3GPP TSG-CN Meeting #25 **NP-040404**
8th – 10th September 2004. Palm Springs, USA

Source:	**TSG CN WG 4**
Title:	**3GPP System to Wireless Local Area Network WLAN Interworking; Stage 3**
Agenda item:	**9.17**
Document for:	**APPROVAL,- Draft technical specification 3GPP TS 29.234 v2.0.0**

Presentation of Technical Specification to TSG

Presentation to:	**TSG CN Meeting #25**
Document for presentation:	**TS 29.234, Version 2.0.0**
Presented for:	**Approval**

Abstract of document:
3GPP TS 29.234 defines the stage-3 protocol description for several reference points in the WLAN-3GPP Interworking System.

Outstanding Issues:

- Dependencies on acceptance in IETF of the following drafts: Diameter EAP, NASREQ, GEOPRIV, DIAMETER CREDIT CONTROL.
- Translation of Radius Ies defined in GEOPRIV to Diameter attributes.
- Whether a new Diameter application is required for authentication/authorization on Wa/Wd.
- ABNF missing on several interfaces.
- Online charging description missing.

Contentious Issues:

- None

3GPP TS 29.234 V2.0.0 (2004-09)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Core Network; 3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 3 (Release 6)

Keywords
3GPP, WLAN

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

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 Wn reference point between the WLAN AN and the 3GPP WAG.
- The Wp reference point between the 3GPP WAG and the PDG.
- The Wg reference point between the 3GPP AAA Server/Proxy and the WAG.

2 References

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

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

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

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

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

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

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

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

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

[8] IETF Draft: "Diameter Extensible Authentication Protocol (EAP) Application", draft-ietf-aaa-eap-06.txt, work in progress.

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

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

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

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

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

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

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

[16] IETF Draft, "Attributes for Access Network Location and Ownership Information"., work in progress .

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

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

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

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

3 Definitions, symbols and abbreviations

3.1 Definitions

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

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

3.2 Symbols

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

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

3.3 Abbreviations

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

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

4 Wa Description

The Wa reference point connects the WLAN AN, possibly via intermediate networks, to a 3GPP Network i.e. the 3GPP AAA Server when the WLAN AN in which the subscriber is currently located is directly connected to the home 3GPP network (also known as "the non-roaming case"), and the 3GPP AAA Proxy) when the WLAN AN is connected to the home 3GPP network through another 3GPP network (also known as "the roaming case"). The reference accommodates both legacy WLAN ANs of which use the RADIUS protocol, as well as future WLAN ANs which are expected to support Diameter.

4.1 Functionality

The functionality of the reference point is to transport:

- data for WLAN session authentication signalling between WLAN-UE and 3GPP Network;
- data for WLAN session authorization signalling between WLAN AN and 3GPP Network;
- keying data for the purpose of radio interface integrity protection and encryption;
- data for purging a user from the WLAN access for immediate service termination, when such functionality is supported by the WLAN AN;
- data to enable the identification of the operator networks within which roaming occurs;
- carrying accounting signalling per WLAN user.

4.2 Protocols

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

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

Therefore the Wa reference point shall contain the following protocols:

1) RADIUS, as defined in RFC 2865 [17], including the following extensions:
   - RFC 2869 [9], which provides RADIUS extensions to support the transport of EAP frames over RADIUS.

- IETF Draft "Attributes for Access Network Location and Ownership Information" [16], which provides RADIUS Extensions for Public WLAN [16] are also used in order to identify uniquely the owner and location of the WLAN.

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

2) Diameter Base, as defined in RFC 3588 [7], as well as IETF Draft " Diameter EAP Application", which [8] provides a Diameter application to support the transport of EAP (RFC 2284 [10] and IETF Draft "EAP" [11]) frames over Diameter.

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

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

4.3 Procedures Description

4.3.1 WLAN Access Authentication and Authorization

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

Diameter usage in Wa:

- This procedure is mapped to the Diameter-EAP-Request and Diameter-EAP-Answer command codes specified in [8] The Diameter-EAP-Request Message shall contain the following information elements.

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

Table 4.3.1.1: Authentication request

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

The Diameter-EAP response message shall contain the following.

Table 4.3.1.2: Authentication response

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

RADIUS usage in Wa:

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

See Annex A.1.1 for signalling flow reference.

4.3.2 Immediate Purging of a User from WLAN access

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

Diameter usage in Wa:

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

Table 4.3.2.1: Information Elements passed in ASR message

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

Table 4.3.2.2: Information Elements passed in ASA message

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

See Annex A.1.2 for signalling flow reference.

RADIUS usage in Wa:

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

4.3.3 Ending a Session

Session termination is initiated when the WLAN-AN needs to inform the 3GPP AAA Server of the WLAN-UEs disconnection from the hot-spot. This occurs via the Session Termination Request (STR) and Session Termination Answer commands (STA) from the base protocol [8]. Information elements to be carried in the STR, STA messages are shown in tables 4.4.3.1 and 4.4.3.2.

