘

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

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

Title:	⌘	Description of the RADIUS session termination procedure
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	16/02/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:

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

Reason for change:	⌘	The description of the RADIUS session termination procedure is missing.
Summary of change:	⌘	Editorial corrections and clarifications throughout the document.
Consequences if not approved:	⌘	The way to terminate a session when using the RADIUS protocol will not be specified, causing potential interworking problems.

Clauses affected:	⌘	4.3.3

	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 <<<<<<<<<<<

4.3.3 Ending a Session

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

Table 4.3.3.1: Information Elements passed in STR message

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

Table 4.3.3.2: Information Elements passed in STA message

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

RADIUS usage in Wa:

- This procedure is triggered by the last RADIUS Accounting Request of Acct.Status Type STOP correlated with this session.

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

3GPP TSG-CN WG4 Meeting #26 **N4-050352**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **39** ⌘ **rev** **1** ⌘ Current version: **6.1.0** ⌘

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

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

Title:	⌘	WLAN Diameter AVP and result codes
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	16/02/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

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

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

Reason for change:	⌘	Fill in the values of the AVP codes and result codes from TS 29.230.
Summary of change:	⌘	Insert the final values of AVP codes and result codes throughout the document. Removal of the code DIAMETER_ERROR_AUTH_METHOD_UNSUPPORTED to be aligned with the requirements in TS 33.234 of supporting both EAP AKA and EAP SIM. Error section moved because it applies to more than one interface.
Consequences if not approved:	⌘	TS will not contain the values of AVP codes and result codes.

Clauses affected:	⌘	6.3.1.1, 6.5, 10.1, 10.3

	Y	N			
Other specs affected: ⌘	X		Other core specifications	⌘	CR29.230-40
		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 <<<<<<<<<<<

6.3.1.1 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 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.

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

   - If the Access_Dependence flag of the user is set and the user has not been already authenticated by WLAN 3GPP Direct access, the authentication shall be denied by sending to the 3GPP AAA Server an answer message with Experimental-Result-Code set to DIAMETER_ERROR_NO_ACCESS_INDEPENDENT_SUBSCRIPTION.

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

~~5. Check that the authentication method indicated in the request is supported. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_AUTH_SCHEME_NOT_SUPPORTEDDIAMETER_ERROR_AUTH_METHOD_UNSUPPORTED.~~

~~6~~5. The HSS shall check if there is an existing 3GPP AAA Server already assisting the user

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

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

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

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

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

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

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

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

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

6.5 ~~Result-Code AVP values~~Void

~~This subclause 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 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.~~

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

>>>>>>>>>>> Third 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 which belong to the reference points mentioned within the scope of this specification 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	~~Tbd~~300	10.1.5	UTF8String	M, V				No
Authentication-Information-SIM	~~Tbd~~301	10.1.6	OctetString	M, V				No
Authorization -Information-SIM	~~Tbd~~302	10.1.7	OctetString	M,V				No
WLAN-User-Data	~~Tbd~~303	10.1.8	Grouped	M, V				No
Charging-Data	~~Tbd~~304	10.1.10	Grouped	M, V				No
WLAN-Access	~~Tbd~~305	10.1.11	Enumerated	M, V				No
WLAN- 3GPP-IP-Access	~~Tbd~~306	10.1.12	Enumerated	M, V				No
APN-Authorized	~~Tbd~~307	10.1.14	Grouped	M, V				No
APN-Id	~~Tbd~~308	10.1.15	OctetString	M, V				No
APN-Authorization	~~Tbd~~309	10.1.16	Enumerated	M, V				No
WLAN-Direct-IP-Access	~~Tbd~~310	10.1.17	Enumerated	M, V				No
EAP payload	Tbd	10.1.20	OctetString	M, V				No
Auth Req Type	Tbd	10.1.21	Enumerated	M,V				No
EAP-Master-Session-Key	Tbd	10.1.22	OctetString	M, V				No
Session-Request-Type	~~Tbd~~311	10.1.23	Enumerated	M, V				No
Routing-Policy	~~Tbd~~312	10.1.24	OctetString	M, V				No
Max-Requested-Bandwidth	~~Tbd~~313	10.1.26	Enumerated	M, V				No
Charging-Characteristics	~~Tbd~~314	10.1.27	Grouped	M, V				No
Charging-Nodes	~~Tbd~~315	10.1.28	Grouped	M, V				No
Primary-OCS-Charging-Function-Name	~~Tbd~~316	10.1.29	DiameterIdentity	M, V				No
Secondary-OCS-Charging-Function-Name	~~Tbd~~317	10.1.30	DiameterIdentity	M, V				No
3GPP-AAA-Server-Name	~~Tbd~~318	10.1.34	DiameterIdentity	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 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 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 is of type OctetString and contains the response SRES.

