ETSI TS 129 234 V7.15.0 (2013-06)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
LTE;
3GPP system to Wireless Local Area Network (WLAN)
interworking;
Stage 3
(3GPP TS 29.234 version 7.15.0 Release 7)

Reference

RTS/TSGC-0429234v7f0

Keywords

UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or
perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF).
In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive
within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

ETSI

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x   the first digit:

1   presented to TSG for information;

2   presented to TSG for approval;

3   or greater indicates TSG approved document under change control.

y   the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z   the third digit is incremented when editorial only changes have been incorporated in the document.

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 Wg reference point between the 3GPP AAA Server/Proxy and the WAG.

- The Pr reference point between the 3GPP AAA Server and the PNA.

2   References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

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

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

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

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

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

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

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

[8]   IETF RFC 4072: "Diameter Extensible Authentication Protocol (EAP) Application".

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

[10]   Void

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

[12]   IETF RFC 4005: "Diameter Network Access Server Application".

[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 RFC 5580, "Carrying Location Objects in RADIUS and Diameter ".

[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 RFC 4006, "Diameter Credit-control Application".

[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 RFC 4372: "Chargeable User Identity".

[27]   Void

[28]   IETF RFC 4186: "Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)" .

[29]   IETF RFC 4187: "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".

[30]   IETF RFC 4849 "RADIUS Filter Rule Attribute".

[31]   3GPP TS 23.141: "Presence Service; Architecture and functional description".

[32]   3GPP TS 32.299: "Telecommunication management; Charging management; Diameter charging applications".

[33]   3GPP TS 32.252: "Telecommunication management; Charging management; Wireless Local Area Network (WLAN) charging".

[34]   Void

[35]   IETF RFC 5777: "Quality of Service Attributes for Diameter".

[36]   IETF RFC 5729: "Clarifications on the Routing of Diameter Requests Based on the Username and the Realm".

[37]   Void

[38]   Void

[39]   IETF RFC 5080 (December 2007): "Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes".

3 Definitions, symbols and abbreviations

3.1 Definitions

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

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

In addition, for the purposes of the present document, the following terms and definitions given in 3GPP TS 23.141 [31] apply.

Presence Network Agent

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)
Wg   Reference point between a 3GPP AAA Server/Proxy and a 3GPP WAG
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
Wx   Reference point between an HSS and a 3GPP AAA Server
Pr   Reference point between a 3GPP AAA Server and a PNA

3.3 Abbreviations

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

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

4 Wa Description

4.1 Functionality

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

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 RFC 5580 [16], which provides RADIUS and Diameter Extensions for Public WLAN which are used in order to identify uniquely the owner and location of the WLAN.

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

   - IETF RFC 4849"RADIUS Filter Rule Attribute" [30], which provides RADIUS Extensions for Public WLAN including attributes to provide filtering and routing enforcement.

   - IETF RFC 4372 "Chargeable User Identity" [26], which provides RADIUS Extensions for carrying a chargeable user identity from the Home PLMN to the WLAN AN.

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

   - IETF RFC 4072 [8], which provides a Diameter application to support the transport of EAP (IETF RFC 3748 [21]) frames over Diameter.

   - IETF RFC 4005 [12], which defines a Diameter protocol application used for Authentication, Authorization and Accounting (AAA) services in the Network Access Server (NAS) environment.

   - IETF RFC 5580 [16], which provides RADIUS and Diameter Extensions for Public WLAN which are used in order to uniquely identify the owner and location of the WLAN. .

   - IETF RFC 5729 [36], which defines the procedures related to the routing of Diameter requests when the User-Name AVP contains a Decorated NAI as defined in 3GPP TS 23.003 [22].

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 or Server.

Diameter usage in Wa:

- This procedure is mapped to the Diameter-EAP-Request and Diameter-EAP-Answer command codes specified in IETF RFC 4072 [8].

- If the User-Name AVP contains a Decorated NAI as defined in 3GPP TS 23.003 [22], then the Diameter request routing shall follow the procedures defined in IETF RFC 5729 [36].

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

Table 4.3.1.1: WLAN Access Authentication and Authorization request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.
EAP payload	EAP-payload	M	Encapsulated EAP payload used for WLAN UE-3GPP AAA Server mutual authentication
Authentication Request Type	Auth Request-Type	M	Defines whether the user is to be authenticated only, authorized only or both. AUTHORIZE_AUTHENTICATE 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.
Supported 3GPP WLAN QoS profile	QoS-Capability	O	If the WLAN AN supports QoS mechanisms, this information element may be included to contain the WLAN AN"s QoS capabilities.

Table 4.3.1.2: WLAN Access Authentication and Authorization response

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.
EAP payload	EAP payload	M	Encapsulated EAP payload used for UE- 3GPP AAA Server mutual authentication
Result code	Result-Code	M	Result of the operation. Result codes are as per in NASREQ. 1xxx should be used for multi-round, 2xxx for success.
Session Alive Time	Session-Timeout	O	Max no of seconds the user session should remain active
Accounting Interim - Interval	Accounting Interim-Interval	O	Charging duration
Pairwise Master Key	EAP-Master-Session-Key	C	Shall be sent if Result Code is set to "Success".
Filter Id	Filter-Id	O	This IE indicates the name of the filter list for the user.
NAS Filter Rule	NAS-Filter-Rule	O	This IE provides filter rules that need to be configured on the NAS for the user by 3GPP Server/Proxy.
Tunneling	Tunneling	O	This IE can be used to provide needed tunnelling configuration on the NAS for the user by 3GPP Server/Proxy.
Authorized 3GPP WLAN QoS profile	QoS -Resources	O	If both supported 3GPP WLAN QoS profile of the WLAN AN and subscribed QoS profile were received by the 3GPP AAA Server, this IE may be present. This IE contains the 3GPP WLAN QoS Profile authorized by the 3GPP AAA Server based on the subscribed QoS parameters from the HSS, WLAN AN"s QoS capabilities and other information, e.g. operators" policies.

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 IETF RFC 3579 [14].

See Annex A.1 for signalling flow reference and section 4.4.1 for the RADIUS profiles for these messages. .

4.3.1.1 WLAN Access Authentication and Authorization for the Emergency Case

On receipt of a WLAN Access and Authentication Request from the WLAN AN with the realm part of the NAI in the User Identity populated with the emergency specific realm as defined in 3GPP TS 23.003 [22], the access authentication and authorization shall proceed as described in subclause 4.3.1 with the following exceptions:

The 3GPP AAA Server shall set the Emergency_Access flag and proceed with authentication.

> NOTE 1: It is open how to proceed if authentication fails but national regulations require the 3GPP AAA Server to proceed and grant access to the WLAN UE. It is FFS how to handle this requirement, in particular what PMK is sent to the WLAN AN.

> NOTE 2: The case of authentication and authorization of a UICC-less WLAN UE is FFS, pending SA3 discussions.

The 3GPP AAA Server shall prioritize this access over other accesses, where possible (e.g. expedite the signalling procedures in this case over those of normal accesses).

4.3.2 Immediate Purging of a User from WLAN access

This procedure is used to communicate between the WLAN AN and the 3GPP AAA Proxy that the 3GPP AAA Server has decided that a specific WLAN-UE shall be disconnected from accessing the WLAN interworking service. The procedure is Diameter or RADIUS based. In RADIUS case, the WLAN AN and the 3GPP AAA Proxy shall support the Disconnect Messages specified in RFC 3576 [13] in order to enable such a procedure. Diameter usage in Wa:

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

Table 4.3.2.1: Information Elements passed in ASR message

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

Table 4.3.2.2: Information Elements passed in ASA message

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

See Annex A.2 for signalling flow reference.

RADIUS usage in Wa:

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

4.3.2.1 Emergency Case

The 3GPP AAA Server shall give preferential treatment to WLAN UEs that have access for emergency purposes in scenarios including (but not necessarily limited to) network overload (where the 3GPP AAA Server uses the Purging procedure.

NOTE: It is FFS under what criteria if any, the 3GPP AAA Server shall use this procedure in the emergency case. In principle, 3GPP AAA Server shall not use this procedure, or shall do so only in very restricted circumstances.

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 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 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.

RADIUS usage in Wa:

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

4.3.4 WLAN Access Authorization Information Update Procedure

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

The procedure is Diameter or RADIUS based.

Diameter usage in Wa:

This procedure is performed in two steps:

- The 3GPP AAA server issues an unsolicited re-authentication and re-authorization request towards the WLAN AN. Upon receipt of such a request, the WLAN AN shall respond to the request and indicate the disposition of the request. This procedure is mapped to the Diameter command codes Re-Auth-Request and Re-Auth-Answer specified in RFC 3588 [7]. Information element content for these messages are shown in tables 4.3.4.1 and 4.3.4.2.

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

Table 4.3.4.1: Re-Authentication and Re-Authorization request

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

Table 4.3.4.2: Re-Authentication and Re-Authorization response

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

RADIUS usage in Wa:

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

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	NA	NA	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 NAS-IPv6-Address
Operator Name	Hot Spot Operator Name as defined in IETF RFC 5580 [16].	Mandatory	NA	NA	NA	Operator-Name
Location Information	This Attribute contains meta-data about the location information, such as sighting time, time-to-live, location-determination method, etc, as defined in IETF RFC5580 [16]. It also indicates the type of location profile (civic or geospatial) contained in the Location-Data Attribute.	Mandatory	NA	NA	NA	Location-Information
Location Data	This Attribute contains the civic or geospatial location of the hotspot operator as defined in IETF RFC 5580 [16].	Mandatory	NA	NA	NA	Location-Data
Basic Location Policy Rules	This Attribute contains basic policy rules for controlling the distribution of location information as defined in IETF RFC 5580 [16], e.g. retention expiry, URI of human-readable privacy instructions.	Optional	Optional	NA	Optional	Basic-Location-Policy-Rules
Extended Location Policy Rules	This Attribute contains a URI that indicates where a richer set of policy rules for controlling the distribution of location information can be found as defined in IETF RFC 5580 [16].	Optional	Optional	NA	Optional	Extended-Location-Policy-Rules
Location Capable	This Attribute allows the RADIUS client to indicate support for the functionality specified in IETF RFC 5580 [16].	Mandatory	NA	NA	NA	Location-Capable
Requested Location Info	This Attribute allows the 3GPP AAA server to indicate which location information about which entity it wants to receive as specified in IETF RFC 5580 [16].	NA	Optional	NA	Optional	Requested-Location-Info

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
Error Cause	The 3GPP AAA server shall include this attribute with a value of "Location-Info-Required" if it did not receive the requested location information as specified in IETF RFC 5580 [16]..	NA	NA	Optional	NA	Error-Cause
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 IE is used when no Diameter-RADIUS translation takes place.	Conditional	NA	NA	Optional	State
Session ID	A 3GPP AAA Server using RADIUS shall include this attribute to facilitate charging correlation between accounting and authorization messaging. If the Radius Client in WLAN-AN receives it, it shall be included in subsequent accounting messages. This IE is used when no Diameter-RADIUS translation takes place.	NA	Conditional	NA	NA	Class
Session Alive Time	This Attribute sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt. A more detailed description of the IE can be found in IETF RFC 3580 [15].	NA	Optional	NA	Optional	Session-Time-Out

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
Charging Duration	This attribute indicates the time between each interim update in seconds for this specific session. A more detailed description of the IE can be found in IETF RFC 2869 [9].	NA	Optional	NA	NA	Acct-Interim-Interval
Termination Action	This Attribute indicates what action the NAS should take when the specified service is completed. More detailed description of the IE can be found in IETF RFC 3580 [15].	NA	Optional	NA	Optional	Termination-Action
Pairwise Master Key (PMK)	This IE is used to carry the Pairwise Master Key. More detailed description of the IE can be found in IETF RFC 4186 [28] and IETF RFC 4187 [29].	NA	Mandatory	NA	NA	Vendor-Specific (MS-MPPE-Recv-Key)
Message Authenticator	Message Authenticator.	Mandatory	Mandatory	Mandatory	Mandatory	Message-Authenticator
WLAN-UE MAC address	Carries the MAC address of the WLAN-UE for verification at the 3GPP AAA Server.	Mandatory	NA	NA	NA	Calling-Station-Id
Chargeable User Identity	This Attribute shall contain the MSISDN and/or the IMSI of the user. The encoding of the MSISDN and the IMSI is defined in GSMA PRD IR.61 [25].	Optional	Mandatory	NA	NA	Chargeable-User-Id
Filter ID	This IE indicates the name of the filter list for the user. Filter ID IE and NAS Filter Rule IE should not be used simultaneously in a same RADIUS message.	NA	Optional	NA	NA	Filter-Id
NAS Filter Rule	This IE enables the provisioning of Layer 2-4/7 filter and redirection rules on the NAS by 3GPP AAA Server/Proxy. More detailed description of the IE can be found in IETF RFC 4849 [30].	NA	Optional	NA	NA	NAS-Filter-Rule
Tunnel Type	This IE contains the used tunnelling protocol.	NA	Optional	NA	NA	Tunnel-Type
Tunnel Medium Type	This IE contains the transport medium to use when creating a tunnel.	NA	Optional	NA	NA	Tunnel-Medium-Type
Tunnel Private Group Id	This IE indicates the group ID for a particular tunneled session.	NA	Optional	NA	NA	Tunnel-Private-Group-Id
Tunnel Client Endpoint	This IE indicates the address of the client end of the tunnel.	NA	Optional	NA	NA	Tunnel-Client-Endpoint
Tunnel Server Endpoint	This Attribute indicates the address of the server end of the tunnel.	NA	Optional	NA	NA	Tunnel-Server-Endpoint
Supported 3GPP WLAN QoS Profile	If the WLAN AN supports QoS mechanisms, this attribute may be used to indicate the supported WLAN AN"s QoS capabilities.	Optional	NA	NA	NA	3GPP-WLAN-QoS-Filter-Support
3GPP WLAN	If the WLAN AN supports	NA	Optional	NA	NA	3GPP-WLAN-

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
QoS profile	QoS mechanisms, this IE may be present in the reponse. In that case, this IE contains the 3GPP WLAN QoS Profile authorized by the 3GPP AAA Server based on the subscribed QoS parameters from the HSS, WLAN AN"s QoS capabilities and other information, e.g. operators" policies.					QoS-Filter-Rule

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

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 ]
    [ QoS-Capability ]
    * [ Proxy-Info ]
    * [ Route-Record ]
    [ Operator-Name ]
    * [ Location-Information ]
    * [ Location-Data ]
    [ Basic-Location-Policy-Rules ]
    [ Extended-Location-Policy-Rules ]
    [ Location-Capable ]
    * [ 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]
    [ QoS-Resources ]
    * [Filter-Id]
    * [NAS-Filter-Rule]
    * [Tunneling]
    * [ Proxy-Info ]
    [ Basic-Location-Policy-Rules ]
```

```
[ Extended-Location-Policy-Rules ]
[ Requested-Location-Info ]
[ Error-Cause ]
* [ AVP ]
```

4.4.2.2   Abort Session Request and Answer AVPs

ABNF for the ASR and ASA commands are as follows:

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

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

4.4.2.3   Session Termination Request and Answer AVPs

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


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

4.4.2.4   Re-Auth Request and Answer AVPs

ABNF for the RAR/RAA commands are as follows:

```
<RAR>  ::= < Diameter Header: 258, REQ, PXY >
```

```
          < Session-Id >
        { Origin-Host }
        { Origin-Realm }
        { Destination-Realm }
        { Destination-Host }
        { Auth-Application-Id }
        { Re-Auth-Request-Type }
        [ User-Name ]
        [ Destination-Host ]
        [ Origin-State-Id ]
        * [ Proxy-Info ]
        * [ Route-Record ]
        [ Basic-Location-Policy-Rules ]
        [ Extended-Location-Policy-Rules ]
        [ Requested-Location-Info ]
        * [ AVP ]

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

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	Mandatory	NA	NAS-IP-Address NAS-IPv6-Address