Table 4.3.3.1: Information Elements passed in STR message

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

Table 4.3.3.2: Information Elements passed in STA message

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

4.4 Information Element Contents

4.4.1 RADIUS based Information Elements Contents

Table 4.4.1: RADIUS based Information Elements Contents

IE NAME	IE description	Access Request	Access Accept	Access Reject	Access Challenge	Attribute
USER ID	This Attribute indicates the identity of the user to be authenticated. More detailed description of the IE can be found in RFC 3580 [15] and 3GPP TS 23.234 [4].	Mandatory	Mandatory	Mandatory	Mandatory	User-Name
RADIUS Client Address	This Attribute indicates the identifying IP Address of the RADIUS Client. It should be unique to the RADIUS Client within the scope of the RADIUS server. More detailed description of the IE can be found in RFC 3580 [15].	Mandatory	NA	NA	NA	NAS-IP Address
Operator Name	Hot Spot Operator Name as defined in [16].	Mandatory	NA	NA	NA	Operator Name
Location Name	Location Name of the hot spot operator as defined in [16].	Mandatory	NA	NA	NA	Location Name
Location Information	Location information regarding the hotspot operator as defined in [16].	Mandatory	NA	NA	NA	Location information
EAP Message	This attribute encapsulates Extensible Authentication Protocol packets so as to allow the NAS to authenticate users via EAP without having to understand the EAP protocol. More detailed description of the IE can be found in RFC 3580 [15].	Mandatory	Mandatory	Mandatory	Mandatory	EAP-Message
Diameter Session ID + 3GPP AAA Server Host AVP + prefix "Diameter"	This attribute is relayed from the 3GPP AAA Proxy to the WLAN-AN when the 3GPP AAA Proxy acts as translation agent. If the WLAN-AN receives such an attribute, it MUST include it in Access Requests.	Conditional	NA	NA	Conditional	State
Diameter Session ID + prefix "Diameter"	This attribute is sent by 3GPP AAA Proxy when acting as a translation agent. If WLAN-AN receives it, is should include it in subsequent accounting messages.	NA	Conditional	NA	NA	Class
Session Alive Time	This Attribute sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt. A more detailed description of the IE can be found in 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 RFC 2869 [9].	NA	Optional	NA	NA	Acct-Interim-Interval
Termination Action	This Attribute indicates what action the NAS should take when the specified service is completed. More detailed description of the IE can be found in RFC 3580 [15].	NA	Optional	NA	Optional	Termination-Action
Cryption Key	This Attribute is available to allow vendors to support their own extended Attributes not suitable for general usage. More detailed description of the IE can be found in RFC 3580 [15].	NA	Mandatory	NA	NA	Vendor-Specific (MS-MPPE-Send-Key)
Message Authenticator	Message Authenticator.	Mandatory	Mandatory	Mandatory	Mandatory	Message Authenticator
WLAN-UE MAC address	Carries the MAC address of the WLAN-UE for verification at the 3GPP AAA Server.	Mandatory	NA	NA	NA	Calling Station ID

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

4.4.2 Diameter based Information Elements Contents

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

4.4.2.1 DER and DEA Commands

ABNF for the DER and DEA messages are given below:

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

For the DEA, the following are necessary:

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

4.4.2.2 Session Termination Request and Answer AVPs

ABNF for the STR and STA commands are as follows:

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

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

4.4.2.3 Session Termination Request and Answer AVPs

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

4.5 Accounting Signalling Across the Wa interface

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

4.5.1 RADIUS

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

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

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

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

4.5.1.1 RADIUS Attributes in accounting messages

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

Table 4.5.1: RADIUS based Information Elements Contents

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

IE NAME	IE description	Accounting Request	Accounting Response	Attribute
Acc-Output-Packets	Indicates the number of packets received by the WLAN-UE over the course of the session. According to RFC 2866 [20], shall only be present if ACC Status Type is set to "Stop".	Optional	N/A	Acc-Output-Packets
Acc-Terminate-Cause	Indicates how the session was stopped. Cause values are as per specified in RFC 3580 [15].	Conditional. Shall be present if Acct-Status-Type set to "Accounting Stop".	N/A	Acc-Terminate-Cause

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

4.5.2 Diameter

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

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

4.5.2.1 Procedures Description

This procedure is used to transport over Diameter, the WLAN accounting specific information between the WLAN AN and the 3GPP AAA Proxy/Server.

Diameter usage in Wa:

- This procedure is mapped to the Diameter-Accounting Request and Accounting Response (ACR/ACA) command codes as defined in NASREQ [12]. The Diameter-ACR Message shall contain the following information elements.