10.1.8 WLAN-User-Data

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

AVP format

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

10.1.9 Void

10.1.10 Charging--Data

The Charging-Data AVP is of type Grouped, and contains the addresses of the charging functions.

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 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-3GPP-IP-Access

The WLAN-3GPP-IP-Access AVP 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 "APN-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 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 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).

Also information is provided about the WLAN UE remote IP address when it has been statically assigned by the operator.

AVP format

```
APN-Authorized::= <AVP header: TBD>
    { APN-Id }
    { APN-Barring-Type}
    [ Framed-IP-Address]
    *[Framed-IPv6-Prefix]
    *[AVP]
```

10.1.15 APN-Id

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

10.1.16 APN- Barring-Type

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_ NO_BARRING (0)

Access is allowed in visited PLMNs and home PLMN.

WLAN_ APN_HOME_BARRED_WHEN_ROAMING (1)

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

WLAN_ APN_VISITED _BARRED (2)

The subscriber is barred to activate the W-APN that access a PDG within the VPLMN when he is located in a VPLMN 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 WLAN Direct IP Access

The WLAN Direct IP Access AVP 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_ DIRECT_IP_ACCESS (0)

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

WLAN_NO_DIRECT_IP_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 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 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 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 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 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 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 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 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 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 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 [24].

10.1.28 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 [23].

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]

10.1.29 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)

10.1.30 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.

10.1.31 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.

10.1.32 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 remote 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

10.1.33 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, a 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+

10.1.34 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.

10.1.35 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[27].

For I-WLAN, only 802.1X value for WLAN 3GPP Direct access and IKEv2 value for WLAN 3GPP IP access are valid.

>>>>>>>>>>> End of third modified section <<<<<<<<<<<

>>>>>>>>>>> Fourth modified section <<<<<<<<<<<

10.3 Result-Code AVP values

This subclause 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.

10.3.1 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.

Errors not defined in this specification may be found in 3GPP TS 29.229 [6]

10.3.1.1 DIAMETER_ERROR_USER_NO_WLAN_SUBSCRIPTON (5041)

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

10.3.1.2 DIAMETER_ERROR_W-APN_UNUSED_BY_USER_(5042)

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

10.3.1.3 DIAMETER_ERROR_NO_ACCESS_INDEPENDENT_SUBSCRIPTION (5043)

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.

10.3.1.4 DIAMETER_ERROR_USER NO_W-APN_SUBSCRIPTION (5044)

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.

>>>>>>>>>>> End of fourth modified section <<<<<<<<<<<

3GPP TSG-CN WG4 Meeting #26 **N4-050353**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **41** ⌘ **rev** **1** ⌘ Current version: **6.1.0** ⌘

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

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

Title:	⌘	WLAN Diameter AVP table and chapters coherence revision
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	16/02/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

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

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

Reason for change:	⌘	The chapters describing Diameter AVPs need corrections to keep coherence.
Summary of change:	⌘	Deletion of: - Three AVPs in the table that are defined by IETF. Correction of: - The name of Charging Nodes AVP in the AVP format of the corresponding chapter. - The name of Secondary Charging Collection Function AVP. - The name of APN-Barring-Type AVP. - The type of Authentication-Method AVP. - The type of Routing-Policy AVP. - The type of Max-Requested-Bandwidth AVP. - The type of Charging-Characteristics AVP. Addition of: - The chapter for the Primary Charging Collection Function AVP.
Consequences if not approved:	⌘	TS will be confusing in the names and types of AVPs.

Clauses affected:	⌘	10.1

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 <<<<<<<<<<<

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 ~~which belong to~~ initially defined by the reference points mentioned within ~~the scope of~~ this specification are listed ~~here~~in Table 10.1.1.

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	tbd	10.1.5	~~UTF8String~~Enumerated	M, V				No
Authentication-Information-SIM	tbd	10.1.6	OctetString	M, V				No
Authorization -Information-SIM	tbd	10.1.7	OctetString	M,V				No
WLAN-User-Data	tbd	10.1.8	Grouped	M, V				No
Charging-Data	tbd	10.1.10	Grouped	M, V				No
WLAN-Access	tbd	10.1.11	Enumerated	M, V				No
WLAN- 3GPP-IP-Access	tbd	10.1.12	Enumerated	M, V				No
APN-Authorized	tbd	10.1.14	Grouped	M, V				No
APN-Id	tbd	10.1.15	OctetString	M, V				No
APN-~~Authorization~~Barring-Type	tbd	10.1.16	Enumerated	M, V				No
WLAN-Direct-IP-Access	tbd	10.1.17	Enumerated	M, V				No
~~EAP payload~~	~~tbd~~	~~10.1.20~~	~~OctetString~~	~~M, V~~				~~No~~
~~Auth Req Type~~	~~tbd~~	~~10.1.21~~	~~Enumerated~~	~~M,V~~				~~No~~
~~EAP Master Session Key~~	~~tbd~~	~~10.1.22~~	~~OctetString~~	~~M, V~~				~~No~~
Session-Request-Type	tbd	10.1.23	Enumerated	M, V				No
Routing-Policy	tbd	10.1.24	~~OctetString~~IPFilterRule	M, V				No
Max-Requested-Bandwidth	tbd	10.1.26	~~Enumerated~~OctetString	M, V				No
Charging-Characteristics	tbd	10.1.27	~~Grouped~~Integer	M, V				No
Charging-Nodes	tbd	10.1.28	Grouped	M, V				No
Primary-OCS-Charging-Function-Name	tbd	10.1.29	DiameterIdentity	M, V				No
Secondary-OCS-Charging-Function-Name	tbd	10.1.30	DiameterIdentity	M, V				No
3GPP-AAA-Server-Name	tbd	10.1.34	DiameterIdentity	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 is of type ~~UTF8String~~ Enumerated 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 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 is of type OctetString and contains the response SRES.