IE NAME	IE description	Accounting Request	Accounting Response	Attribute
	found in IETF RFC 3580 [15].			
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	Acct-Session-Id
Operator Name	Hot Spot Operator Name as defined in IETF RFC 5580 [16].	Mandatory	NA	Operator-Name
Location Information	This Attribute contains meta-data about the location information, such as sighting time, time-to-live, location-determination method, etc, as defined in IETF RFC5580 [16]. It also indicates the type of location profile (civic or geospatial) contained in the Location-Data Attribute.	Mandatory	NA	Location-Information
Location Data	This Attribute contains the civic or geospatial location of the hotspot operator as defined in IETF RFC 5580 [16].	Mandatory	NA	Location-Data
Basic Location Policy Rules	This Attribute contains basic policy rules for controlling the distribution of location information as defined in IETF RFC 5580 [16], e.g. retention expiry, URI of human-readable privacy instructions.	Optional	NA	Basic-Location-Policy-Rules
Extended Location Policy Rules	This Attribute contains a URI that indicates where a richer set of policy rules for controlling the distribution of location information can be found as defined in IETF RFC 5580 [16].	Optional	NA	Extended-Location-Policy-Rules
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 the IETF RFC 5080 [39], updating the IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Interim" or "Stop".	Conditional. Shall be present if Acct-Status-Type set to "Accounting Interim" or "Accounting Stop".	N/A	Acct-Input-Octets
Acc-Output Octets	Indicates the number of octets received by the WLAN-UE. According to the IETF RFC 5080 [39], updating the IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Interim" or "Stop".	Conditional. Shall be present if Acct-Status-Type set to "Accounting Interim" or "Accounting Stop".	N/A	Acct-Output-Octets
Acc-Session-Time	This attribute indicates how many seconds the user has received service for. According to the IETF RFC 5080 [39], updating the IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Interim" or "Stop".	Conditional. Shall be present if Acct-Status-Type set to "Accounting Interim" or "Accounting Stop".	N/A	Acct-Session-Time
Acc-Input-Packets	Indicates the number of packets sent by the WLAN UE over the course of the session. According to the IETF RFC 5080 [39], updating the IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Interim" or "Stop"	Optional	N/A	Acct-Input-Packets
Acc-Output-Packets	Indicates the number of packets received by the WLAN-UE over the course of the	Optional	N/A	Acct-Output-Packets

IE NAME	IE description	Accounting Request	Accounting Response	Attribute
	session. According to the IETF RFC 5080 [39], updating the IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Interim" or "Stop".			
Acc-Terminate-Cause	Indicates how the session was stopped. Cause values are as per specified in IETF RFC 3580 [15]. According to the IETF RFC 5080 [39], updating the IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop".	Conditional. Shall be present if Acct-Status-Type set to "Accounting Stop".	N/A	Acct-Terminate-Cause
Chargeable User Identity	This Attribute shall contain the MSISDN and/or the IMSI of the user. The encoding of the MSISDN and the IMSI is defined in GSMA PRD IR.61 [25].	Mandatory	NA	Chargeable-User-Id
Event Time Stamp	Number of second elapsed since January 1st 1970. UTC time.	Mandatory	NA	Event-Time-Stamp
Session ID	This attribute is used to link related authentication and accounting sessions and should be included unmodified to accounting request messages. This IE is used when no Diameter-RADIUS translation takes place.	Conditional. Shall be present if received in an Access Accept.	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).

4.5.2   Diameter

When Diameter is used on the Wa interface, the accounting messaging is as per defined in NASREQ IETF RFC 4005 [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 IETF RFC 4005 [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.
Operator Name	Operator-Name	M	Hot Spot Operator Name.
Location Information	Location-information	M	Contains meta-data about the location information.
Location Data	Location-Data	M	Contains the civic or geospatial location of the hotspot operator.
Basic Location Policy Rules	Basic-Location-Policy-Rules	O	Contains basic policy rules for controlling the distribution of location information.
Extended Location Policy Rules	Extended-Location-Policy-Rules	O	Contains a URI that indicates where a richer set of policy rules for controlling the distribution of location information can be found.

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]

[Operator-Name]

* [Location-Information]

* [Location-Data]

[Basic-Location-Policy-Rules]

[Extended-Location-Policy-Rules]

* [AVP]

<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]

5 Wd Description

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.

5.2 Protocols

The Wd reference point shall use only a single AAA protocol per WLAN session. RADIUS or Diameter based protocols shall be used.

The Wd protocol reference point shall contain the following protocols:

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

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

  - IETF RFC 5580 [16], which provides RADIUS and Diameter Extensions for Public WLAN to identify uniquely the owner and location of the WLAN.

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

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

- IETF RFC 4372 "Chargeable User Identity" [26], which provides RADIUS Extensions for carrying a chargeable user identity from Home PLMN to Visited PLMN.

2) Diameter Base, as defined in IETF RFC 3588 [7], as well as IETF RFC 4072 [8], which provides a Diameter application to support the transport of EAP (IETF RFC 3748 [11]) frames over Diameter, and IETF RFC5580 which provides RADIUS and Diameter Extensions for Public WLAN which are used in order to uniquely identify the owner and location of the WLAN. In addition, Diameter Base (IETF RFC 3588 [7]) and NASREQ (IETF RFC 4005 [12]) specify the accounting messaging to be exchanged. . IETF RFC 5729 [36] defines the procedures related to the routing of Diameter requests when Decorated NAIs (as defined in 3GPP TS 23.003 [22]) are used.

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

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

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

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

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

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

If the Wd reference point uses RADIUS then:

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

If the Wd reference point uses Diameter then:

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

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

If the WLAN AN is determined to be Diameter based, the operation mode of the 3GPP AAA Server shall be the normal behaviour as described in Diameter (IETF RFC 4072 [8]) and the Diameter Base (IETF RFC 3588 [7]) for authentication and NASREQ (IETF RFC 4005 [12]) for accounting.

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

If the Wd reference point is using RADIUS then:

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

If the Wd reference point is using Diameter then:

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

    - Diameter AVPs to RADIUS attributes compatibility:

        - 3GPP AAA Server shall restrict itself to use only Diameter AVPs that are compatible with RADIUS attributes. In general, 3GPP AAA Server shall use Diameter AVPs with codes not greater than 255. See section 9.5 in IETF RFC 4005 [12] for further detail.

    - Diameter specific procedures when interacting with RADIUS clients:

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

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

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

A RADIUS/Diameter Translation Agent has the following requirements:

- Receive RADIUS requests (sent to UDP port 1812);

- Diameter proxy functionality (communicate over TCP/SCTP port TBD, mandatory support for IPSec, optional support for TLS, etc.);

- Convert RADIUS requests to Diameter requests;

- Convert Diameter responses to RADIUS responses;

- Advertise to the 3GPP AAA Server whether the client located in WLAN AN is RADIUS or Diameter based;

- Managing the transaction state information of the RADIUS requests.

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

5.3.1.1 Conversion of RADIUS Request to Diameter Request

When receiving a RADIUS Request on the Wa reference point, the 3GPP AAA Proxy Translation Agent shall translate it into a Diameter Request to be forwarded on the Wd reference point, as described in IETF RFC 4005 [12].

If the RADIUS Request contains EAP frames, additional actions described in IETF RFC 4072 [8] are taken by the 3GPP AAA Proxy Translation Agent to convert this into a Diameter Request containing EAP frames. Typically, RADIUS Access Request command is translated into Diameter-EAP-Request command.

If the RADIUS Request contains the 3GPP-WLAN-QoS-Filter-Support attribute indicating support of the 3GPP-WLAN-QoS-Filter-Rule attribute in the WLAN AN, the 3GPP AAA Proxy Translation Agent shall translate it into a Diameter QoS-Capability AVP indicating support of the QoS-Resources AVP.

5.3.1.2 Conversion of Diameter Response to RADIUS Response

When receiving a Diameter Response on the Wd reference point, if the WLAN AN supports only RADIUS based Wa reference point, the 3GPP AAA Proxy Translation Agent shall translate it into a RADIUS Response to be forwarded on the Wa reference point, as described in IETF RFC 4005 [12].

If the Diameter Response contains EAP frames, additional actions described in IETF RFC 4072 [8] are taken by the 3GPP AAA Proxy Translation Agent to convert this into a RADIUS Response containing EAP frames. Typically, Diameter-EAP-Answer command is translated into RADIUS Access-Accept/Reject/Challenge command.

If the Diameter Response contains the QoS-Resources AVP, the 3GPP AAA Proxy Translation Agent shall translate it into a RADIUS 3GPP-WLAN-QoS-Filter-Rule attribute. If the 3GPP AAA Server determines that the WLAN AN is

RADIUS based (see section 5.3.1.3), it shall construct the Diameter QoS-Resources AVP such that it can be translated into a RADIUS 3GPP-WLAN-QoS-Filter-Rule attribute.

5.3.1.3   3GPP AAA Proxy advertisement of RADIUS or Diameter client to 3GPP AAA Server.

Some Diameter AVPs are defined specifically for use in Diameter messages that result from the translation of a RADIUS message into a Diameter message, or for use in Diameter messages that are to be translated into RADIUS messages. When the 3GPP AAA Proxy receives RADIUS messages on the Wa reference point, it may use these AVP's in the Diameter message it sends to the 3GPP AAA Server on the Wd reference point to indicate to the 3GPP AAA Server that the WLAN AN is RADIUS based. The 3GPP AAA Server shall modify its Response to the Diameter command in such a way that the Diameter Response message can be translated into a RADIUS Response by the 3GPP AAA Proxy Translation Agent, to be sent on by the 3GPP AAA Proxy to the WLAN AN.

The 3GPP AAA Proxy shall indicate to the 3GPP AAA Server that the WLAN AN that it is attached to is RADIUS based by including one or more of the following Diameter AVPs in the resultant Diameter command that is sent to the 3GPP AAA Server:

- NAS-IP-Address AVP.

- NAS-IPv6-Address AVP.

- State AVP.

- Termination-Cause AVP.

Further details on usage of these AVPs can be found in IETF RFC 4005 [12].

5.3.1.4   Managing the transaction state and session state information

The 3GPP AAA Proxy Translation Agent shall maintain the session state and transaction state, as indicated in IETF RFC 3588 [7].

The 3GPP AAA Proxy shall be able to keep the relationship between the RADIUS-Request and Diameter-Requests, as well as for Diameter-Responses to RADIUS-Responses.

The 3GPP AAA Proxy for every RADIUS-Request received shall maintain RADIUS transaction state information as follows, see IETF RFC 4005 [12]:

- RADIUS Identifier Field in the RADIUS-Request as described in IETF RFC 2685 [17].

- Source IP address of the RADIUS-Request message.

- Source UDP port of the RADIUS-Request message.

- RADIUS Proxy-State in the RADIUS-Request as described in IETF RFC 2685 [17].

Additionally, for every Diameter-Request that is sent to the 3GPP AAA Server, the 3GPP AAA Proxy shall maintain a Diameter transaction state information based on the Diameter Hop-by-Hop Id as described in IETF RFC 3588 [7].

Upon the reception of a RADIUS-Request, translation of that RADIUS-Request to a Diameter-Request and sending out of that Diameter-Request to the 3GPP AAA Server, the 3GPP AAA Proxy shall create the RADIUS transaction state and link it to the Diameter transaction state.

When receiving the Diameter-Response corresponding to the Diameter-Request sent to the 3GPP AAA Server, it should be possible for the 3GPP AAA Proxy to relate it to a RADIUS-Response based on the information available in the Diameter-transaction state and RADIUS transaction state.

Every RADIUS-Request received, translated to Diameter-Request and sent to the 3GPP AAA Server by the 3GPP AAA Proxy, shall be linked to a Session State as described in IETF RFC 4005 [12]:

- If the RADIUS-Request contains the State attribute and "Diameter/" prefixes its data, the data following the prefix is the Diameter Session Id.

- If the RADIUS-Request does not contain the State attribute and it is an Access_Accept, a new Diameter Session Id is generated in the 3GPP AAA Proxy.

The Diameter Session Id is included in the Session-Id AVP in the Diameter-Request.

5.4 Procedures description

5.4.1 WLAN Access Authentication and Authorization

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

Diameter usage in Wd:

This procedure is mapped to the Diameter-EAP-Request and Diameter-EAP-Answer command codes specified in IETF RFC 4072 [8] tables 5.4.1.1 and 5.4.1.2 show the information elements that should be exchanged across Wd. If the User-Name AVP contains a Decorated NAI as defined in 3GPP TS 23.003 [22], then the Diameter request routing shall follow the procedures defined in IETF RFC 5729 [36].

Table 5.4.1.1: Diameter EAP Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User Name	M	This information element shall contain the identity of the user
EAP payload	EAP payload	M	Encapsulated EAP payload used for WLAN-UE/3GPP AAA Server mutual authentication
Authentication Request Type	Auth–Request-Type	M	Defines whether the user is to be re-authenticated only, re-authorized only or both. AUTHORIZE_AUTHENTICATE 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.
Supported 3GPP WLAN QoS profile	QoS-Capability	O	If the WLAN AN supports QoS mechanisms, this information element may be included and shall contain the WLAN AN"s QoS capabilities.
Operator Name	Operator-Name	M	Hot Spot Operator Name.
Location Information	Location-Information	M	Contains meta-data about the location information.
Location Data	Location-Data	M	Contains the civic or geospatial location of the hotspot operator.
Basic Location Policy Rules	Basic-Location-Policy-Rules	O	Contains basic policy rules for controlling the distribution of location information.
Extended Location Policy Rules	Extended-Location-Policy-Rules	O	Contains a URI that indicates where a richer set of policy rules for controlling the distribution of location information can be found.
Location Capable	Location-Capable	M	Allows the RADIUS client to indicate support for the functionality specified in IETF RFC 5580.

Table 5.4.1.2: Diameter EAP answer message

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User Name	M	This information element contains the identity of the user.
EAP payload	EAP payload	M	Encapsulated EAP payload used for UE-3GPP AAA Server mutual authentication
Result code	Result Code	M	Result of the operation. Result code as per definition in NASREQ.1xxx shall be used for multi-round, 2xxx for success.
Session Alive Time	Session-Timeout	O	Max no of seconds the user session should remain active
Accounting Interim-Interval	Accounting Interim-Interval	O	Charging duration
Subscription-ID	Subscription-ID	C	This AVP shall contain the MSISDN and/or the IMSI of the user. This AVP shall be present if the result code is set to "Success", 2xxx.
Pairwise Master Key	EAP-Master-Session-Key	C	Shall be sent if Result Code is set to "Success".
Authorized 3GPP WLAN QoS profile	QoS-Resources	O	If both supported 3GPP WLAN QoS profile of the WLAN AN and subscribed QoS profile were received by the 3GPP AAA Server, this IE may be present. This IE contains the 3GPP WLAN QoS Profile authorized by the 3GPP AAA Server based on the subscribed QoS parameters from the HSS, WLAN AN"s QoS capabilities and other information, e.g. operators" policies.
Routing Policy	Routing-Policy	O	This AVP includes the routing policies and IP filtering. This AVP shall be present when Operator Determined Barring requires additional filtering information to be passed to the Access Network. The exact format of this AVP is specified in section 10.1.24.
Basic Location Policy Rules	Basic-Location-Policy-Rules	O	Contains basic policy rules for controlling the distribution of location information.
Extended Location Policy Rules	Extended-Location-Policy-Rules	O	Contains a URI that indicates where a richer set of policy rules for controlling the distribution of location information can be found.
Requested Location Info	Requested-Location-Info	O	Allows the RADIUS server to indicate which location information about which entity it wants to receive.
Error Cause	Error-Cause	O	The 3GPP AAA Proxy shall include this attribute with a value of "Location-Info-Required" if it did not receive the requested location information as specified in IETF RFC 5580 [16].