Table 4.5.2.1: Accounting request

Information element name	Mapping to Diameter AVP	Cat.	Description
Username NAI	User-Name	M	This information element contains the identity of the user.
NAS-IP address	NAS-IP Address	C	IPv4 address of the hot-spot
NAS-Ipv6 address	NAS-Ipv6 address	C	IPv6 address of the hot-spot
Accounting Record type	Accounting Record type	M	2= Start, 4= Stop, 3= Interim Record
Accounting Session-ID	Accounting Session-ID	M	Uniquely Identifies the accounting session. May be the same Session-ID as for the authentication signalling over the Wa
Accounting-Input-Octets	Accounting-Input-Octets	O	Number of octets sent by the WLAN UE
Accounting-Output-Octets	Accounting-Output-Octets	O	Number of octets received by the WLAN UE
Accounting-Input-Packets	Accounting-Input-Packets	O	Number of packets sent by the WLAN UE
Accounting-Output-Packets	Accounting-Output-Packets	O	Number of packets received by the WLAN UE
Accounting-Session-Time	Accounting-Session-Time	C	Indicates the length of the current session in seconds. Shall only be present if Accounting-Record-Type is set to Stop or Interim
Termination-Cause	Termination-Cause	C	Shall be present only if Accounting-Record-Type is set to Stop.

The Diameter-Accounting response message shall contain the following.

Table 4.5.2.2: Accounting response

Information element name	Mapping to Diameter AVP	Cat.	Description
Username NAI	User-Name	M	This information element contains the permanent identity of the user, i.e. the IMSI.
Result code	Result Code	M	Result of the operation. Result codes are as per in NASREQ. 1xxx should be used for multi-round, 2xxx for success.

5 Wd Description

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

5.1 Functionality

The functionality of the reference point is to transport:

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

5.2 Protocols

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

The Wd protocol reference point shall contain the following protocols:

1) RADIUS, as defined in RFC 2865 [17], including the following extensions:
   - RFC 2869 [9], which provides RADIUS extensions to support the transport of EAP frames over RADIUS.
   - IETF Draft "Attributes for Access Network Location and Ownership Information" [16], which provides RADIUS Extensions for Public WLAN are to identify uniquely the owner and location of the WLAN.
   - RFC 3576 [13], which provides RADIUS extensions to supports, amongst other capabilities, the capability to immediately disconnect a user from the WLAN AN.
2) Diameter Base, as defined in RFC 3588 [7], as well as IETF Draft "Diameter EAP Application" [8], which provides a Diameter application to support the transport of EAP (RFC 2284 [10] and IETF Draft "EAP" [11]) frames over Diameter. In addition, Diameter Base (RFC 3588 [7]) and NASREQ [12] specify the accounting messaging to be exchanged.

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

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

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

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

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

If the Wd reference point uses RADIUS then:

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

If the Wd reference point uses Diameter then:

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

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

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

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

If the Wd reference point is using RADIUS then:

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

If the Wd reference point is using Diameter then:

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

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

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

A RADIUS/Diameter Translation Agent has the following requirements:

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

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

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 [12].

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

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 [12].

If the Diameter Response contains EAP frames, additional actions described in [8] are taken by the 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.

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 [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 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 [12]:

- RADIUS Identifier Field in the RADIUS-Request as described in 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 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 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 [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 over Diameter.

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

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

Table 5.4.1.1: Diameter EAP Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Username NAI	User Name	M	This information element shall contain the identity of the user
EAP payload	EAP payload	M	Encapsulated EAP payload used for UE-3GPP AAA Server mutual authentication
Authentication Request Type	Auth Req Type	M	Defines whether authentication or authentication procedure is requested. AUTHENTICATE_ONLY is required in this case.
NAS-IP address	NAS-IP Address	C	IP address of the hot-spot
NAS-Ipv6 address	NAS-Ipv6 address	C	Ipv6 address of the hot-spot
Visited-Network-Identifier	Visited-Network-Identifier	M	Identifies the VPLMN

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

Table 5.4.1.2: Diameter EAP answer message

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

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 based.

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

5.4.3 Ending a Session

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

5.5 Information Elements Contents

FFS

6 Wx Description

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

6.1 Functionality

The functionality of the reference point is to enable:

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

6.2 Protocols

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

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

6.3 Procedures Description

6.3.1 Authentication Procedures

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

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

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

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

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

Table 6.3.1.1: Authentication request

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element contains the permanent identity of the user, i.e. the IMSI.
Visited Network Identifier	Visited-Network-Identifier	M	Identifier that allows the home network to identify the Visited Network. Editor's note: See 3GPP TS 29.229 [6] for a description of this parameter
Number Authentication Items	SIP-Number-Auth-Items	M	This information element indicates the number of authentication vectors requested
Authentication Data	SIP-Auth-Data-Item	C	See tables 6.3.1.2 and 6.3.1.3 for the contents of this information element. The content shown in table 6.3.1.2 shall be used for a normal authentication request; the content shown in table 6.3.1.3 shall be used for an authentication request after synchronization failure.
Routing Information	Destination-Host	C	If the 3GPP AAA Server knows the HSS name, this AVP shall be present. This information is available if the 3GPP AAA Server already has the HSS name stored. The HSS name is obtained from the Origin-Host AVP, which is received from the HSS, e.g. included in the MAA command. Otherwise only the Destination-Realm is included so that it is resolved to an HSS address in an SLF-like function. Once resolved the Destination-Host AVP is included with the suitable HSS address and it is stored in the 3GPP AAA Server for further usage.