10.1.8 WLAN-User-Data

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

AVP format

```
WLAN-User-Data::= <AVP header: TBD>
    [Subscription-ID ]
    { WLAN-Access }
    { WLAN-3GPP-IP-Access }
```

```
[ Session-Timeout ]
1* { Charging-Data  }
*[ APN-Authorized ]
{ WLAN-Direct-IP-Access }
* [AVP]
```

10.1.9 Void

10.1.10 Charging--Data

The Charging-Data AVP is of type Grouped, and contains the addresses of the charging functions.

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 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-3GPP-IP-Access

The WLAN-3GPP-IP-Access AVP 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 "APN-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 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 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).

Also information is provided about the WLAN UE remote IP address when it has been statically assigned by the operator.

AVP format

```
APN-Authorized::= <AVP header: TBD>
    { APN-Id }
    { APN-Barring-Type}
    [ Framed-IP-Address]
    *[Framed-IPv6-Prefix]
    *[AVP]
```

10.1.15 APN-Id

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

10.1.16 APN-Barring-Type

The APN-Barring-Type~~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_ NO_BARRING (0)

Access is allowed in visited PLMNs and home PLMN.

WLAN_ APN_HOME_BARRED_WHEN_ROAMING (1)

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

WLAN_ APN_VISITED _BARRED (2)

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

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 WLAN Direct IP Access

The WLAN Direct IP Access AVP 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_ DIRECT_IP_ACCESS (0)

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

WLAN_NO_DIRECT_IP_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 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 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 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 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 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 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 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 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 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 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 [24].

10.1.28 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 [23].

AVP format

Charging~~Data~~Nodes::= <AVP header: TBD>

[Primary-OCS-Charging-Function-Name]

[Secondary-OCS-Charging-Function-Name]

{ Primary-Charging-Collection-Function-Name }

[Secondary-Charging-Collection-Function-Name]

* [AVP]

10.1.29 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)

10.1.30 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.

10.1.31 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 Collection Function.

10.1.32 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 remote 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

10.1.33 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, a 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+

10.1.34 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.

10.1.35 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[27].

For I-WLAN, only 802.1X value for WLAN 3GPP Direct access and IKEv2 value for WLAN 3GPP IP access are valid.

10.1.36 Primary-Charging-Collection-Function-Name

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

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

g3GPP TSG-CN WG4 Meeting #26 **N4-050303**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.234** **CR** **42** ⌘ **rev** **2** ⌘ Current version: **6.1.0** ⌘

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

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

Title:	⌘	PDG Behaviour on the Wm interface
Source:	⌘	CN4
Work item code:	⌘	WLAN
Date:	⌘	19/01/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:

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

Reason for change:	⌘	PDG behaviour on the Wm interface is not sufficiently well defined, which could lead to implementation problems.
Summary of change:	⌘	Section 8.3.2 has some clarifications added.
Consequences if not approved:	⌘	Handling of authorization and authentication may not be properly implemented.

Clauses affected:	⌘	8.3.2

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

Other comments: ⌘

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

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

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

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

8.3.1 Authentication Procedures

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

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

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

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

Table 8.3.1.1: Authentication Request

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

Table 8.3.1.2: Authentication Answer

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

8.3.1.1 3GPP AAA Server Detailed Behaviour

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

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

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

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

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

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

8.3.1.2 3GPP AAA Proxy Detailed Behaviour

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

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

8.3.2 Authorization Procedures

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

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

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

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

Table 8.3.2.1 Wm Authorization Request

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

Table 8.3.2.2: AA-Response

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

3GPP TSG CN WG4 Meeting #26 ***N4-050357***
Sydney, AUSTRALIA, 14th – 18th February 2005

CR-Form-v7

CHANGE REQUEST

⌘ **29.234** **CR** **047** ⌘ **rev** **1** ⌘ Current version: **6.1.0** ⌘

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

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

Title:	⌘	Wa Interface RADIUS profile Information Element corrections
Source:	⌘	CN4
Work item code:	⌘	WLAN-IW
Date:	⌘	17/02/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

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

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

Reason for change:	⌘	Addition of missing Information Elements to the RADIUS Wa profile
Summary of change:	⌘	This adds clarifications and missing Information Elements to the RADIUS Wa profile when no Diameter-RADIUS translation takes place.
Consequences if not approved:	⌘	Information Element descriptions for the Class and State attributes are misleading.