RADIUS usage in Wd:

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

5.4.2 Immediate Purging of a User from WLAN access

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

Diameter usage in Wd:

- This procedure is mapped to the Diameter command codes Diameter-Abort-Session-Request and Diameter-Abort-Session-Answer specified in RFC 3588 [7]. Information elements are as per described in section 4.3.2.

RADIUS usage in Wd:

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

5.4.3 Ending a Session

Session termination occurs when a user de-registers from the 3GPP AAA Server. This occurs via the Session Termination Request (STR) and Session Termination Answer commands (STA), defined in the base protocol IETF RFC 3588 [7]. Information elements are as per described in subclause 4.3.3.

5.4.4 Authorization Information Update Procedure

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

The procedure is Diameter or RADIUS based.

-   Diameter usage in Wd:

    -   If the 3GPP AAA server issues an unsolicited re-authentication and/or re-authorization request towards the WLAN AN, the 3GPP AAA proxy shall forward the request to the WLAN AN, which triggers the WLAN access authentication and authorization information update procedure described in the section 4.3.4.

    -   If the 3GPP AAA server issues an unsolicited re-authentication and/or re-authorization request towards the PDG located in the visited network, the 3GPP AAA proxy shall forward the request to the PDG, which triggers the access and service authorization information update procedure described in the section 8.3.5.

RADIUS usage in Wd:

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

5.5 Information Elements Contents

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 ]
            [ QoS-Capability ]
            * [ Proxy-Info ]
            * [ Route-Record ]
            [ Operator-Name ]
            * [ Location-Information ]
            * [ Location-Data ]
            [ Basic-Location-Policy-Rules ]
            [ Extended-Location-Policy-Rules ]
            [ Location-Capable ]
            * [ 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 ]
1* [ Subscription-ID ]
[ EAP-Master-Session-Key ]
[ QoS-Resources ]
* [ Proxy-Info ]
[ Basic-Location-Policy-Rules ]
[ Extended-Location-Policy-Rules ]
[ Requested-Location-Info ]
[ Error-Cause ]
* [ AVP ]
```

5.5.2 Abort Session Requests and Answer AVPs

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

5.5.3 Session Termination Request and Answer AVPs

ABNF for the STR and STA commands on the Wd interface are identical to those on the Wa interface described in section 4.4.2.3.

5.5.3A Authorization Information Update Procedure

ABNF for the RAR and RAA commands on the Wd interface are identical to those described in section 4.4.2.4.

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

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 NAS-IPv6-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	NA	NA	User-Name
Operator Name	Hot Spot Operator Name as defined in IETF RFC 5580 [16].	Mandatory	NA	NA	NA	Operator-Name
Location Information	This Attribute contains meta-data about the location information, such as sighting time, time-to-live, location-determination method, etc, as defined in IETF RFC5580 [16]. It also indicates the type of location profile (civic or geospatial) contained in the Location-Data Attribute.	Mandatory	NA	NA	NA	Location-information
Location Data	This Attribute contains the civic or geospatial location of the hotspot operator as defined in IETF RFC 5580 [16].	Mandatory	NA	NA	NA	Location-Data
Basic Location Policy Rules	This Attribute contains basic policy rules for controlling the distribution of location information as defined in IETF RFC 5580 [16], e.g. retention expiry, URI of human-readable privacy instructions.	Optional	Optional	NA	Optional	Basic-Location-Policy-Rules
Extended Location Policy Rules	This Attribute contains a URI that indicates where a richer set of policy rules for controlling the distribution of location information can be found as defined in IETF RFC 5580 [16].	Optional	Optional	NA	Optional	Extended-Location-Policy-Rules
Location Capable	This Attribute allows the RADIUS client to indicate support for the functionality specified in IETF RFC 5580 [16].	Mandatory	NA	NA	NA	Location-Capable
Requested Location Info	This Attribute allows the RADIUS server to indicate which location information about which entity it wants to receive as specified in IETF RFC 5580 [16].	NA	Optional	NA	Optional	Requested-Location-Info

Error Cause	The 3GPP AAA Proxy shall include this attribute with a value of "Location-Info-Required" if it did not receive the requested location information as specified in IETF RFC 5580 [16].	NA	NA	Optional	NA	Error-Cause
EAP Message	This attribute encapsulates Extensible Authentication Protocol packets so as to allow the NAS to authenticate users via EAP without having to understand the EAP protocol. More detailed description of the IE can be found in IETF RFC 3580 [15].	Mandatory	Mandatory	Mandatory	Mandatory	EAP-Message
State information	This attribute may be sent by the 3GPP AAA server to the WLAN-AN . If the RADIUS client in the WLAN-AN receives such an attribute, it shall be included in subsequent Access Requests.	Conditional	NA	NA	Optional	State
Session ID	This attribute is sent by 3GPP AAA server to the visited network. If the RADIUS client in the WLAN-AN receives it, it should be included in subsequent accounting messages.	NA	Mandatory	NA	NA	Class
Session Alive Time	This Attribute sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt. A more detailed description of the IE can be found in IETF RFC 3580 [15].	NA	Optional	NA	Optional	Session-Time-Out

Charging Duration	This attribute indicates the time between each interim update in seconds for this specific session. A more detailed description of the IE can be found in IETF RFC 2869 [9].	NA	Optional	NA	NA	Acct-Interim-Interval
Termination Action	This Attribute indicates what action the NAS should take when the specified service is completed. More detailed description of the IE can be found in IETF RFC 3580 [15].	NA	Optional	NA	Optional	Termination-Action
Pairwise Master Key (PMK)	This IE is used to carry the Pairwise Master Key. More detailed description of the IE can be found in IETF RFC 4186 [28] and IETF RFC 4187 [29].	NA	Mandatory	NA	NA	Vendor-Specific (MS-MPPE-Recv-Key)
Message Authenticator	Message Authenticator.	Mandatory	Mandatory	Mandatory	Mandatory	Message-Authenticator
WLAN-UE MAC address	Carries the MAC address of the WLAN-UE for verification at the 3GPP AAA Server.	Mandatory	NA	NA	NA	Calling-Station-Id
Chargeable User Identity	This Attribute shall contain the MSISDN and/or the IMSI of the use. The encoding of the MSISDN and the IMSI is defined in GSMA PRD IR.61 [25].	Optional	Mandatory	NA	NA	Chargeable-User-Id
Visited Operator Identity	Identifies the VPLMN as specified in GSMA PRD IR.61 [25]	Mandatory	NA	NA	NA	Vendor-Specific (Visited-Operator-Id)
Supported 3GPP WLAN QoS Profile	If the WLAN AN supports QoS mechanisms, this attribute may be used to indicate the supported WLAN AN"s QoS capabilities.	Optional	NA	NA	NA	3GPP-WLAN-QoS-Filter-Support
3GPP WLAN QoS profile	If the WLAN AN supports QoS mechanisms, this IE may be present in the reponse. In that case, this IE contains the 3GPP WLAN QoS Profile authorized by the 3GPP AAA Server based on the subscribed QoS parameters from the HSS, WLAN AN"s QoS capabilities and other information, e.g. operators" policies.	NA	Optional	NA	NA	3GPP-WLAN-QoS-Filter-Rule
NAS Filter Rule	This IE enables the provisioning of Layer 2-4/7 filter and redirection rules on the NAS by 3GPP AAA Server/Proxy. More detailed description of the IE can be found in IETF RFC 4849 [30].	NA	Optional	NA	NA	NAS-Filter-Rule

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).

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 NAS-IPv6-Address
Acc-Session-ID	According to IETF RFC 2866 [20], this attribute is an accounting ID which uniquely identifies the user's session.	Mandatory	Mandatory	Acct-Session-Id
Operator Name	Hot Spot Operator Name as defined in IETF RFC 5580 [16].	Mandatory	NA	Operator-Name
Location Information	This Attribute contains meta-data about the location information, such as sighting time, time-to-live, location-determination method, etc, as defined in IETF RFC5580 [16]. It also indicates the type of location profile (civic or geospatial) contained in the Location-Data Attribute.	Mandatory	NA	Location-Information
Location Data	This Attribute contains the civic or geospatial location of the hotspot operator as defined in IETF RFC 5580 [16].	Mandatory	NA	Location-Data
Basic Location Policy Rules	This Attribute contains basic policy rules for controlling the distribution of location information as defined in IETF RFC 5580 [16], e.g. retention expiry, URI of human-readable privacy instructions.	Optional	NA	Basic-Location-Policy-Rules
Extended Location Policy Rules	This Attribute contains a URI that indicates where a richer set of policy rules for controlling the distribution of location information can be found as defined in IETF RFC 5580 [16].	Optional	NA	Extended-Location-Policy-Rules
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 the IETF RFC 5080 [39], updating the IETF RFC 2866 [20], shall only be present if ACC Status Type is set to ""Interim" or Stop".	Conditional. Shall be present if Acct-Status-Type set to "Accounting Interim" or "Accounting Stop".	N/A	Acct-Input-Octets
Acc-Output Octets	Indicates the number of octets received by the WLAN-UE. According to the IETF RFC 5080 [39], updating the IETF RFC 2866 [20], shall only be present if ACC Status Type is set to ""Interim" or Stop".	Conditional. Shall be present if Acct-Status-Type set to ""Accounting Interim" or Accounting Stop".	N/A	Acct-Output-Octets
Acc-Session-Time	This attribute indicates how many seconds the user has received service for. According to IETF RFC 5080 [39], updating	Conditional. Shall be present if Acct-Status-Type set to	N/A	Acct-Session-Time

	the IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Interim" or "Stop".	"Accounting Interim" or "Accounting Stop".		
Acc-Input-Packets	Indicates the number of packets sent by the WLAN UE over the course of the session. According to the IETF RFC 5080 [39], updating the IETF RFC 2866 [20], shall only be present if ACC Status Type is set to ""Interim" or Stop"	Optional	N/A	Acct-Input-Packets
Acc-Output-Packets	Indicates the number of packets received by the WLAN-UE over the course of the session. According to I the IETF RFC 5080 [39], updating the ETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Interim" or "Stop".	Optional	N/A	Acct-Output-Packets
Acc-Terminate-Cause	Indicates how the session was stopped. Cause values are as per specified in IETF RFC 3580 [15]. According to IETF RFC 5080 [39], updating the IETF RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop".	Conditional. Shall be present if Acct-Status-Type set to "Accounting Stop".	N/A	Acct-Terminate-Cause
Event Time Stamp	Number of second elapsed since January 1st 1970. UTC time.	Mandatory	NA	Event-Time-Stamp
Chargeable User Identity	This attribute shall contain the MSISDN and/or the IMSI of the user. The encoding of the MSISDN and the IMSI is defined in GSMA PDR IR.61 [25].	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.	Conditional. Shall be present if received in an Access Accept.	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).

6 Wx Description

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].

6.2 Protocols

The Wx reference point shall be Diameter based and shall have an application ID defined for it. It is defined as an IETF vendor specific Diameter application, where the vendor is 3GPP. The application identifier is to 16777219. It is assigned by IANA (http://www.iana.org/assignments/enterprise-numbers).

6.3 Procedures Description

6.3.1 Authentication Procedures

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

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

- Checking of user subscription information at the HSS

This procedure is used between the 3GPP AAA Server and the HSS. The procedure is invoked by the 3GPP AAA Server when a new set of authentication information for a given subscriber is to be retrieved from an HSS. This can happen for example, when a new 3GPP subscriber has accessed the 3GPP AAA Server for authentication or when a new set of authentication information is required for one of the 3GPP subscribers already registered in the 3GPP AAA server. The procedure shall be invoked by 3GPP AAA Server when it detects that the VPLMN selected by a user has changed. This can happen, for example, when a user is performing a VPLMN re-selection procedure and is initiating a new authentication procedure via a new VPLMN.

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

- To retrieve authentication vectors from the HSS.

- To resolve synchronization failures between the sequence numbers in the WLAN-UE and the HSS.

Table 6.3.1.1: Authentication request

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element contains the permanent identity of the user, i.e. the IMSI.
Visited Network Identifier	Visited-Network-Identifier	C	Identifier that allows the home network to identify the Visited Network. The 3GPP AAA Server shall include this information element in the roaming case i.e. when 3GPP AAA Server receives this information element from signalling across the Wd. Editor's note: See 3GPP TS 29.229 [6] for a description of this parameter
Number Authentication Items	SIP-Number-Auth-Items	M	This information element indicates the number of authentication vectors requested
Authentication Data	SIP-Auth-Data-Item	C	See tables 6.3.1.2 and 6.3.1.3 for the contents of this information element. The content shown in table 6.3.1.2 shall be used for a normal authentication request; the content shown in table 6.3.1.3 shall be used for an authentication request after synchronization failure.
Routing Information	Destination-Host	C	If the 3GPP AAA Server knows the HSS name, this AVP shall be present. This information is available if the 3GPP AAA Server already has the HSS name stored. The HSS name is obtained from the Origin-Host AVP, which is received from a previous command from the HSS or from the SLF. Otherwise only the Destination-Realm is included so that it is resolved to an HSS address in an SLF-like function. Once resolved the Destination-Host AVP is included with the suitable HSS address and it is stored in the 3GPP AAA Server for further usage.
Access Type	NAS-Port-Type	M	This AVP shall contain the value 19 (Wireless - IEEE 802.11) if the user accessed the I-WLAN network by WLAN Direct IP Access and shall contain the value 5 (Virtual) if the user accessed the I-WLAN network by WLAN 3GPP IP Access, according to IETF RFC 2865 [17].

Table 6.3.1.2: Authentication Data content - request

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

Table 6.3.1.3: Authentication Data content - request, synchronization failure

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

Table 6.3.1.4: Authentication answer

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

Table 6.3.1.5: Authentication Data content - response

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

6.3.1.1 Detailed behaviour

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

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

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

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

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

   - If the Access_Dependence flag of the user is set and the user has been already authenticated by WLAN Direct IP 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 Direct IP Access, the authentication shall be denied by sending to the 3GPP AAA Server an answer message

      with Experimental-Result-Code set to
      DIAMETER_ERROR_NO_ACCESS_INDEPENDENT_SUBSCRIPTION.

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

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

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

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

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

        The requester 3GPP AAA Server, upon detection of a 3GPP AAA Server name in the response assumes that the user already has a 3GPP AAA Server assigned, so makes use of Diameter redirect function to indicate the 3GPP AAA Server name where to address the authentication request. For cases where RADIUS is used over the Wa and Wd interfaces, the 3GPP AAA Server shall use procedures defined on Wa/Wd interface to refuse the connection request. For recommendations as to how to avoid the frequent occurrence of such situations and to mitigate them when they do, please refer to Annex X of this specification

   - 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.

- To register the current 3GPP AAA Server address in the HSS for a given 3GPP user. This procedure is invoked by the 3GPP AAA Server after a new subscriber has been authenticated by the 3GPP AAA Server.

- To de-register the current 3GPP AAA Server address in the HSS for a given 3GPP user. When 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 / AUTHENTICATION_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	User-Name	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-Data	C	Addresses of the charging functions. It shall be present when Server-Assignment-Type in the request is equal to REGISTRATION or NO_ASSIGNMENT and the Result-Code is equal to DIAMETER_SUCCESS. When this parameter is included, the Primary-Charging-Collection-Function-Name or the Primary-OCS-Charging-Function-Name 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 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 check that the 3GPP AAA Server name stored for the
     subscriber matches the 3GPP AAA Server name received in the request, set the subscribers User Status to
     REGISTERED 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 /
     AUTHENTICATION_FAILURE, the HSS shall remove the 3GPP AAA Server name previously assigned
     for the 3GPP subscriber, set the User Status for the subscriber to NOT_REGISTERED and set the Result-
     Code AVP to DIAMETER_SUCCESS in the Server-Assignment-Response command.

   - If it indicates NO_ASSIGNMENT, the HSS shall check that the 3GPP AAA Server name stored for the
     subscriber matches the 3GPP AAA Server name received in the request, 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.

Once the 3GPP AAA server has downloaded the user profile data as a result of successful registration to the HSS, the
3GPP AAA server shall create appropriate routing policies and IP filtering information according to the retrieved
operator defined barring information. These routing policies and IP filtering informations are used for the subsequent
W-APN authorizations.

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 HSS shall clear the user's 3GPP AAA Server name and set the User Status to NOT_REGISTERED. The 3GPP AAA Server should start the network initiated de-registration towards the user.

6.3.3 User Data Handling

6.3.3.1 Void

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	C	Updated user profile. It shall be present if the user profile is changed in the HSS. If the WLAN-User-Data AVP is not present, the Charging-Information AVP shall be present.
Charging Information	Charging-Data	C	Addresses of the charging functions. If the Charging-Information AVP is not present, the WLAN-User-Data AVP shall be present.
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 or charging 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.

After a successful user profile download the 3GPP AAA server shall initiate re-authentication procedure as described in sub-clause 4.3.4 if the subscriber has previously been authenticated and authorized to 3GPP Direct Access. If the subscriber has previously been authenticated and authorized to WLAN 3GPP IP Access then the 3GPP AAA server shall initiate a re-authorization procedure as described in sub-clause 8.3.5.

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.

6.4 Information Elements Contents

6.4.1 Authentication Procedures

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

Message Format