Table 6.3.1.2: Authentication Data content - request

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

Table 6.3.1.3: Authentication Data content - request, synchronization failure

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

Table 6.3.1.4: Authentication answer

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

Table 6.3.1.5: Authentication Data content - response

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

6.3.1.1 Detailed behaviour

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

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

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

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

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

5. If the request indicates there is a synchronization failure, the HSS shall compare the 3GPP AAA Server name received in the request to the 3GPP AAA Server name stored in the HSS:

   - If they are identical, the HSS shall process AUTS as described in 3GPP TS 33.203 [3] and return the requested authentication information. The Result-Code shall be set to DIAMETER_SUCCESS.

6. The HSS shall store the 3GPP AAA Server name. The HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The Result-Code shall be set to DIAMETER_SUCCESS.

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

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

6.3.2 Location Management Procedures

6.3.2.1 WLAN Registration/DeRegistration Notification

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

- Registration of the 3GPP AAA Server of an authorized WLAN user in the HSS.

- Retrieval of online charging / offline charging function addresses from HSS.

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

- Retrieval of WLAN subscriber profile from HSS.

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

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

- To de-register the current 3GPP AAA Server address in the HSS for a given 3GPP user. When WLAN WLAN-UE has disappeared from WLAN coverage or when the OCS has initiated a disconnection, the 3GPP AAA Server informs the HSS about an ongoing disconnection process and the HSS de-registers the WLAN user.

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

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

Table 6.3.2.1: WLAN Registration request

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element contains the permanent identity of the user, i.e. the IMSI.
Server Assignment Type	Server-Assignment-Type	M	Type of procedure the 3GPP AAA Server requests in the HSS. When this IE contains REGISTRATION value, the HSS performs a registration of the WLAN user. When this IE contains USER_DEREGISTRATION / ADMINISTRATIVE_DEREGISTRATION / REAUTHENTICATION_FAILURE / ONLINE_CHARGING_FAILURE the HSS performs a de-registration of the WLAN user. When this IE contains NO_ASSIGNMENT value, the HSS initiates the download of the subscriber user profile towards the 3GPP AAA Server, but no registration is performed. Any other value is considered as an error case.
Routing Information (See clause 7.13)	Destination-Host	C	If the 3GPP AAA Server knows the HSS name this AVP shall be present. This information is available if the 3GPP AAA Server already has the HSS name stored. The HSS name is obtained from the Origin-Host AVP, which is received from the HSS, e.g. included in the MAA command. Otherwise only the Destination-Realm is included so that it is resolved to an HSS address in an SLF-like function. Once resolved the Destination-Host AVP is included with the suitable HSS address and it is stored in the 3GPP AAA Server for further usage.

Table 6.3.2.2: Subscriber profile retrieval response

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	Permanent-User-Identity	M	This information element contains the permanent identity of the user, i.e. the IMSI.
Registration result	Result-Code / Experimental-Result	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Wx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
User Profile	User-Data	C	Relevant user profile. It shall be present when Server-Assignment-Type in the request is equal to NO_ASSIGNMENT.
Charging Information	Charging-Information	C	Addresses of the charging functions. It shall be present when Server-Assignment-Type in the request is equal to REGISTRATION and when Result-Code is equal to DIAMETER_SUCCESS. When this parameter is included, the Primary Charging Collection Function address shall be included. All other elements shall be included if they are available.

6.3.2.1.1 Detailed behaviour

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

The 3GPP AAA server sends Server-Assignment-Request command to the HSS indicating the registration procedure. The subscriber is identified by the User-Name AVP.

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

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

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

   - If it indicates REGISTRATION, the HSS shall store the 3GPP AAA Server name for the authenticated and authorized 3GPP subscriber.

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

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

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

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

6.3.2.2 Network Initiated De-Registration by HSS, Administrative

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

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

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

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

Table 6.3.2.3: Network Initiated Deregistration by HSS request

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element contains the permanent identity of the user, i.e. the IMSI.
Reason for de-registration	Deregistration-Reason	M	The HSS shall send to the 3GPP AAA server a reason for the de-registration. The de-registration reason is composed of two parts: one textual message (if available) that is intended to be forwarded to the user that is de-registered, and one reason code (see 3GPP TS 29.229 [6]) that determines the behaviour of the 3GPP AAA Server.
Routing Information	Destination-Host	M	The 3GPP AAA server name is obtained from the Origin-Host AVP, which is received from the 3GPP AAA Server, e.g. included in the MAR command.