Clauses affected:	⌘	4.4.1, 4.5.1.1

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

Other comments:	⌘	

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

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

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

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

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

4.4.1 RADIUS based Information Elements Contents

Table 4.4.1: RADIUS based Information Elements Contents

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

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
	IE is used when no Diameter-RADIUS translation takes place.					
Session ID	A 3GPP AAA Server using RADIUS shall include this attribute to facilitate charging correlation between accounting and authorization messaging. If the Radius Client in WLAN-AN receives it, it shall be included in subsequent accounting messages. This IE is used when no Diameter-RADIUS translation takes place.	NA	Conditional	NA	NA	Class
Session Alive Time	This Attribute sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt. A more detailed description of the IE can be found in IETF RFC 3580 [15].	NA	Optional	NA	Optional	Session-Time-Out
Charging Duration	This attribute indicates the time between each interim update in seconds for this specific session. A more detailed description of the IE can be found in IETF RFC 2869 [9].	NA	Optional	NA	NA	Acct-Interim-Interval
Termination Action	This Attribute indicates what action the NAS should take when the specified service is completed. More detailed description of the IE can be found in IETF RFC 3580 [15].	NA	Optional	NA	Optional	Termination-Action
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 [26].	Optional	Mandatory	NA	NA	Chargeable-User-Id
Visited Operator Identity	Identifies the VPLMN as specified in GSMA PRD IR.61 [25]	Mandatory	NA	NA	NA	Vendor-Specific (Visited-Operator-Id)

The parameters listed above as 'mandatory' are only optional in the particular RADIUS (extension) specification in which they are originally defined. However, in order for 3GPP WLAN-IW to function, these attributes shall be passed in messaging over the 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 #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 [16].	Mandatory	NA	Operator Name
Location Type	Location Name of the hot spot operator as defined in IETF Draft draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	Location Type
Location Information	Location information regarding the hotspot operator as defined in IETF Draft draft-ietf-geopriv-radius-lo-01 [16].	Mandatory	NA	Location information
Acct.Status Type	Indicates whether this is: (i) Accounting Start. (ii) Stop. (iii) Interim Report. Accounting start indicates that this is the beginning of the user service, Account stop the end.	Mandatory	N/A	Acct.Status Type
Acc-Input-octets	Indicates the number of octets sent by the WLAN UE over the course of the session. According to IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop".	Optional	N/A	Acc-Input-octets
Acc-Output Octets	Indicates the number of octets received by the WLAN-UE. According to IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop".	Optional	N/A	
Acc-Session-Time	This attribute indicates how many seconds the user has received service for.	Conditional. Shall be present if Acct-Status-Type set to Accounting Stop	N/A	Acc-Session-Time
Acc-Input-Packets	Indicates the number of packets sent by the WLAN UE over the course of the session. According to IETF RFC 2866 [20],	Optional	N/A	Acc-Input-Packets

IE NAME	IE description	Accounting Request	Accounting Response	Attribute
	shall only be present if ACC Status Type is set to "Stop"			
Acc-Output-Packets	Indicates the number of packets received by the WLAN-UE over the course of the session. According to IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop".	Optional	N/A	Acc-Output-Packets
Acc-Terminate-Cause	Indicates how the session was stopped. Cause values are as per specified in IETF RFC 3580 [15].	Conditional. Shall be present if Acct-Status-Type set to "Accounting Stop".	N/A	Acc-Terminate-Cause
Chargeable User Identity	This Attribute shall contain the MSISDN of the user as specified in IETF Draft draft-adrangi-radius-chargeable-user-identity-02 [26].	Mandatory	NA	Chargeable-User-Id
Visited Operator Identity	Identifies the VPLMN as specified in GSMA PRD IR.61 [25]	Mandatory	NA	Vendor-Specific (Visited-Operator-Id)
Event Time Stamp	Number of second elapsed since January 1st 1970. UTC time.	Mandatory	NA	Event-Time-Stamp
Session ID	This attribute is used to link related authentication and accounting sessions and should be included unmodified to accounting request messages. This IE is used when no Diameter-RADIUS translation takes place.	Optional	NA	Class

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

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