```
< Multimedia-Authentication-Request > ::= < Diameter Header: 303, REQ, 16777219 >
```

```
    < Session-Id >
    { Vendor-Specific-Application-Id }
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    [ Destination-Host ]
    { NAS-Port-Type }
    { User-Name}
    [ Visited-Network-Identifier]
    [ SIP-Auth-Data-Item ]
    [ SIP-Number-Auth-Items ]
    * [ AVP ]
    * [ Proxy-Info ]
    * [ Route-Record ]
```

The Multimedia-Authentication-Answer (MAA) command, indicated by the Command-Code field set to 303 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Multimedia-Authentication-Request command. The Result-Code or Experimental-Result AVP may contain one of the values defined in section 6.2 of 3GPP TS 29.229 [6] in addition to the values defined in RFC 3588 [7].

Message Format

```
< Multimedia-Authentication-Answer > ::=  < Diameter Header: 303, 16777219 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    [ Result-Code ]
    [ Experimental-Result ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    { User-Name}
    [ SIP-Number-Auth-Items ]
    [ SIP-Auth-Data-Item ]
    [ 3GPP-AAA-Server-Name ]
    * [ AVP ]
    * [ Proxy-Info ]
    * [ Route-Record ]
```

6.4.2 HSS Initiated Update of User Profile

The Push-Profile-Request -Request (PPR) command, indicated by the Command-Code field set to 305 and the 'R' bit set in the Command Flags field, is sent by the HSS to the 3GPP AAA Server in order to update the subscription data of a WLAN user in the 3GPP AAA Server whenever a modification has occurred in the subscription data.

```
< Push-Profile-Request > ::= < Diameter Header: 305, REQ, 16777219 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Host }
    { Destination-Realm }
    { User-Name }
    [ WLAN-User-Data ]
    [ Charging-Data ]
    *[ AVP ]
    *[ Proxy-Info ]
    *[ Route-Record ]
```

The Push-Profile-Answer (PAA) command, indicated by the Command-Code field set to 305 and the 'R' bit cleared in the Command Flags field, is sent by the HSS in response to the Push-Profile-Request command. The Result-Code or Experimental-Result AVP may contain one of the values defined in section 6.2 of 3GPP TS 29.229 [6] in addition to the values defined in RFC 3588 [7].

```
< Push-Profile-Answer > ::=< Diameter Header: 305, 16777219 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    [Result-Code ]
    [ Experimental-Result ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    *[ AVP ]
```

```
   *[ Proxy-Info ]
   *[ Route-Record ]
```

6.4.3   Registration procedure and Profile download in Wx

The Server-Assignment-Request (SAR) command, indicated by the Command-Code field set to 301 and the 'R' bit set in the Command Flags field, is sent by the 3GPP AAA Server to the HSS in order to register or deregister a WLAN user or to download the WLAN User Profile.

```
Message Format
< Server-Assignment-Request > ::= < Diameter Header: 301, REQ, PXY, 16777219 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    [ Destination-Host ]
    { Destination-Realm }
    { User-Name}
    { Server-Assignment-Type }
   *[ AVP ]
   *[ Proxy-Info ]
   *[ Route-Record ]
```

The Server-Assignment-Answer (SAA) command, indicated by the Command-Code field set to 301 and the 'R' bit cleared in the Command Flags field, is sent by the HSS to the 3GPP AAA Server to confirm the registration, de-registration or user profile download procedure. The Result-Code or Experimental-Result AVP may contain one of the values defined in section 6.2 of 3GPP TS 29.229 [6] in addition to the values defined in RFC 3588 [7].

Message Format

```
< Server-Assignment-Answer > ::=    < Diameter Header: 301, 16777219 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    [ Result-Code ]
    [ Experimental-Result ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    { User-Name}
    [ WLAN-User-Data ]
    [ Charging- Data]
   *[ AVP ]
   *[ Proxy-Info ]
   *[ Route-Record ]
   *[ Route-Record ]
```

6.4.4   Registration Termination in Wx

This procedure is an exact copy of the existing Registration-Termination-Request (RTR) / Registration-Termination-Answer (RTA) commands from Cx reference point. See 3GPP TS 29.229 [6].

WLAN Wx reference point shall not make use of the optional Public-Identity AVP defined in RTR command.

6.5   Void

6.6   User identity to HSS resolution

The User identity to HSS resolution mechanism enables the 3GPP AAA Server to find the address of the HSS, that holds the subscriber data for a given user identity when multiple and separately addressable HSSs have been deployed by the network operator. The resolution mechanism is not required in networks that utilize a single HSS.

The resolution mechanism described in 3GPP TS 23.234 [4] is based on the Subscription Locator Function (SLF), already used in the IMS architecture 3GPP TS 29.228 [5]. The subscription locator is accessed via the Dw interface. The Dw interface is only used in conjunction with the Wx interface. The Dw interface is based on Diameter. Its functionality is implemented by means of the routing mechanism provided by an enhanced Diameter redirect agent, which is able to extract the identity of the user from the received requests.

To get the HSS address the 3GPP AAA Server sends to the SLF the Wx requests aimed for the HSS. On receipt of the HSS address from the SLF, the 3GPP AAA Server shall send the Wx requests to the HSS. Further requests associated to the same user shall make use the stored HSS address.

In networks where the use of the user identity to HSS resolution mechanism is required, each 3GPP AAA Server shall be configured with the address/name of the SLF implementing this resolution mechanism.

Note: The user identity to perform the HSS resolution is the IMSI.

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.

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

The Wm reference point shall also support procedures in order that an IMS emergency call specific W-APN shall be supported.

8.2 Protocols

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

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

8.3 Procedures Description

8.3.1 Authentication Procedures

According to the requirements specified in chapter 8.1, 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 an IKE Security Association (SA) between the UE and the PDG. Once the IKE SA has been authenticated, more than one tunnel IPSec SA can be negotiated inside the IKE SA. Hence additional (IPSec) tunnels between the UE and PDG do not need to trigger further Diameter_EAP authentication messaging to the 3GPP AAA Server.

The UE may attempt to set up additional accesses (IKE SA) via the IKE_SA procedure. In such cases, the authentication procedure is triggered over the Wm interface. Each new additional IKE SA shall be handled in a different Diameter session.

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.
Access Type	NAS-Port-Type	M	This AVP shall contain the value 5 (Virtual) to indicate that the user accessed the I-WLAN network by WLAN 3GPP IP Access, according to IETF RFC 2865 [17].

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	It 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 a 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). .

8.3.1.3 Authentication Procedures for the Emergency Case

For the case where the WLAN-UE is attempting to set up a tunnel (IPSec SA) to the emergency W-APN, authentication shall proceed as described in subclauses 8.3.1.1 and 8.3.1.2 with the following exceptions:

   NOTE 1: The UICC-less case is FFS, pending SA3 discussions.

   NOTE 2: PDG behaviour for cases where authentication procedures fail are FFS.

   NOTE 3: Optimizations whereby authentication procedures may be skipped for emergency case are FFS.

8.3.2 Authorization Procedures

According to the requirements stated in subclause 8.1, 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 IETF RFC 4005 [12] AAR-AAA command set.

Table 8.3.2.1 Wm Authorization Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element contains the identity of the user.
Diameter Session ID	Session-Id	M	This information element uniquely identifies the session.

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	3GPP-WLAN-APN-Id	C	This information element contains the W-APN which the UE is requesting authorization. This AVP is present when Session-Request-Type AVP is set to AUTHORIZATION REQUEST.
Routing Policy	Routing-Policy	C	This AVP includes the routing policy of the tunnel set-up. This AVP shall be present when Session-Request-Type AVP is set to ROUTING POLICY. The exact format of this AVP is specified in section 10.1.24.
Routing Information	Destination-Host	M	The 3GPP AAA Server name is obtained from the Origin-Host AVP of a previously received message.
PDG Charging Identifier	PDG-Charging-Id	C	The PDG charging identifier is generated by PDG and used to correlate PDG and WLAN AN charging data. This AVP is present when Session-Request-Type AVP is set to AUTHORIZATION REQUEST.
Supported 3GPP WLAN QoS profile	QoS-Capability	O	If the PDG supports QoS mechanisms, this information element may be included to contain PDG"s QoS capabilities.

Table 8.3.2.2: AA-Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Diameter Session ID	Session-Id	M	This information element uniquely identifies the session.
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	Subscription-ID AVP	C	This AVP shall contain the MSISDN and/or the IMSI of the user. This AVP shall be present if 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 Information	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.
Permanent User Identity	User-Name	C	This information element contains the IMSI of the user. This shall be present if Registration Result Code is set to "Success" and the AAR did not contain the IMSI.
WLAN Session Identifier	WLAN-Session-Id	C	This information element contains the charging identifier generated by the 3GPP AAA Server. It shall be present when Result-Code is equal to DIAMETER_SUCCESS and when the received Session-Request-Type was set to AUTHORIZATION REQUEST, and if WLAN access authentication and authorization procedure is done before tunnel establishment.
Authorized 3GPP WLAN QoS Profile	QoS-Resources	O	If both supported 3GPP WLAN QoS profile of the PDG and subscribed QoS profile were received by the 3GPP AAA Server, this IE may be present. This IE contains the 3GPP WLAN QoS Profile authorized by the 3GPP AAA Server based on the subscribed QoS parameters from the HSS, PDG"s QoS capabilities and other information, e.g. operators" policies.
Routing Policy	Routing-Policy	O	This AVP includes the routing policy (i.e. IP filters) needed for the Operator Determined Barring purposes. The exact format of this AVP is specified in section 10.1.24. It is up to the PDG implementation whether these routing policies are applied to Wi interface or applied at IPsec level using IKEv2 Traffic Selectors.

8.3.2.1 3GPP AAA Server Detailed Behaviour

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

1) Check that the user exists in the 3GPP AAA Server. The check shall be based on Diameter Session-id. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2) Check the Session-Request-Type AVP:

- If Request type is set to AUTHORIZATION REQUEST, it indicates that the WLAN-UE is attempting to access the particular W-APN at the PDG and is requesting authorization for such a W-APN access.

  • The 3GPP AAA Server shall check whether the Emergency_Access flag is set. If the Emergency_Access flag is set and the W-APN is not that for emergency as defined in 3GPP TS 23.003 [22], the Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED. If the W-APN is that defined for emergency access, the behaviour is as described in subsclause 8.3.2.3.

  • The 3GPP AAA Server shall check whether the subscriber is barred from completely from Interworking WLAN interworked service capabilities. If the subscription is barred then Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED.

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

  • The 3GPP AAA Server shall check whether the user has access to that W-APN. This information is obtained from the HSS within the APN-Authorized AVP. If not, Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED.

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

  • If the WLAN UE does not already have an active access to this W-APN, the 3GPP AAA Server shall initiate an Access-Number counter for that W-APN and set it to one. If the Access-Number counter has already been initiated, the 3GPP AAA Server shall increment the counter by one. The 3GPP AAA Server shall then check the counter value against the Maximum-Number-Accesses for that W-APN from that user"s data. If the Access-Number exceeds Maximum-Number-Accesses, the 3GPP AAA Server shall use the 3GPP AAA Server initiated disconnection procedures towards the PDG with which the user has the oldest established access in order to initiate the tear down of the SA associated with that access. The 3GPP AAA Server shall update accordingly the information of active accesses for the W-APN and shall store the PDG IP address and the Session-ID associated with the access.

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

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

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

8.3.2.2 AAA Proxy Detailed Behaviour

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

Check the Request Type AVP:

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

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

2) If Request-Type indicates ROUTING POLICY:

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

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

8.3.2.3 Authorization Procedures in the Emergency Case

8.3.2.3.1 PDG Procedures

For the case where the WLAN-UE is attempting to set up a tunnel (IPSec SA) to the emergency W-APN authorization shall proceed as described in subclauses 8.3.2.1 and 8.3.2.2 with the following exceptions:

National regulations define whether the access for emergencies shall still be granted to UE even if authentication fails. In such case PDG shall skip authentication procedures and W-APN authorization procedures on the Wm interface.

   NOTE 1: PDG behaviour in the UICC less case is FFS.

   NOTE 2: Cases where authentication fails are FFS.

On receipt of an Authorization Answer from the 3GPP AAA Server with result code set to DIAMETER_ERROR_UNSUITABLE_NETWORK, the PDG shall use procedures defined in 3GPP TS 24.234 to reject the tunnel setup procedure

8.3.2.3.2 3GPP AAA Server Procedures

For the case where the WLAN-UE is attempting to set up a tunnel (IPSec SA) to the emergency W-APN authorization shall proceed as described in subclauses 8.3.2.1 and 8.3.2.2 with the following exceptions:

On receipt of the Authorization Request from the PDG containing the emergency W-APN, the 3GPP AAA Server shall in the following order:

-   check whether the user is roaming. If the user is roaming and the PDG is in the HPLMN, the 3GPP AAA Server shall reject the authorization request and set the Experimental-Result-Code to DIAMETER_ERROR_UNSUITABLE_NETWORK

-   if the WLAN-UE is not roaming, or is roaming and the PDG is in the VPLMN, the 3GPP AAA Server shall accept the authorization request without subscription check. The 3GPP AAA Server shall not update the Access-Number counter. For this access, the 3GPP AAA Server shall store the indication that this is for IMS emergency case and shall not use procedures described in subclause .8.3.4 to disconnect it (based on Diameter Session ID).

8.3.3 PDG Initiated Session Termination Procedure

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

W here the user has several accesses(IKE_SA) active, a separate Session Termination procedure shall be initiated for each access (even if the accesses are to the same W-APN).

Table 8.3.3.1: Session Termination Request

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

Table 8.3.3.2: Session Termination Answer

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

8.3.3.1 3GPP AAA Server Detailed behaviour

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

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

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

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

8.3.3.2 3GPP AAA Proxy Detailed Behaviour

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

8.3.3.3 PDG Initiated Session Termination Procedure in Emergency Case

PDG shall not use the Session Termination procedures unless triggered by WLAN UE or until after the expiry of the underlying IKE and IPSec SA timers at the PDG associated with the emergency W-APN.

8.3.4 3GPP AAA Server Initiated Tunnel Disconnect Procedure

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

For the case where the user has several accesses (IKE_SA) active at a PDG, a separate Session Termination procedure shall be initiated for each.

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

The 3GPP AAA Server shall not use this procedure in the emergency case.

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

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.
W-APN-Id (see clause 10.5.15)	3GPP-WLAN-APN-Id	M	W-APN Identification.
Routing Information	Destination-Host	M	The PDG name is obtained from the Origin-Host AVP of a previous message received from the PDG e.g. included in the authentication command.

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

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

8.3.4.1 Detailed Behaviour

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

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

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

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

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

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

8.3.4.2 3GPP AAA Proxy Behaviour

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

8.3.5 Access and Service Authorization information Update Procedure

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

This procedure is performed in two steps:

- The 3GPP AAA server issues an unsolicited re-authentication and/or re-authorization request towards the PDG. Upon receipt of such a request, the PDG shall respond to the request and indicate the disposition of the request. This procedure is mapped to the Diameter command codes Re-Auth-Request and Re-Auth-Answer specified in RFC 3588 [7]. Information element content for these messages are shown in tables 8.3.5.1 and 8.3.5.2.

- Receiving the re-authorization request, the PDG shall invoke the authorization procedure as described in the sections 8. 3.2. Information element content for these messages are shown in tables 8.3.2.1 and 8.3.2.2.

For emergency W-APN, 3GPP AAA Server shall not use the Access and Service Authorization information update Procedure.

Table 8.3.5.1: Access and Service Authorization Information Update request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element contains the identity of the user.
Re-Auth Request Type	Re-Auth–Request-Type	M	Defines whether the user is to be re-authenticated only, re-authorized only or both. The following value can only be used: AUTHORIZE_ONLY Receiving entity may receive Re-Auth Request Type value other than AUTHORIZE_ONLY if the 3GPP AAA server is based on earlier releases. For more information see sub-clause 8.3.5.1.
Routing Information	Destination-Host	M	This information element is obtained from the Origin-Host AVP, which was included in a previous command received from the PDG.

Table 8.3.5.2: Access and Service Authorization information Update response

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

8.3.5.1 Detailed behaviour

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

The PDG shall perform the following check and if there is an error detected, the PDG shall stop processing and return the corresponding error code.

Check the Re-Auth–Request-Type AVP:

1) If it indicates AUTHENTICATE_ONLY, Result-Code shall be set to DIAMETER_INVALID_AVP_VALUE.

2) If it indicates AUTHORIZE_ONLY, the PDG shall just perform an authorization procedure as described in section 8.3.2.

3) If it indicates AUTHORIZE_AUTHENTICATE, Result-Code shall be set to DIAMETER_INVALID_AVP_VALUE.

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

8.4 Information Element Contents

8.4.1 Authentication Request/Answer Messages

ABNF for the Wm Authentication Request and Authentication Answer are given below:

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

For the DEA, the following are necessary:

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

8.4.2 Authorization Procedures

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