Table 6.3.2.4: Network Initiated Deregistration by HSS response

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

6.3.2.2.1 Detailed behaviour

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

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

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

6.3.3 User Data Handling

FFS

6.3.3.1 User Profile Download

FFS

6.3.3.2 HSS Initiated Update of User Profile

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

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

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

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

Table 6.3.3.1: User Profile Update request

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element contains the permanent identity of the user, i.e. the IMSI.
User profile	User-Data	M	Updated user profile. Editor's note: The format of the user profile is for further study.
Routing Information	Destination-Host	M	The 3GPP AAA Server name is obtained from the Origin-Host AVP, which is received from the 3GPP AAA Server, e.g. included in the MAR command.

Table 6.3.3.2: User Profile Update response

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

6.3.3.2.1 Detailed behaviour

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

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

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

Table 6.3.3.3: User profile response valid result codes

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

6.4 Information Elements Contents

6.4.1 Authentication Procedures

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

Message Format

```
< Multimedia-Authentication-Request > ::= < Diameter Header: 303, YYYY, REQ >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    [ Destination-Host ]
    { User-Name}
    { Visited-Network-Identifier}
    [ SIP-Auth-Data-Item ]
    [ SIP-Number-Auth-Items ]
    * [ AVP ]
    * [ Proxy-Info ]
    * [ Route-Record ]
```

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

Message Format

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

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, YYYY, REQ >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Host }
    { Destination-Realm }
    { User-Name}
    [ WLAN-User-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 x.x in addition to the values defined in RFC 3588 [7].

```
< Push-Profile-Answer > ::=< Diameter Header: 305, YYY >
    < 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, YYY, REQ, PXY >
    < 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 in addition to the values defined in RFC 3588 [7].

Message Format

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

6.5.1 Permanent Failures

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

6.5.1.1 DIAMETER_ERROR_USER_NO_SERVICE_SUBSCRIPTON (500x)

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

6.5.1.2 DIAMETER_ERROR_AUTH_METHOD_UNSUPPORTED (500x)

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

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

6.5.1.3 DIAMETER_ERROR_W-APN_UNUSED_BY_USER

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

6.6 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.

7 Wn Description

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

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

8 Wm Description

8.1 Functionality

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

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

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

8.2 Protocols

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

8.3 Procedures Description

8.3.1 Authentication Procedures

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

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

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

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

Table 8.3.1.1: Authentication Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element contains the permanent identity of the user, i.e. the IMSI.
EAP payload	EAP payload	M	Encapsulated EAP payload used for UE - 3GPP AAA Server mutual authentication
Authentication Request Type	Auth Req Type	M	Defines whether authentication only or authentication and authorization are required. AUTHENTICATION_ONLY is required in this case
Visited Network Identifier	Visited-Network-Identifier	C	Identifier that allows the home network to identify the Visited Network. This AVP shall be present if the PDG is not in the WLAN-UE's home network i.e. the WLAN-UE is roaming.

Table 8.3.1.2: Authentication Answer

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

8.3.1.1 3GPP AAA Server Detailed Behaviour

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

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

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

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

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

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

8.3.1.2 3GPP AAA Proxy Detailed Behaviour

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

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

8.4 Procedures Description

8.4.1 Authorization Procedures

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

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

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

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

Table 8.4.1.1 Wm Authorization Request

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

Table 8.4.1.2: AA-Response

Information element name	Mapping to Diameter AVP	Cat.	Description
Registration Result	Result Code/ Experimental Result Code	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. **Experimental-Result AVP shall be used for Wm errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP**
Subscription-ID AVP	Subscription-ID AVP	C	This AVP shall contain the MSISDN of the user. This AVP shall be present is the Diameter Result Code is set to DIAMETER_SUCCESS
Max-Subscribed-Bandwidth	Max-Requested-Bandwidth	O	The Max requested bandwidth AVP. Can be sent by the 3GPP AAA Server to the PDG if it is present in the user subscription info held at the 3GPP AAA Server.

8.4.1.1 3GPP AAA Server Detailed Behaviour

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

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

2) Check the Session-Request-Type AVP:

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

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

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

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

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

     - The 3GPP AAA Server shall download APN-User-Data AVP. The Result-Code shall be set to DIAMETER_SUCCESS.

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

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

8.4.1.2 AAA Proxy Detailed Behaviour

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

Check the Request Type AVP:

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

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

2) If Request-Type indicates ROUTING POLICY:

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

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

8.5 PDG Initiated Session Termination Procedure

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

Table 8.5.1: Session Termination Request

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

Table 8.5.2: Session Termination Answer

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

8.5.1 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.

8.5.2 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.

8.6 3GPP AAA Server Initiated Tunnel Disconnect Procedure

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

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

Table 8.6.1: 3GPP AAA Server Initiated Tunnel Disconnection - Request

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

Table 8.6.2: 3GPP AAA Server Initiated Tunnel Disconnection - Answer

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

8.6.1 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.

8.6.2 3GPP AAA Proxy Behaviour

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

9 Wg Description

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

9.1 Functionality

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

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

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

9.2 Protocols

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

9.3 Procedures Description

9.3.1 Policy Download Procedures

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

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

Table 9.3.1.1: Wg Policy Download Request

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

Table 9.3.1.2: Wg Policy Download Response

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

9.3.1.1 WAG Detailed Behaviour

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

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

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

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

9.4 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 9.4.1: 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 9.4.2: 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.

9.4.1 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.

9.5 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 9.5.1: 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 9.5.2: 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.

9.5.1 Detailed Behaviour

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

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

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

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

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

10 Information Elements Contents

10.1 AVPs

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

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

Table 10.1.1: Diameter Multimedia Application AVPs

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

10.1.1 Auth-Session-State

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

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

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

10.1.2 User-Name

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

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

10.1.3 Visited-Network-Identifier

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

10.1.4 SIP-Auth-Data-Item

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

AVP format

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

10.1.5 Authentication-Method

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

WLAN_EAP_SIM (0)

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

WLAN_EAP_AKA (1)

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

10.1.6 Authentication-Information-SIM

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

10.1.7 Authorization -Information-SIM

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

10.1.8 WLAN-User-Data

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

AVP format

```
WLAN-User-Data::= <AVP header: TBD>
    [ MSISDN ]
    { WLAN-Access }
    { WLAN-Tunneling }
    [ Session-Timeout ]
    1* { Charging-Data  }
    *[ APN-Authorized ]
    { Local-Access }
    * [AVP]
```

10.1.9 MSISDN

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

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

10.1.10 Charging-Information

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

10.1.11 WLAN-Access

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

WLAN_SUBSCRIPTION_ALLOWED (0)

- The subscriber has WLAN subscription.

WLAN_SUBSCRIPTION_BARRED (1)

- The subscriber has no WLAN subscription.

10.1.12 WLAN-Tunnelling

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

WLAN_ APNS _ENABLE (0)

- Enable all APNs.

WLAN_ APNS _DISABLE (1)

- Disable all APNs.

10.1.13 Session-Timeout

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

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

10.1.14 APN-Authorized

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

AVP format

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

10.1.15 APN-Id

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

10.1.16 APN-Authorization

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

WLAN_ APN_HOME (0)

- Access is allowed in home PLMN only.

WLAN_ APN_VISITED (1)

- Access is allowed in visited PLMNs and home PLMN.

10.1.17 Local-Access

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

WLAN_LOCAL_ACCESS (0)

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

WLAN_NO_LOCAL_ACCESS (1)

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

10.1.18 Server-Assignment-Type

The Server-Assignment-Type AVP (AVP code 15) is defined in 3GPP TS 29.229 [6] and indicates the type of procedure the 3GPP AAA Server is asking to the HSS.

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

10.1.19 Deregistration-Reason

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

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

10.1.20 EAP-Payload

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

10.1.21 Auth Req Type

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

10.1.22 EAP-Master-Session-Key

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

10.1.23 Session-Request-Type

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

AUTHORIZATION REQUEST (0)

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

ROUTING POLICY (1)

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

10.1.24 Routing-Policy

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

Editor's Note: Its exact format is ffs.

10.1.25 Subscription-ID