```
<AA-Request> ::= < Diameter Header: 265, REQ, PXY >
           < Session-Id >
```

```
                    { Auth-Application-Id }
                    { Origin-Host }
                    { Origin-Realm }
                    { Destination-Realm }
                    { Auth-Request-Type }
                    { Destination-Host }
                    [ Session-Request-Type ]
                    [ Visited-Network-Identifier ]
                    [3GPP-WLAN-APN-ID]
                    [ QoS-Capability ]
                  * [ Routing-Policy]
                    [ NAS-Identifier ]
                    [ NAS-IP-Address ]
                    [ NAS-IPv6-Address ]
                    [ NAS-Port ]
                    [ NAS-Port-Id ]
                    [ NAS-Port-Type ]
                    [ Origin-State-Id ]
                    [ Port-Limit ]
                    [ User-Name ]
                    [ User-Password ]
                    [ Service-Type ]
                    [ State ]
                    [ Authorization-Lifetime ]
                    [ Auth-Grace-Period ]
                    [ Auth-Session-State ]
                    [ Callback-Number ]
                    [ Called-Station-Id ]
                    [ Calling-Station-Id ]
                    [ Originating-Line-Info ]
                    [ Connect-Info ]
                    [ CHAP-Auth ]
                    [ CHAP-Challenge ]
                  * [ Framed-Compression ]
                    [ Framed-Interface-Id ]
                    [ Framed-IP-Address ]
                    [ Framed-IP-Netmask ]
                    [ Framed-MTU ]
                    [ Framed-Protocol ]
                    [ ARAP-Password ]
                    [ ARAP-Security ]
                  * [ ARAP-Security-Data ]
                  * [ Login-IP-Host ]
                  * [ Login-IPv6-Host ]
                    [ Login-LAT-Group ]
                    [ Login-LAT-Node ]
                    [ Login-LAT-Port ]
                    [ Login-LAT-Service ]
                  * [ Tunneling ]
                  * [ Proxy-Info ]
                  * [ Route-Record ]
                  * [ AVP ]
```

The ABNF for the AAA is as follows:

```
    <AA-Answer> ::= < Diameter Header: 265, PXY >
            < Session-Id >
            { Auth-Application-Id }
            { Auth-Request-Type }
            { Result-Code }
            { Origin-Host }
            { Origin-Realm }
            1*[ Subscription-ID-AVP]
            [ Max-Subscribed-Bandwidth ]
            [ QoS-Resources ]
            [ Framed-IP-Address ]
            [ Framed-IP-Prefix ]
            [ Charging-Data ]
            [ Service-Type ]
          * [ Class ]
          * [ Configuration-Token ]
            [ Acct-Interim-Interval ]
            [ Error-Message ]
            [ Error-Reporting-Host ]
          * [ Failed-AVP ]
            [ Idle-Timeout ]
            [ Authorization-Lifetime ]
            [ Auth-Grace-Period ]
```

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

8.4.3   PDG Initiated Session Termination Procedure

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

```
<STR> ::= < Diameter Header: 275, REQ, PXY >
            < Session-Id >
            { Origin-Host }
            { Origin-Realm }
            { Destination-Realm }
            { Auth-Application-Id }
            { Termination-Cause }
            [ User-Name ]
            [3GPP-WLAN-APN-Id ]
            [ Destination-Host ]
          * [ Class ]
            [ Origin-State-Id ]
          * [ Proxy-Info ]
          * [ Route-Record ]
          * [ AVP ]
```

For the response:

```
<STA>  ::= < Diameter Header: 275, PXY >
            < Session-Id >
            { Result-Code }
```

```
                    { Origin-Host }
                    { Origin-Realm }
                    [ User-Name ]
                  * [ Class ]
                    [ Error-Message ]
                    [ Error-Reporting-Host ]
                  * [ Failed-AVP ]
                    [ Origin-State-Id ]
                  * [ Redirect-Host ]
                    [ Redirect-Host-Usage ]
                    [ Redirect-Max-Cache-Time ]
                  * [ Proxy-Info ]
                  * [ AVP ]
```

8.4.4 3GPP AAA Server Initiated Tunnel Disconnect Procedure

ABNF for the 3GPP AAA Server Initiated Tunnel Disconnect Procedure are mapped onto the ASR and ASA commands are as follows:

<ASR> ::= < Diameter Header: 274, REQ, PXY >

< Session-Id >

{ Origin-Host }

{ Origin-Realm }

{ Destination-Realm }

{ Destination-Host }

{ Auth-Application-Id }

[User-Name]

[3GPP-WLAN-APN-Id]

[Origin-State-Id]

* [Proxy-Info]

* [Route-Record]

* [AVP]

<ASA> ::= < Diameter Header: 274, PXY >

 < Session-Id >

{ Result-Code }

{ Origin-Host }

{ Origin-Realm }

[User-Name]

[Origin-State-Id]

[Error-Message]

[Error-Reporting-Host]

* [Failed-AVP]

* [Redirected-Host]

[Redirected-Host-Usage]

[Redirected-Max-Cache-Time]

* [Proxy-Info]

```
* [ AVP ]
```

8.4.5   Access and Service Authorization Information Update Procedure

ABNF for the RAR/RAA commands on the Wm interface are identical to those described in section 4.4.2.4.

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

9   Wg Description

9.1   Functionality

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

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

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

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

9.2   Protocols

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

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

9.3   Procedures Description

9.3.1   Policy Download Procedures

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

The Wg reference point performs routing policy download based on the reuse of the NASREQ IETF RFC 4005 [12] AAR-AAA command set. If the WAG is located in the VPLMN the 3GPP AAA Server shall send the AAR command over the Wd interface to the 3GPP AAA Proxy and then it is 3GPP AAA Proxy"s task to find the WAG serving the user.

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

Table 9.3.1.1: Wg Policy Download Request

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

Table 9.3.1.2: Wg Policy Download Response

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

9.3.1.1 WAG Detailed Behaviour

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

-   If it has, the WAG shall modify the routing policy accordingly.

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

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

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

9.3.2 Routing Policy Cancellation Procedure

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

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

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

Table 9.3.2.1: Policy Cancellation - Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element contains the permanent identity of the user, i.e. the IMSI.
Routing Information	Destination-Host	M	The WAG name is obtained from the Origin-Host AVP of a previous message received from the WAG.

Table 9.3.2.2: Policy Cancellation- Answer

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

9.3.2.1 Detailed Behaviour

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

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

- If the User is known, the WAG shall remove all routing policies configured for that session. The WAG shall further remove any stored user information pertaining to that W-APN.

- The WAG shall set the Result-Code to DIAMETER_SUCCESS and send back the ASA command to the 3GPP AAA Server.

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

9.3.3 WAG Initiated Routing Policy Cancellation Procedure

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

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

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

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

Table 9.3.3.1: WAG Initiated Policy Cancellation - Notification

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element contains the permanent identity of the user, i.e. the IMSI.
Routing Information	Destination-Host	M	This information element contains the 3GPP AAA Server/Proxy name obtained from previous messages.

Table 9.3.3.2: WAG Initiated Policy Cancellation- Response

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

9.3.3.1 Detailed Behaviour

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

- Check the user is known in the 3GPP AAA Server. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

- If the User is known the 3GPP AAA Server behaviour is implementation dependent. The 3GPP AAA Server may:

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

  (ii) take steps to remove the users session at the 3GPP AAA Server and the PDG.

- The 3GPP AAA Server shall set the Result-Code to DIAMETER_SUCCESS and send back the ASA command to the WAG.

Exceptions to the cases specified here shall be treated by 3GPP AAA Server as error situations, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY.

9.4 Information Element Contents

9.4.1 Policy Download Procedures

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

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

```
           [ Login-LAT-Group ]
           [ Login-LAT-Node ]
           [ Login-LAT-Port ]
           [ Login-LAT-Service ]
         * [ Tunneling ]
         * [ Proxy-Info ]
         * [ Route-Record ]
         * [ AVP ]
```

The ABNF for the AAA is as follows:

```
<AA-Answer> ::= < Diameter Header: 265, PXY >
           < Session-Id >
           { Auth-Application-Id }
           { Auth-Request-Type }
           { Result-Code }
           { Origin-Host }
           { Origin-Realm }
           [ User-Name ]
           [ Service-Type ]
         * [ Class ]
         * [ Configuration-Token ]
           [ Acct-Interim-Interval ]
           [ Error-Message ]
           [ Error-Reporting-Host ]
         * [ Failed-AVP ]
           [ Idle-Timeout ]
           [ Authorization-Lifetime ]
           [ Auth-Grace-Period ]
           [ Auth-Session-State ]
           [ Re-Auth-Request-Type ]
           [ Session-Timeout ]
           [ State ]
         * [ Reply-Message ]
           [ Origin-State-Id ]
         * [ Filter-Id ]
           [ Password-Retry ]
           [ Port-Limit ]
           [ Prompt ]
           [ ARAP-Challenge-Response ]
           [ ARAP-Features ]
           [ ARAP-Security ]
         * [ ARAP-Security-Data ]
           [ ARAP-Zone-Access ]
           [ Callback-Id ]
           [ Callback-Number ]
           [ Framed-Appletalk-Link ]
         * [ Framed-Appletalk-Network ]
           [ Framed-Appletalk-Zone ]
         * [ Framed-Compression ]
           [ Framed-Interface-Id ]
           [ Framed-IP-Address ]
         * [ Framed-IPv6-Prefix ]
           [ Framed-IPv6-Pool ]
         * [ Framed-IPv6-Route ]
           [ Framed-IP-Netmask ]
         * [ Framed-Route ]
           [ Framed-Pool ]
           [ Framed-IPX-Network ]
           [ Framed-MTU ]
           [ Framed-Protocol ]
           [ Framed-Routing ]
         * [ Login-IP-Host ]
         * [ Login-IPv6-Host ]
           [ Login-LAT-Group ]
           [ Login-LAT-Node ]
           [ Login-LAT-Port ]
           [ Login-LAT-Service ]
           [ Login-Service ]
           [ Login-TCP-Port ]
         * [ NAS-Filter-Rule ]
         * [ QoS-Filter-Rule ]
         * [ Tunneling ]
         * [ Redirect-Host ]
           [ Redirect-Host-Usage ]
           [ Redirect-Max-Cache-Time ]
         * [ Proxy-Info ]
         * [ AVP ]
```

9.4.2 Routing Policy Cancellation Procedure

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

```
<ASR>  ::= < Diameter Header: 274, REQ, PXY >
< Session-Id >
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Destination-Host }
{ Auth-Application-Id }
[ User-Name ]
[3GPP-WLAN-APN-Id ]
[ Origin-State-Id ]
* [ Proxy-Info ]
* [ Route-Record ]
* [ AVP ]


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

9.4.3 WAG Initiated Routing Policy Cancellation Procedure

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

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

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

* [AVP]

10 Information Elements Contents

10.1 AVPs

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

Only those AVPs initially defined by the reference points mentioned within this specification are listed in Table 10.1.1.

Table 10.1.1: Diameter Multimedia Application AVPs

Attribute Name	AVP Code	Section defined	Value Type	Shall	May	Should not	Must not	May Encr.
3GPP-WLAN-APN-Id	100	10.1.15	OctetString	M, V				No
Authentication-Method	300	10.1.5	Enumerated	M, V				No
Authentication-Information-SIM	301	10.1.6	OctetString	M, V				No
Authorization -Information-SIM	302	10.1.7	OctetString	M,V				No
WLAN-User-Data	303	10.1.8	Grouped	M, V				No
Charging-Data	304	10.1.10	Grouped	M, V				No
WLAN-Access	305	10.1.11	Enumerated	M, V				No
WLAN- 3GPP-IP-Access	306	10.1.12	Enumerated	M, V				No
APN-Authorized	307	10.1.14	Grouped	M, V				No
APN-Barring-Type	309	10.1.16	Enumerated	M, V				No
WLAN-Direct-IP-Access	310	10.1.17	Enumerated	M, V				No
Session-Request-Type	311	10.1.23	Enumerated	M, V				No
Routing-Policy	312	10.1.24	IPFilterRule	M, V				No
Max-Requested-Bandwidth	313	10.1.26	OctetString	M, V				No
Charging-Characteristics	314	10.1.27	Integer	M, V				No
Charging-Nodes	315	10.1.28	Grouped	M, V				No
Primary-OCS-Charging-Function-Name	316	10.1.29	DiameterIdentity	M, V				No
Secondary-OCS-Charging-Function-Name	317	10.1.30	DiameterIdentity	M, V				No
3GPP-AAA-Server-Name	318	10.1.34	DiameterIdentity	M, V				No
Maximum-Number-Accesses	319	10.1.38	Unsigned32	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 IETF RFC 3588 [7].								

10.1.1 Auth-Session-State

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

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

The client (server) shall include in its requests (responses) the Auth-Session-State AVP set to the value NO_STATE_MAINTAINED (1), as described in 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 NAI format User Identity as described in 3GPP TS 23. 003 [22].

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 : 612 >
    [ 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 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: 303>
    [Subscription-ID ]
    { WLAN-Access }
```

```
{ WLAN-3GPP-IP-Access }
[ Session-Timeout ]
*[ APN-Authorized ]
*[ Maximum-Number-Accesses ]
{ WLAN-Direct-IP-Access }
[ QoS- Resources ]
* [AVP]
```

The QoS-Auth-Resources AVP in the WLAN-User-Data grouped AVP shall contain the subscribed QoS in WLAN Direct IP Access case.

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: 304>

> { 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: 307>
    { 3GPP-WLAN-APN-Id }
    { APN-Barring-Type}
    [ Framed-IP-Address]
    *[Framed-IPv6-Prefix]
    [ Max-Requested-Bandwidth ]
    [ QoS- Resources ]
    *[AVP]
```

10.1.15 3GPP-WLAN-APN-Id

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

10.1.16 APN-Barring-Type

The APN-Barring-Type AVP 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.

WLAN_ APN_INTERNET_ACCESS_BARRED (4)

> The subscriber is barred to access internet through any W-APN regardless of whether he is located in a VPLMN or 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 AUTHENTICATION_FAILURE.

Pr reference point defines as valid only REGISTRATION, USER_DEREGISTRATION.

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 IETF RFC 4072 [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 IETF RFC 4072 [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, i.e. Pairwise Master Key (PMK) or Master Session Key (MSK). It is defined in the IETF RFC 4072 [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 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 Routing-Policy 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 grouped and indicates the user identity to be used for charging purposes. It is defined in the IETF RFC 4006 [19].

WLAN shall make use only of the values MSISDN or IMSI. This grouped AVP shall set the sub-AVP Subscription-Id-Type to value "END_USER_E164" or to value "END_USER_IMSI" 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-Subscriber-Bandwidth. If present, shall be downloaded from HSS to 3GPP AAA Server, and 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-Nodes::= <AVP header: 315>

> [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 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 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-Charging-Collection-Function-Name AVP is defined in 3GPP TS 29.229 [6] and contains the address of the Secondary 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 the Framed-IP-Address AVP is not 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 IETF RFC 4005 [12]:

   Framed-IP-Address | 0-1 | 0-1 |

10.1.33 Framed-IPv6-Prefix

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

When the Framed-IPv6-Prefix AVP is not 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 IETF RFC 4005 [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 Void

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.

10.1.37 NAS-Port-Type

The NAS-Port-Type AVP is the Diameter translation of the NAS-Port-Type RADIUS attribute and contains an indication of the type of access that the user is requesting (tunnel or WLAN access).

10.1.38 Maximum-Number-Accesses

The Maximum-Number-Accesses AVP is of type Unsigned32, and used to specify the maximum number of concurrent accesses (IKE security associations) per W-APN.

10.1.39. WLAN-Session-Id

The WLAN-Session-Id AVP is of type Unsigned32. It is specified in 3GPP TS 32.299 [32]. The identifier is used to correlate PDG and WLAN AN charging data (see 3GPP TS 32.252 [33]).

The WLAN-Session-Id AVP contains the charging identifier generated by the 3GPP AAA Server when WLAN access authentication and authorization proceudre is done successfully.

The WLAN-Session-Id AVP is sent to PDG from 3GPP AAA Server during Wm authorization procedure and PDG includes the WLAN Session Id to PDG charging data.

10.1.40. PDG-Charging-Id

The PDG-Charging-Id AVP is of type Unsigned32. It is specified in 3GPP TS 32.299 [32]. The identifier is used to correlate PDG and WLAN AN charging data (see 3GPP TS 32.252 [33]).

The PDG-Charging-Id AVP contains the charging identifier generated by the PDG for the tunnel.

The PDG-Charging-Id AVP is sent to 3GPP AAA Server from PDG during Wm authorization procedure and 3GPP AAA Server includes the PDG Charging Id to WLAN AN charging data.

10.1.41. 3GPP-WLAN-QoS-Filter-Rule

The 3GPP-WLAN-QoS-Filter-Rule attribute contains the 3GPP WLAN QoS Profile formatted as a QoSFilterRule string as defined in IETF RFC 4005 [12]. This 3GPP vendor-specific RADIUS attribute is only applicable on the RADIUS-based Wa and Wd reference points and is encoded as follows (as per IETF RFC 2865 [17]).

				Bits					
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
1	Type = 26								
2	Length = n								
3	3GPP Vendor id octet 1								
4	3GPP Vendor id octet 2								
5	3GPP Vendor id octet 3								
6	3GPP Vendor id octet 4								
7	3GPP type = [a]								
8	3GPP Length = (n-6)								
9-n	QoSFilterRule (UTF-8 encoded characters)								

10.1.42. QoS-Resources

The QoS-Resources AVP is defined in IETF 5777 [35]. It includes the description of the resources that have been stored in the HSS as a part of a user"s subscription or authorized by the 3GPP AAA Server.

Over the Wx interface, this AVP is used to contain subscribed 3GPP WLAN QoS Profile, and over the Wm interface, this AVP is used to contain authorized 3GPP WLAN QoS profile. The following information shall be provided at least over the Wx interface:

- DiffServ DSCP information.

10.1.43. QoS-Capability

The QoS-Capability grouped AVP is defined in IETF 5777 [35]. It includes a list of supported Quality of Service profiles. The QoS-Profile sub-AVP shall have Vendor-ID and Specifier fields set to default value 0 (zero).

10.1.44 3GPP-WLAN-QoS-Filter-Support

The 3GPP-WLAN-QoS-Filter-Support attribute is a 3GPP vendor-specific attribute only applicable on the RADIUS-based Wa and Wd reference points.It indicates whether the WLAN AN supports the 3GPP-WLAN-QoS-Filter-Rule attribute and is encoded as follows (as per IETF RFC 2865 [38])

Octets	Bits							
	8	7	6	5	4	3	2	1
1	Type = 26							
2	Length = 9							
3	3GPP Vendor id octet 1							
4	3GPP Vendor id octet 2							
5	3GPP Vendor id octet 3							
6	3GPP Vendor id octet 4							
7	3GPP type = [b]							
8	3GPP Length = 3							
9	Support-Indicator octet							

The following values are defined for the Support-Indicator octet:

   0 – 3GPP-WLAN-QoS-Filter-Rule attribute is not supported by the WLAN AN.

   1 – 3GPP-WLAN-QoS-Filter-Rule attribute is supported by the WLAN AN.

If the 3GPP-WLAN-QoS-Filter-Support attribute is not present in the request, the 3GPP-WLAN-QoS-Filter-Rule attribute is not supported by the WLAN AN.

10.2 Handling of Information Elements

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

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

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

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

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

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

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 Direct IP 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.

11 Pr Description

The Pr Reference Point is defined in 3GPP TS 23.141 [31] and allows the 3GPP AAA Server to report presence relevant events to the Presence Network Agent (PNA).

11.1 Functionality

The functionality of the Pr reference point is to enable:

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

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

11.2 Protocols

The Pr reference point shall be Diameter based and shall have an application ID defined for it. It is defined as an IETF vendor specific Diameter application, where the vendor is 3GPP. The application identifier is to 16777230. It is assigned by IANA (http://www.iana.org/assignments/enterprise-numbers).

11.3 Procedures Description

11.3.1 WLAN Attach/Detach Indication

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

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

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

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

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

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

Table 11.3.1.1: WLAN Attach / Detach Indication Request

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

Table 11.3.1.2: WLAN Attach / Detach Indication Answer

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

11.3.1.1 Detailed behaviour

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

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

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

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

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

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

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

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

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

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

11.3.2   W-APN Activation/De-Activation Indication

11.3.2.1 W-APN Activation Indication

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

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

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

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

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

Table 11.3.2.1: W-APN Activation Indication request

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element contains the identity of the user.
Visited Network Identifier	Visited-Network-Identifier	C	An identifier that allows the home network to identify the Visited Network. This AVP shall be present if the PDG is not in the WLAN-UE's home network, i.e. the WLAN-UE is roaming.
W-APN-ID	3GPP-WLAN-APN-Id	M	This information element shall contain the W-APN for which the UE has been granted authorization.
Routing Information	Destination-Host	C	The PNA name is obtained from the Origin-Host AVP of a previously received message.

Table 11.3.2.2:W-APN Activation Indication Answer

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

11.3.2.1.1 Detailed behaviour

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

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

2) Store the current active W-APN

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

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

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

11.3.2.2 W-APN De-Activation Indication

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

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

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

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

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

Table 11.3.3.1: W-APN Deactivation Indication Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user.
W-APN-Id	3GPP-WLAN-APN-Id	M	This information element shall contain the W-APN Identification associated with the deactivation.
Routing Information	Destination-Host	M	The PNA name shall be obtained from the Origin-Host AVP of a previous message received from the PNA.

ETSI

Table 11.3.3.2: W-APN DeActivation Indication Answer

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

11.3.2.2.1 Detailed behaviour

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

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

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

11.4 Information Elements Contents

11.4.1 WLAN Attach/Detach Indication

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

Message Format

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

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

Message Format

```
<Server-Assignment-Answer> ::=      < Diameter Header: 301, PXY, XXXX >
                    < Session-Id >
                    { Vendor-Specific-Application-Id }
                    [ Result-Code ]
                    [Experimental-Result ]
                    { Auth-Session-State }
                    { Origin-Host }
                    { Origin-Realm }
```

```
                              [ User-Name ]
                              *[ AVP ]
                              *[ Proxy-Info ]
                              *[ Route-Record ]
```

11.4.2   W-APN Activation/DeActivation Indication

11.4.2.1 W-APN Activation Indication

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

```
<AA-Request> ::= < Diameter Header: 265, REQ, PXY >
            < Session-Id >
            { Auth-Application-Id }
            { Origin-Host }
            { Origin-Realm }
            { Destination-Realm }
            { Auth-Request-Type }
            [ Destination-Host ]
            [ Visited-Network-Identifier]
            { 3GPP-WLAN-APN- Id }
            [ User-Name ]
            [ Authorization-Lifetime ]
            [ Auth-Grace-Period ]
            [ Auth-Session-State ]
            [ Framed-IP-Address ]
            [ Framed-IP-Netmask ]
            * [ Tunneling ]
            * [ Proxy-Info ]
            * [ Route-Record ]
            * [ AVP ]
```

The ABNF for the AAA is defined as follows:

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

11.4.2.2 W-APN Deactivation Indication

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

```
<ASR>  ::= < Diameter Header: 274, REQ, PXY >
            < Session-Id >
            { Origin-Host }
            { Origin-Realm }
            { Destination-Realm }
            { Destination-Host }
            { Auth-Application-Id }
            [ User-Name ]
            { 3GPP-WLAN-APN-Id }
            [ Origin-State-Id ]
            * [ Proxy-Info ]
            * [ Route-Record ]
             *[ AVP ]


<ASA>  ::= < Diameter Header: 274, PXY >
```

```
 < Session-Id >
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
[ User-Name ]
[ Origin-State-Id ]
[ Error-Message ]
[ Error-Reporting-Host ]
* [ Failed-AVP ]
* [ Redirected-Host ]
[ Redirected-Host-Usage ]
 [ Redirected-Max-Cache-Time ]
* [ Proxy-Info ]
* [ AVP ]
```

```
 < Session-Id >
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
[ User-Name ]
[ Origin-State-Id ]
[ Error-Message ]
```

12 User identity to HSS resolution

The User identity to HSS resolution mechanism enables the 3GPP AAA servers to find the identity of the HSS that holds the subscriber data for a given user identity when multiple and separately addressable HSSs have been deployed by the network operator. The resolution mechanism is not required in networks that utilise a single HSS or when a 3GPP AAA server is configured to use pre-defined HSS address/identity.

In networks where more than one independently addressable HSS are utilized by a network operator, and the 3GPP AAA servers are not configured to use pre-defined HSS address/identity, each 3GPP AAA server shall be configured with the address/identity of the Diameter Agent (Redirect or Proxy) implementing this resolution mechanism.

To get the HSS identity that holds the subscriber data for a given user identity, the 3GPP AAA server shall send the Diameter request normally destined to the HSS to a pre-configured address/identity of a Diameter agent supporting the User identity to HSS resolution mechanism.

- If this Diameter request is received by a Diameter Redirect Agent, the Diameter Redirect Agent shall determine the HSS identity based on the provided user identity and shall send to the 3GPP AAA server a notification of redirection towards the HSS identity, in response to the Diameter request. Multiple HSS identities may be included in the response, as specified in IETF RFC 3588 [7]. In such a case, the 3GPP AAA server shall send the Diameter request to the first HSS identity in the ordered list received in the Diameter response from the Diameter Redirect Agent. If the 3GPP AAA server does not receive a successful response to the Diameter request, the 3GPP AAA server shall send a Diameter request to the next HSS identity in the ordered list. This procedure shall be repeated until a successful response from an HSS is received.

- If this Diameter request is received by a Diameter Proxy Agent, the Diameter Proxy Agent shall determine the HSS identity based on the provided user identity and shall forward the Diameter request directly to the HSS. The 3GPP AAA server shall determine the HSS identity from the response to the Diameter request received from the HSS.

After the user identity to HSS resolution, the 3GPP AAA server shall store the HSS identity/name/Realm and shall use it in further Diameter requests associated to the same user dentity.

Annex A (normative):
Wa and Wd Procedures Signalling Flows

A.1 Authentication, Authorization and Key Delivery

The purpose of this signalling sequence is to carry WLAN-UE - 3GPP AAA Server authentication signalling over the Wa and Wd reference points. As a result of a successful authentication, authorization information and session keying material for the authenticated session is delivered from the 3GPP AAA Server to the WLAN.

This Wa and Wd signalling sequence is initiated by the WLAN when authentication of a WLAN-UE is needed. This can take place when a new WLAN-UE accesses WLAN, when a WLAN-UE switches between WLAN APs or when a periodic re-authentication is performed.

The signalling sequences shown are based on RADIUS and Diameter, as specified in clauses 4 and 5. For more information on proxying and protocol translation associated with using RADIUS and Diameter between the Wa and Wd reference points see subclause 5.3.
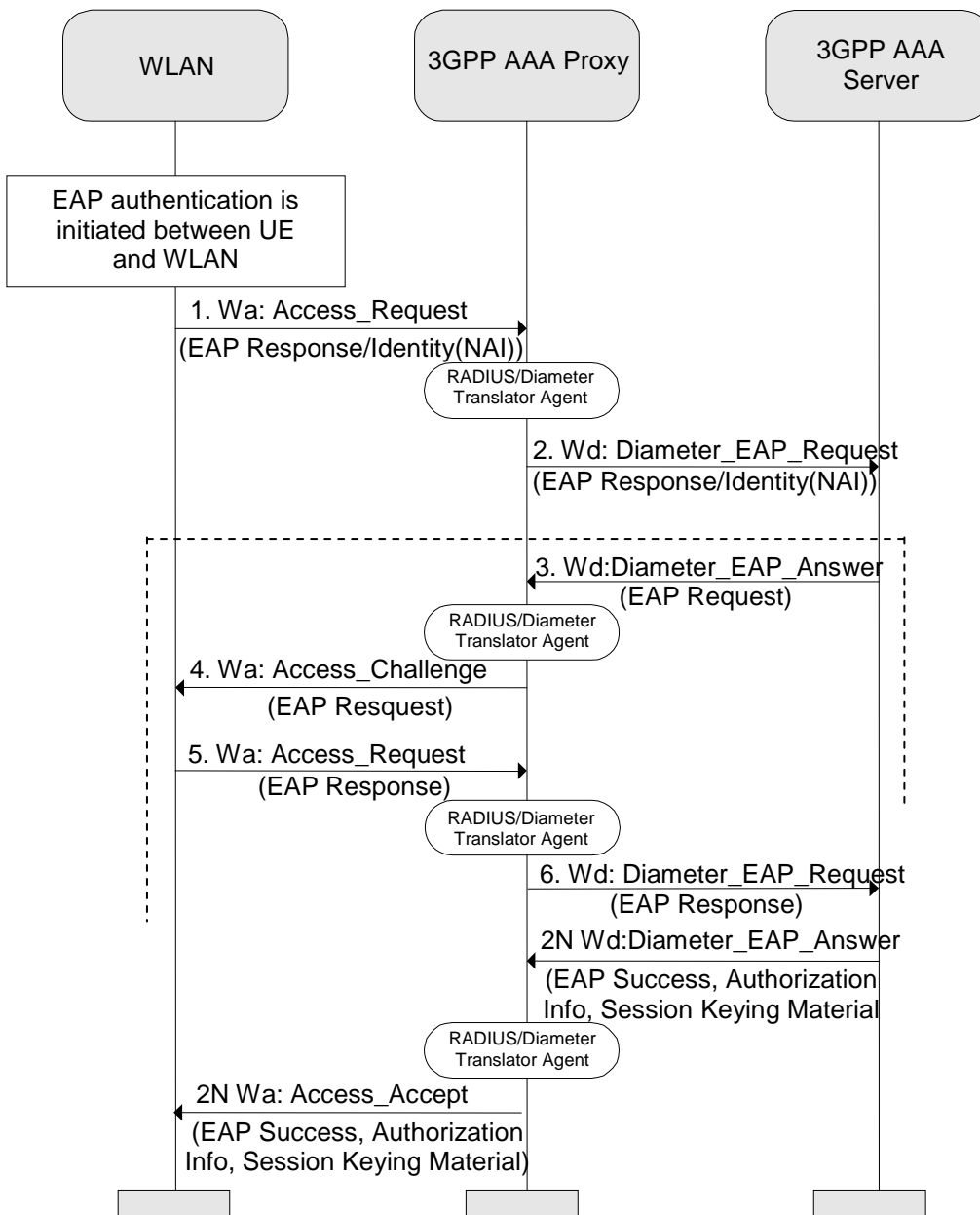
Figure A.1: Wa and Wd message flow for WLAN Session Authentication and Authorization Case a) Wa using RADIUS and Wd using Diameter
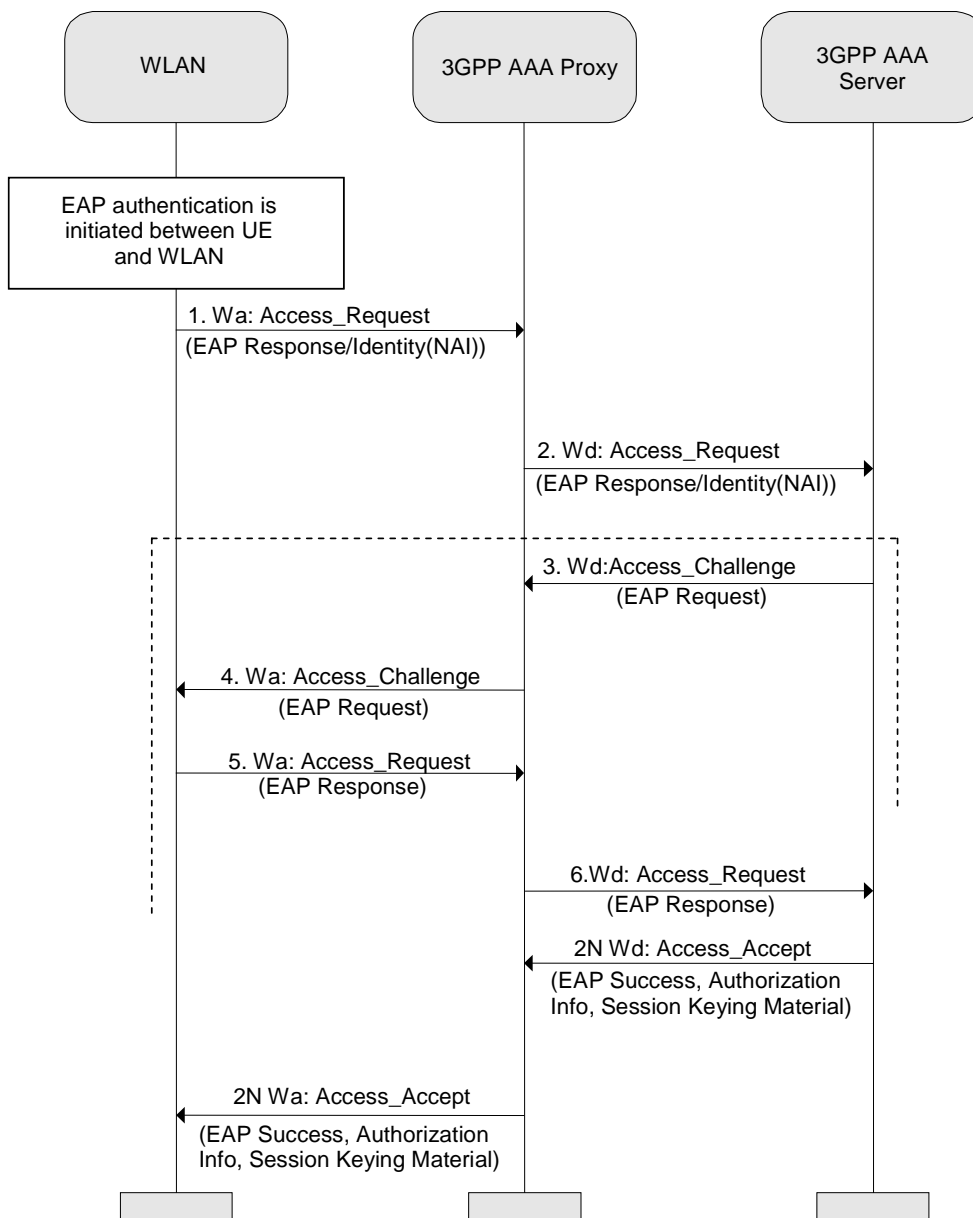
Figure A.2: Wa and Wd message flow for WLAN Session Authentication and Authorization Case b) Wa and Wd using RADIUS
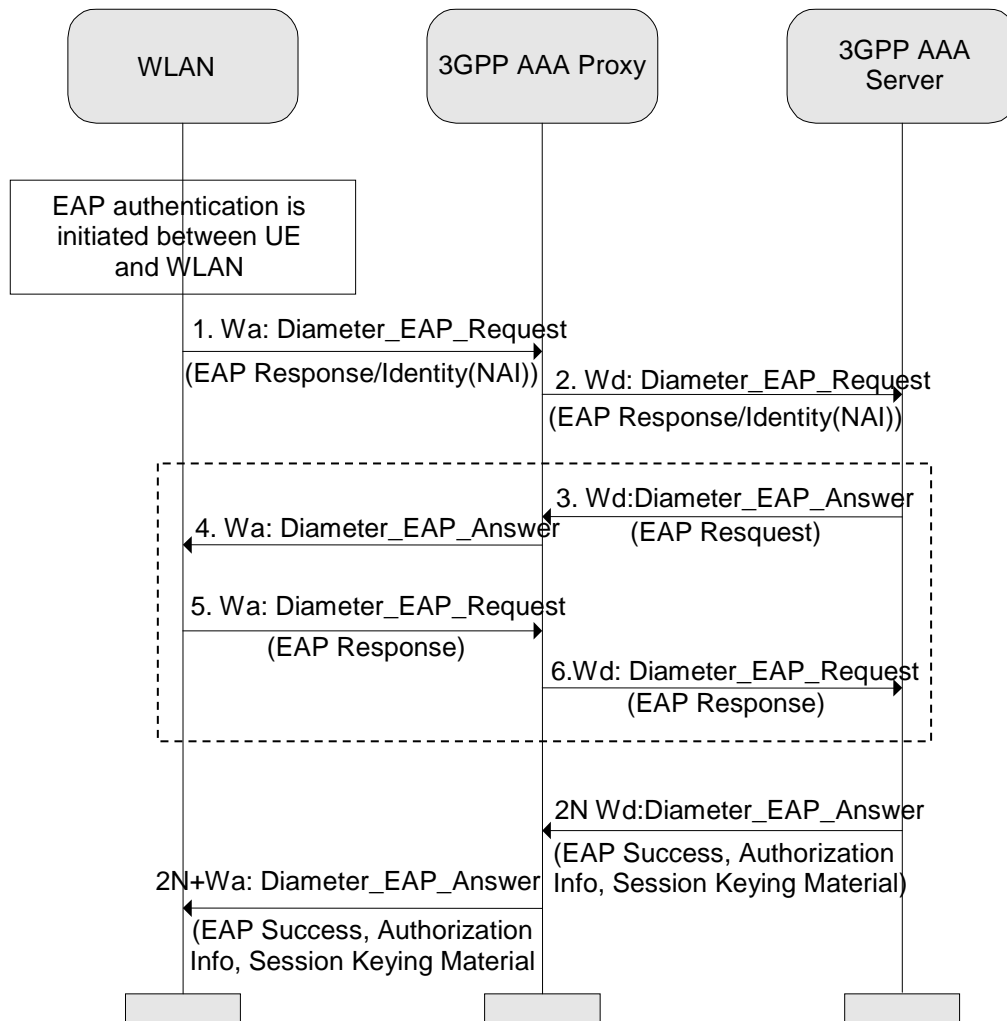
Figure A.3: Wa and Wd message flow for WLAN Session Authentication and Authorization Case c) Wa and Wd using Diameter

1. The WLAN AN initiates an authentication procedure towards the 3GPP network by sending to 3GPP AAA Proxy either:

   a) "Access_Request" message;

   b) "Diameter_EAP_Request" message.

The 3GPP AAA Proxy then sends to the 3GPP AAA Server either:

   a) "Access_Request" message;

   b) "Diameter_EAP_Request" message.

Both messages carry encapsulated EAP Response/Identity message to the 3GPP AAA Server. The message also carries a Session-ID used to identify the session within the WLAN AN.

2. The "Access_Request" message sent by the 3GPP AAA Proxy is generated due to the proxying by the 3GPP AAA Proxy of the "Access_Request" message originated in WLAN AN. The "Diameter_EAP_Request" message sent by 3GPP AAA Proxyis generated in the following two way:

   a) Conversion by the 3GPP AAA Proxy "Translator Agent" from the RADIUS "Access_Request" to "Diameter_EAP_Message";

   b) Proxying by the 3GPP AAA Proxy of the "Diameter_EAP_Message" originated in WLAN AN.

3. The 3GPP AAA Server performs the authentication procedure based on information retrieved from HSS/HLR. The 3GPP AAA Server sends to the 3GPP AAA Proxy either the message "Access_Challenge" if it received an "Access_Request" message or an "Diameter_EAP_Answer" " message if it received a "Diameter_EAP_Message". Both of these messages carry an encapsulated "EAP Request message". The content of the "EAP Request message" is dependent on the EAP type being used.

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

   a) Converts the "Diameter_EAP_Answer" message to "Access_Accept Message" by use of the RADIUS/Diameter "Translator Agent" and sends the "Access_Accept" to the WLAN AN;

   b) Proxyies the "Access_Challenge" or "Diameter_EAP_Answer" message to the WLAN AN.

The WLAN-AN then conveys the EAP Request message to the WLAN-UE.

5. The WLAN-UE responds to the WLAN AN by an EAP Response message. The WLAN AN encapsulates it into either:

   a) "Access_Request message" and sends it to 3GPP AAA Proxy;

   b) "Diameter_EAP_Request" message and sends it to 3GPP AAA Proxy.

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

   a) Converts the "Access_Request" to the "Diameter_EAP_Request" message by using the RADIUS/Diameter "Translator Agent" and sending one to the 3GPP AAA Server;

   b) Proxies the "Access_Request" message or "Diameter_EAP_Request" message to 3GPP AAA Server.

The contents of the EAP Response message are dependent on the EAP type being used.

The number of roundtrip Diameter signalling exchanges similar to the signals 3 to 6 is dependent e.g. on the EAP type being used.

2N. When the 3GPP AAA server has successfully authenticated the 3GPP subscriber, the 3GPP AAA Server sends to the 3GPP AAA Proxy a either an "Access_Accept" message, if it received an "Access_Request" or a Diameter_EAP_Answer message , if it received a "Diameter_EAP_Request". Both messages carry an encapsulated EAP Success message.

2N+1. The 3GPP AAA Proxy then acts in one of two ways:

   a) Conversion of the "Diameter_EAP_Answer" message to "Access_Accept" by the "Translator Agent" and sending one to the WLAN AN.

   b) Proxy the "Access_Accept" or "Diameter_EAP_Answer" message to the WLAN AN.

The WLAN AN then forwards the EAP Success message to the WLAN-UE.

This Diameter_EAP_Answer message also carries the authorization information (e.g. NAS Filter Rule or Tunnelling attributes) for the authenticated session. The message also carries the keying material from the 3GPP AAA Server to the WLAN AN to be used for the authenticated session by WLAN AN.

A.2 Immediate Purging of a WLAN User from the WLAN Access Network

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

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

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

The 3GPP AAA Proxy/Server manipulates the Root/Decorated/Alternative NAI as defined in 3GPP TS 23.003 [22].

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

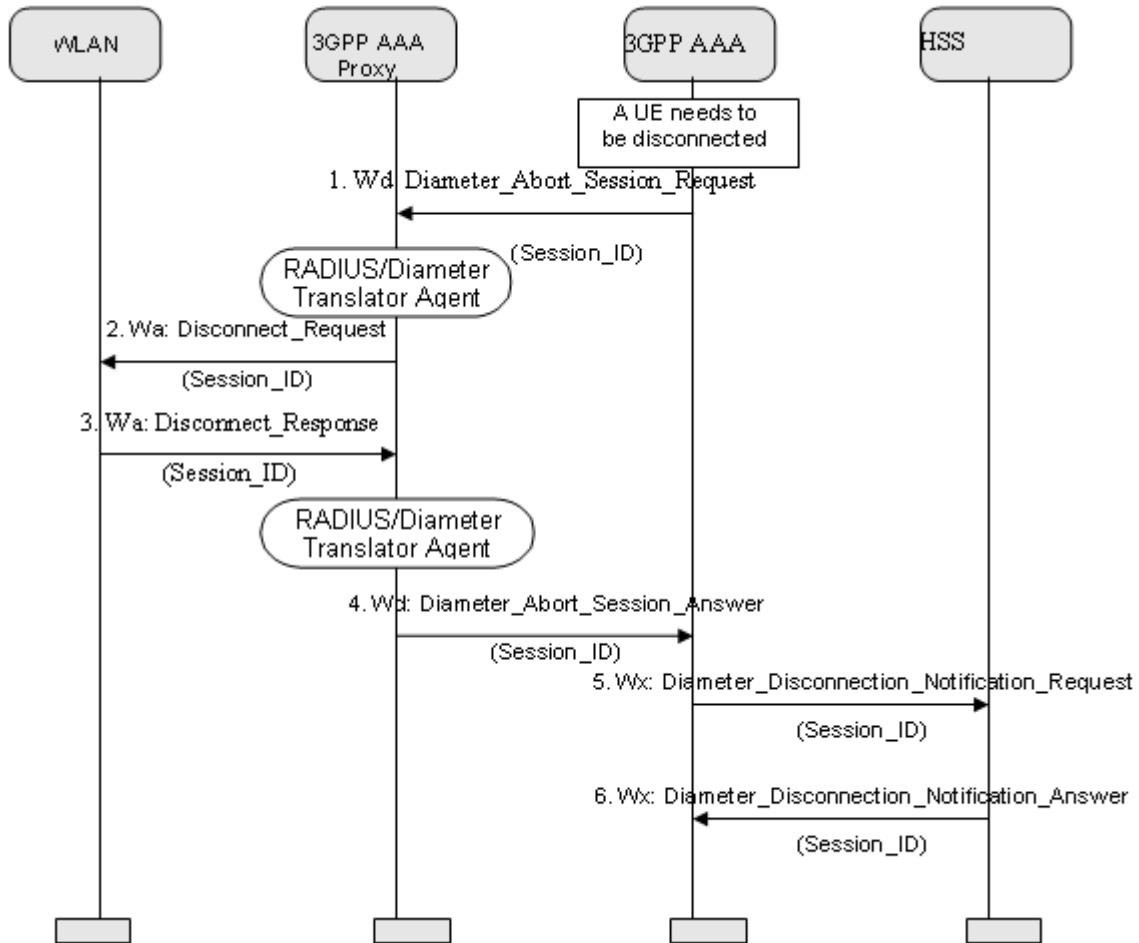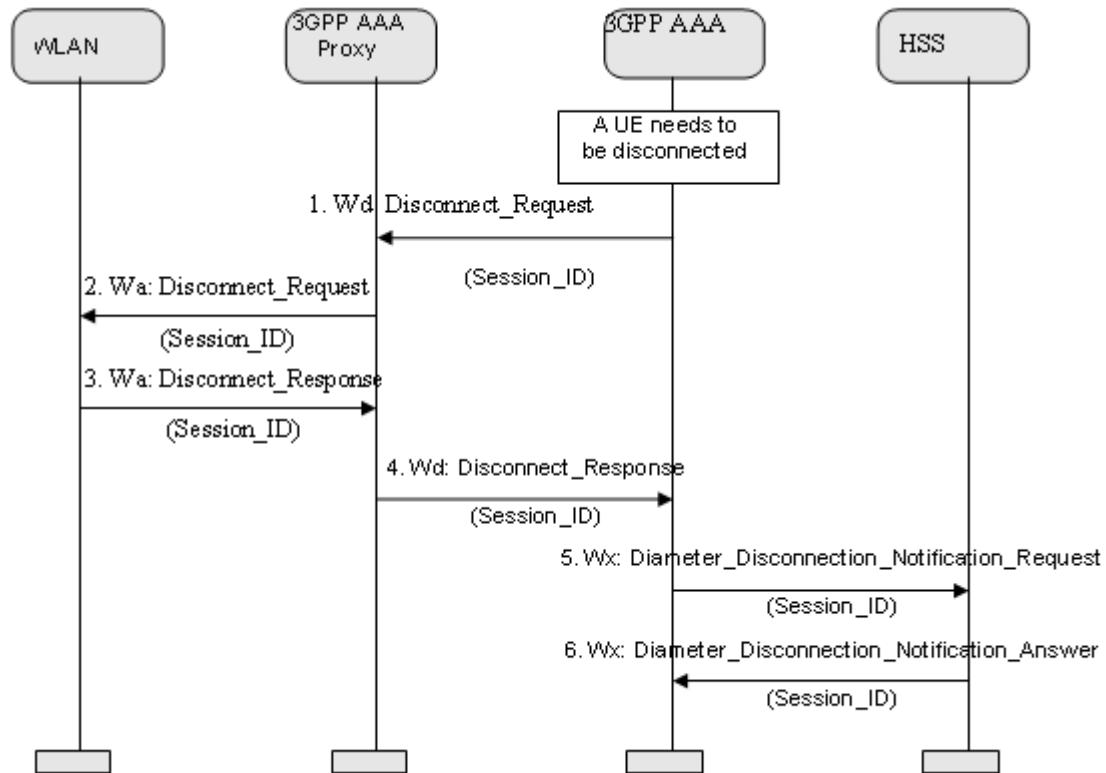**Figure A.5: Wa and Wd message flow for User Purging. Case b) Wa and Wd using RADIUS**
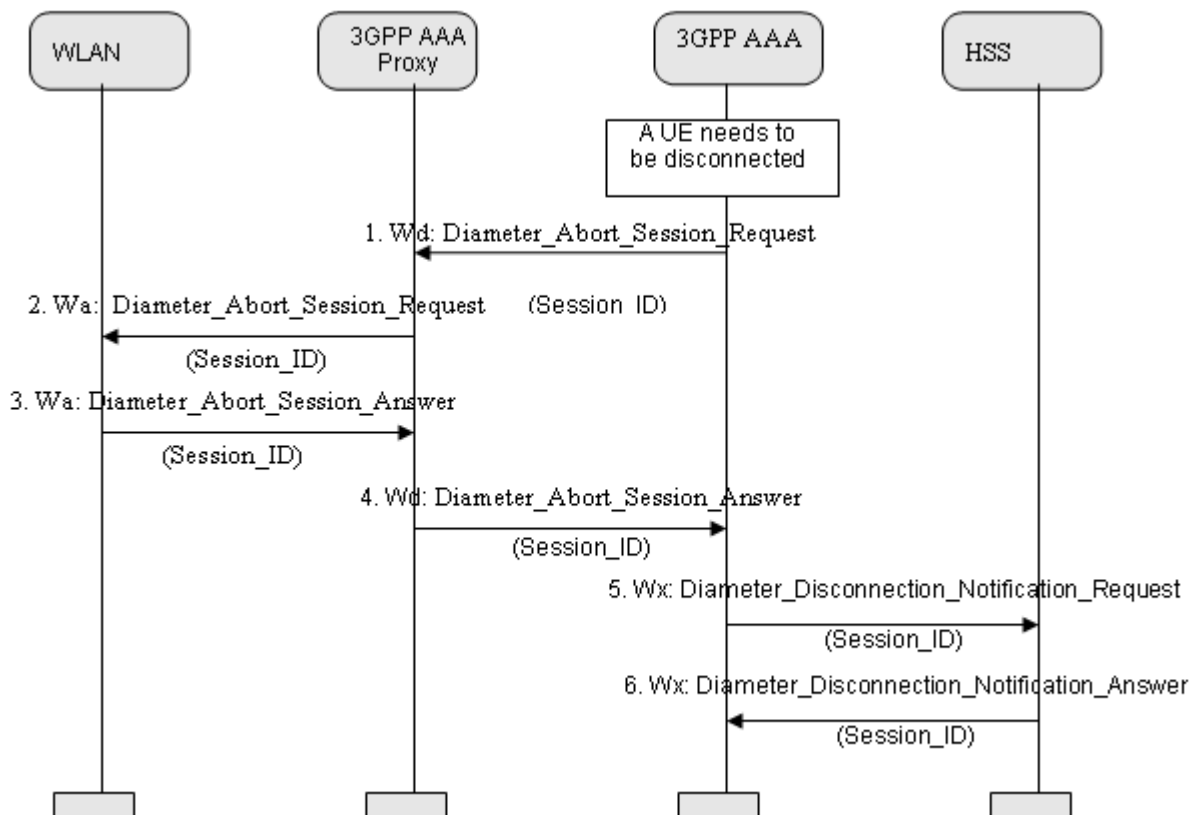

Figure A.6: Wa and Wd message flow for User Purging. Case c) Wa and Wd using Diameter

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

    a) "Disconnect_Request" message;

    b) "Diameter_Abort_Session_Request" message.

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

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

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

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

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

    a) "Disconnect_Response" message;

    b) "Diameter_Abort_Session_Answer" message.

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

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

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

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

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

Annex B (Informative):
Network configuration information

This Annex describes how an operator may configure its network in order to avoid problems associated with 3GPP AAA Server Redirect for the case where the Wa / Wd interfaces are implemented with RADIUS.

> NOTE: Since Diameter provides redirect functionality, no such problems exist once Diameter is adopted on these interfaces.

Four problem cases have been identified:

1. WLAN UE makes a WLAN Direct IP connection via a given WLAN AN, which is directed to a given 3GPP AAA Server. This is subsequently followed by e.g. a (re)authentication by the WLAN UE from the same WLAN AN. This is redirected to a different 3GPP AAA Server.

2. WLAN UE makes a WLAN Direct IP connection via a given WLAN AN, which is directed to a given 3GPP AAA Server. The WLAN UE then goes out of coverage and then tries to reconnect for WLAN Direct IP Access to a different WLAN AN. This is directed to a different 3GPP AAA Server.

3. WLAN UE makes a WLAN Direct IP connection via a given WLAN AN, which is directed to a given 3GPP AAA Server via a VPLMN. The WLAN UE then tries to activate a WLAN 3GPP IP Access to a PDG in the VPLMN. The Wm signalling is then proxied across the Wd interface by the 3GPP AAA Proxy to a different 3GPP AAA Server than that to which the user is registered for WLAN Direct IP access.

4. WLAN UE activates a WLAN 3GPP IP Access to a PDG in a VPLMN without having first made a WLAN Direct IP Access connection. The associated Wm signalling will be proxied across the Wd interface by the 3GPP AAA Proxy to a given 3GPP AAA Server in the HPLMN. The WLAN UE then performs reauthentication and the Wm signalling is proxied across the Wd to a different 3GPP AAA Server than that to which the user is registered.

In order to avoid cases (1), (3) and (4), it is recommended that the operator configures the network such that all incoming requests from a given external network are directed to the same 3GPP AAA Server

> NOTE: The external network in case (1) is the WLAN AN. In cases (3) and (4) it is the VPLMN.

Avoidance of case (2) is more problematic, since it cannot be known a priori from which WLAN AN the new attach request will come. To avoid this case, it is recommended that the operator configures the same 3GPP AAA Server to serve all geographically close WLAN ANs. Since this mitigates rather than solves the problem entirely, it is further recommended that the reauthentication timer is set to a low value (of the order of minutes) in order to avoid any hang time associated with old Direct IP connections.

Annex C (informative): Change history

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
09-2004	CN#25				Approved in CN#25	2.0.0	6.0.0
12-2004	CN#26	NP-040581	001	1	PLMN advertising and selection	6.0.0	6.1.0
			002		WLAN User Profile update		
			003		Charging related data from 3GPP AAA Server to PDG		
			004	1	3GPP WLAN IP Access parameter rename		
			005	1	Static Remote IP address		
			006		Removal of "Scenario" wording		
			007		Editorial correction on Auth-Req-Type AVP		
			008	1	Online charging failure report		
			009		Rejection of Multiple WLAN connections		
			010		Application-Ids to Wa, Wd, Wm and Wg		
			012	2	Wd Interface RADIUS profile clarifications		
			014	2	RADIUS Profile for Wa and Wd		
			015	1	Addition of ABNF definitions missing onWa, Wd Wm, Wg interfaces		
			016	1	Access Independence for WLAN 3GPP IP access		
			019	1	Editorial Modifications		
			021	1	Clarification on the reauthorization and reauthentication procedures in Wa chapter		
			021	1	To replace "Permanent User ID" by "User Id"		
			025	2	To make VPLMN-Id Conditional in Wd interface		
			026		Addition of calling station id in DEA. Deletion of the same from DER		
			028	1	Editorial Changes		
			029		Handling of Information Element marked as (M), (C) or (O)		
03-2005	CN#27	NP-050047	030	1	Removal of material duplicating 23.234 in 29.234	6.1.0	6.2.0
			031		Removal of Wn reference point Definition from the Stage 3		
			032		Wa Interface RADIUS profile corrections		
			033		Wd Interface RADIUS profile corrections		
			034	1	Removal of unnecessary attributes on Wa		
			035		Information Element corrections on Wd		
			037	1	Editorial corrections		
			038	1	Description of the RADIUS session termination procedure		
			039	1	WLAN Diameter AVP and result codes		
			041	1	WLAN Diameter AVP table and chapters coherence revision		
			042	2	PDG Behaviour on the Wm interface		
			043		Editorial corrections		
			047	1	Wa Interface RADIUS profile Information Element corrections		
06-2005	CT#28	CP-050196	049	1	Addition of missing functionality to Wa Interface RADIUS profile	6.2.0	6.3.0
			050	1	Addition of missing functionality to Wa Interface Diameter profile		
			051	2	Mandating RFC 3576 in WLAN-IW		
			052		Removal of Reference to User Data AVP on the Wm interface		
			053		Clean up of 29.234		
			054	1	Visited Network Identifier on the Wx interface		
			055		Reference to W-APN definition in 23.003		
			056	1	Clarifications on Wa and Wd RADIUS profiles		
			058	2	WAG address resolution on Wg interface		
			060	2	Missing functionality in stage 3		
			061	2	Pr Interface for Presence via I-WLAN		
			062	2	Limit on the number of session in WLAN 3GPP IP Access		
09-2005	CT#29	CP-050303	064		Clean up of Chapters 4 & 5	6.3.0	6.4.0
			065		Clarification of Location Management description in Section 6.3.2		
			066		Correction to handling of Maximum-Number-Accesses description		
			067	2	Clarifications to multiple sessions on the Wm interface		
			068	2	Correction to the utilization of the list of authorized visited network identifiers		
			070	1	Adding ABNFfor STA command		
			071	1	Update references for EAP lower layer attributes		
			072		IMSI handling at the PDG		

12-2005	CT#30	CP-050610	0073	1	Update of IETF references	6.4.0	6.5.0
			0074	1	IETF references update		
			0077	1	Updating the Routing Policy		
12-2005	CT#30				Rel-7 version was created because of ETSI TISPAN references.	6.5.0	7.0.0
03-2006	CT#31	CP-060073	0080		Adding definition of Maximum-Number-Accesses AVP and some other corrections	7.0.0	7.1.0
			0082		Transfer of Max-Requested-Bandwidth AVP over Wx reference point		
			0084	1	IETF references update		
			0086		Correction to Max-Requested-Bandwidth description in 29.234		
			0088	1	Correction to procedure for handling of Authorization Request in Wm interface		
06-2006	CT#32	CP-060309	0090	1	IETF References Update for RADIUS Filter Rules	7.1.0	7.2.0
			0092	2	Charging Identity Correction		
			0094	1	Diameter AVP naming correction		
			0101	1	The corrections to the usage of Master Session Key		
			0103	1	Handling of Redirects at 3GPP AAA Servers supporting only RADIUS on Wa/Wd		
09-2006	CT#33	CP-060406	0108		Removal of editor"s note about Pr ref. point	7.2.0	7.3.0
12-2006	CT#34	CP-060557	0110	2	Charging identifier exchange between 3GPP AAA Server and PDG	7.3.0	7.4.0
			0115		Correction to Charging Data handling over the Wx interface		
			0117	1	Correction to the Charging-Nodes AVP of the Wx interface		
			0119		The storing of 3GPP AAA server name and User Status handling		
			0122	1	IETF update on filtering		
			0124	1	IETF update on location information		
			0126	1	Identity usage correction on Wm		
			0113	1	Correct the Access and service Authorization information update procedure		
			0120	2	Modification of Wa interface to support emergency call case		
			0127	2	Modification of Wm interface to support emergency call case		
03-2007	CT#35	CP-070012	0130		Correction on location information on RADIUS Wd	7.4.0	7.5.0
		CP-070023	0132	1	Operator Determined Barring for I-WLAN		
		CP-070024	0133	3	QoS parameters definition and delivery		
06-2007	CT#36	CP-070311	0134	1	IETF References Update	7.5.0	7.6.0
09-2007	CT#37	CP-070526	0136		Correction of the PPR/PPA behavior	7.6.0	7.7.0
12-2007	CT#38	CP-070747	0137		QoS attributes correction	7.7.0	7.8.0
06-2008	CT#40	CP-080266	0139		Correction of Server Assignment Type	7.8.0	7.9.0
03-2009	CT#43	CP-090037	0143	1	User to HSS resolution	7.9.0	7.10.0
12-2009	CT#46	CP-090759	0145		IETF RFC 5580 Alignment	7.10.0	7.11.0
03-2010	CT#47	CP-100016	0150		NAI decoration and realm-based routing clarifications	7.11.0	7.12.0
06-2011	CT#52	CP-110347	0158	1	Clean up QSPEC references	7.12.0	7.13.0
06-2011	CT#52	CP-110346	0165		Alignment of AVP Codes	7.12.0	7.13.0
06-2011	CT#52	CP-110346	0169		Missing 3GPP-AAA-Server-Name AVP in MAA	7.12.0	7.13.0
12-2012	CT#58	CP-120709	0174		RADIUS Attributes Alignment	7.13.0	7.14.0
06-2013	CT#60	CP-130277	0181	1	Support of RFC 5080	7.14.0	7.15.0

History

Document history		
V7.0.0	December 2005	Publication
V7.1.0	March 2006	Publication
V7.2.0	June 2006	Publication
V7.3.0	September 2006	Publication
V7.4.0	December 2006	Publication
V7.5.0	March 2007	Publication
V7.6.0	June 2007	Publication
V7.7.0	October 2007	Publication
V7.8.0	January 2008	Publication
V7.9.0	July 2008	Publication
V7.10.0	April 2009	Publication
V7.11.0	January 2010	Publication
V7.12.0	April 2010	Publication
V7.13.0	June 2011	Publication
V7.14.0	January 2013	Publication
V7.15.0	June 2013	Publication