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

WLAN shall make use only of the value MSISDN.

10.1.26 Max-Requested-Bandwidth

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

10.1.27 Routing Policy

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

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

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

The IPFilterRule type shall be used with the following restrictions:

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

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

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

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.

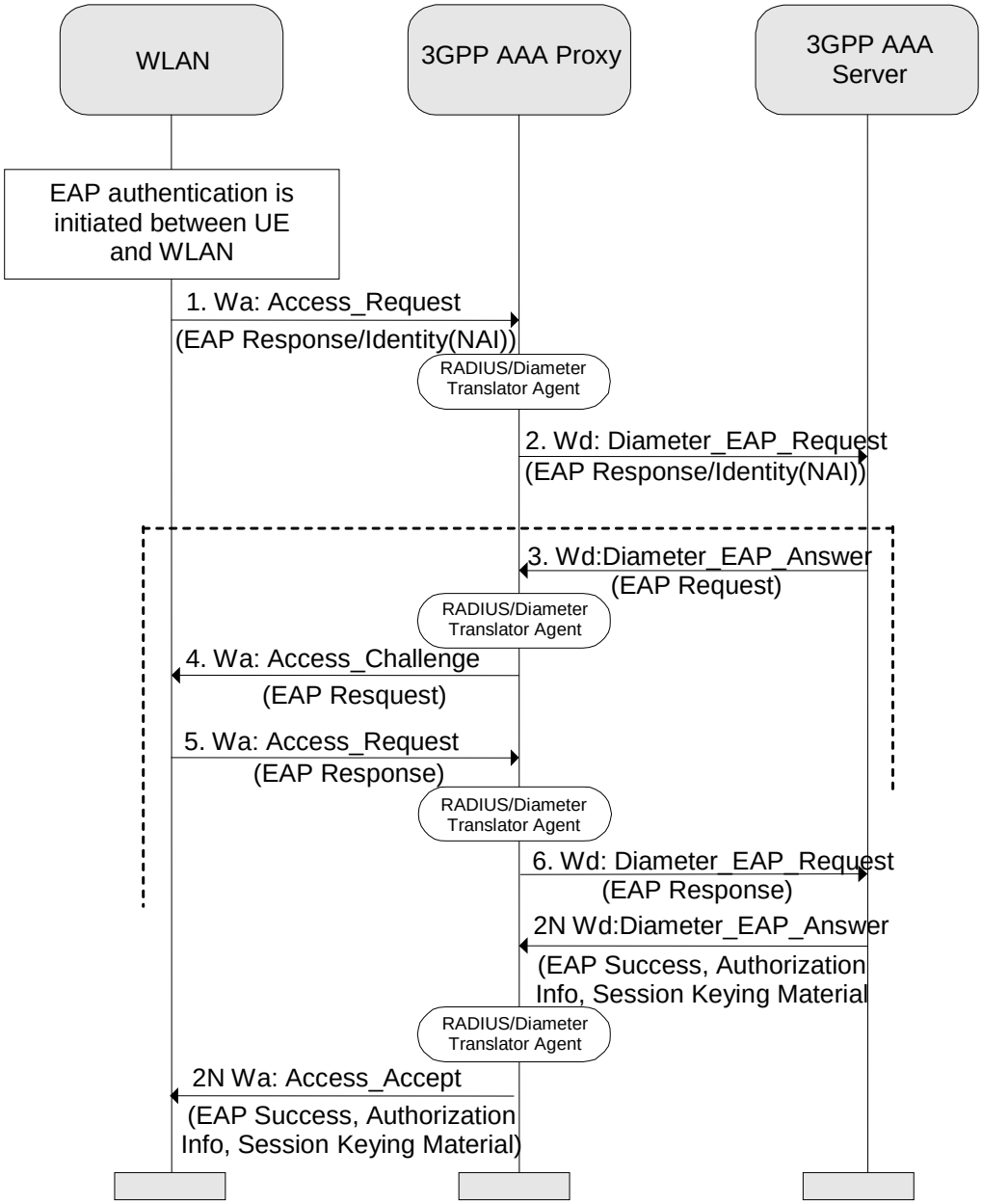

Figure A.1: Wa and Wd message flow for WLAN Session Authentication and Authorization Case a) Wa using RADIUS and Wd using Diameter

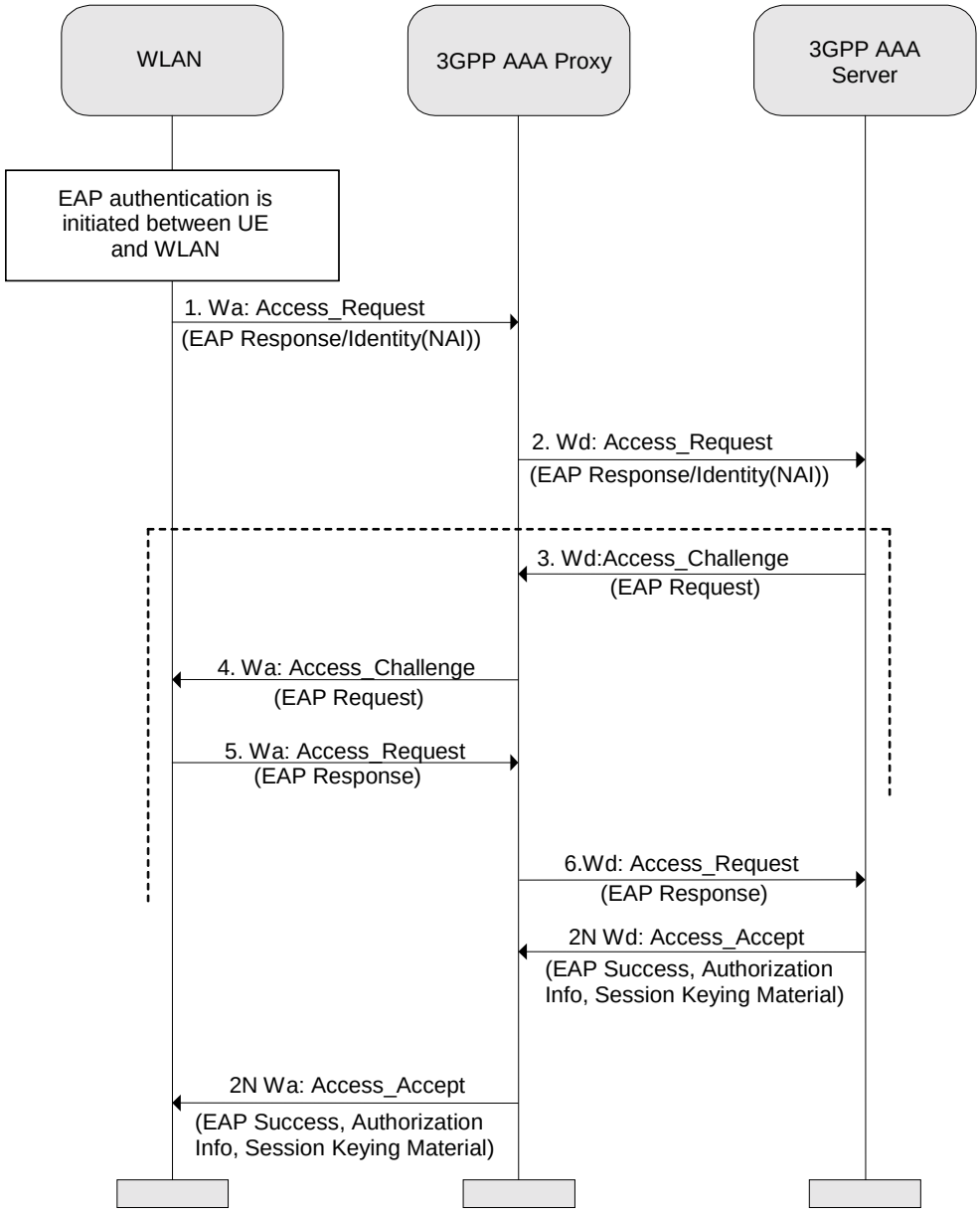

Figure A.2: Wa and Wd message flow for WLAN Session Authentication and Authorization Case b) Wa and Wd using RADIUS

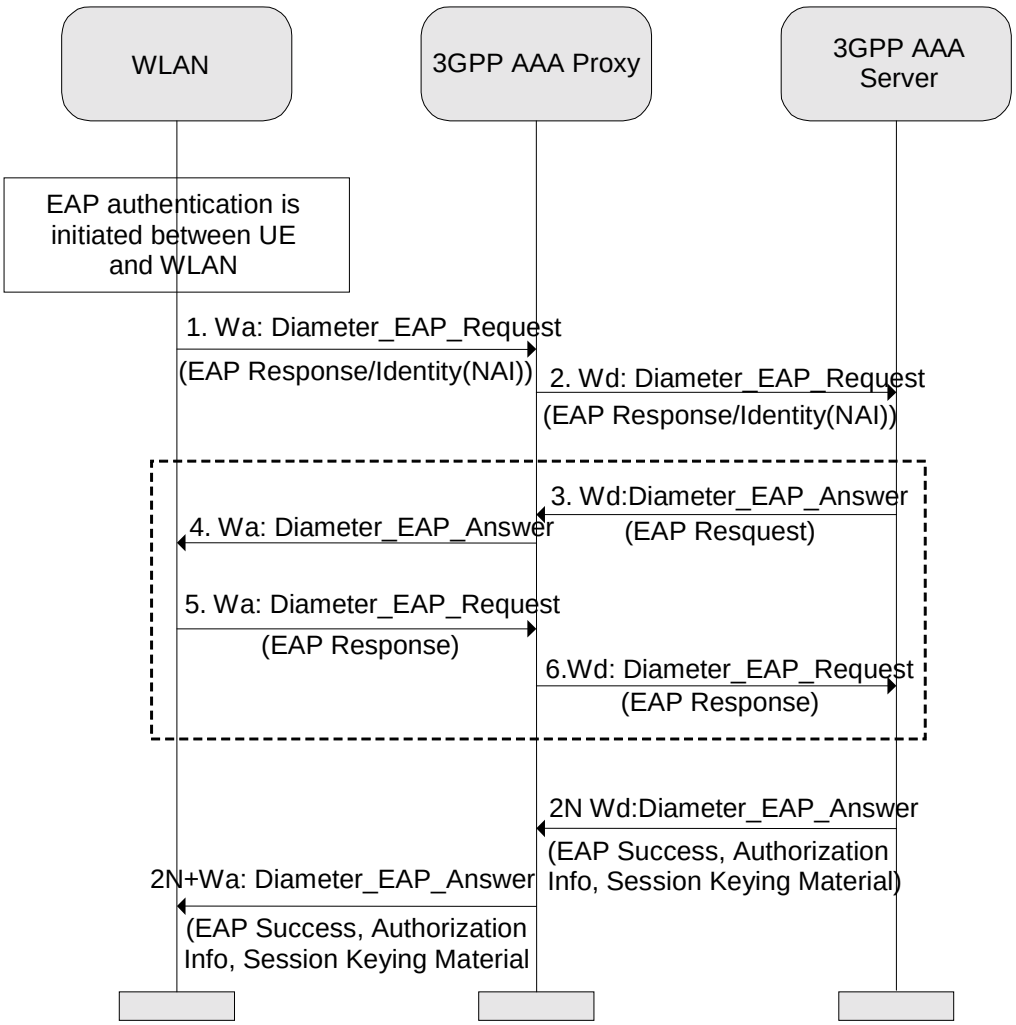

Figure A.3: Wa and Wd message flow for WLAN Session Authentication and Authorization Case c) Wa and Wd using Diameter

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 sequencies 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 sequence 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.

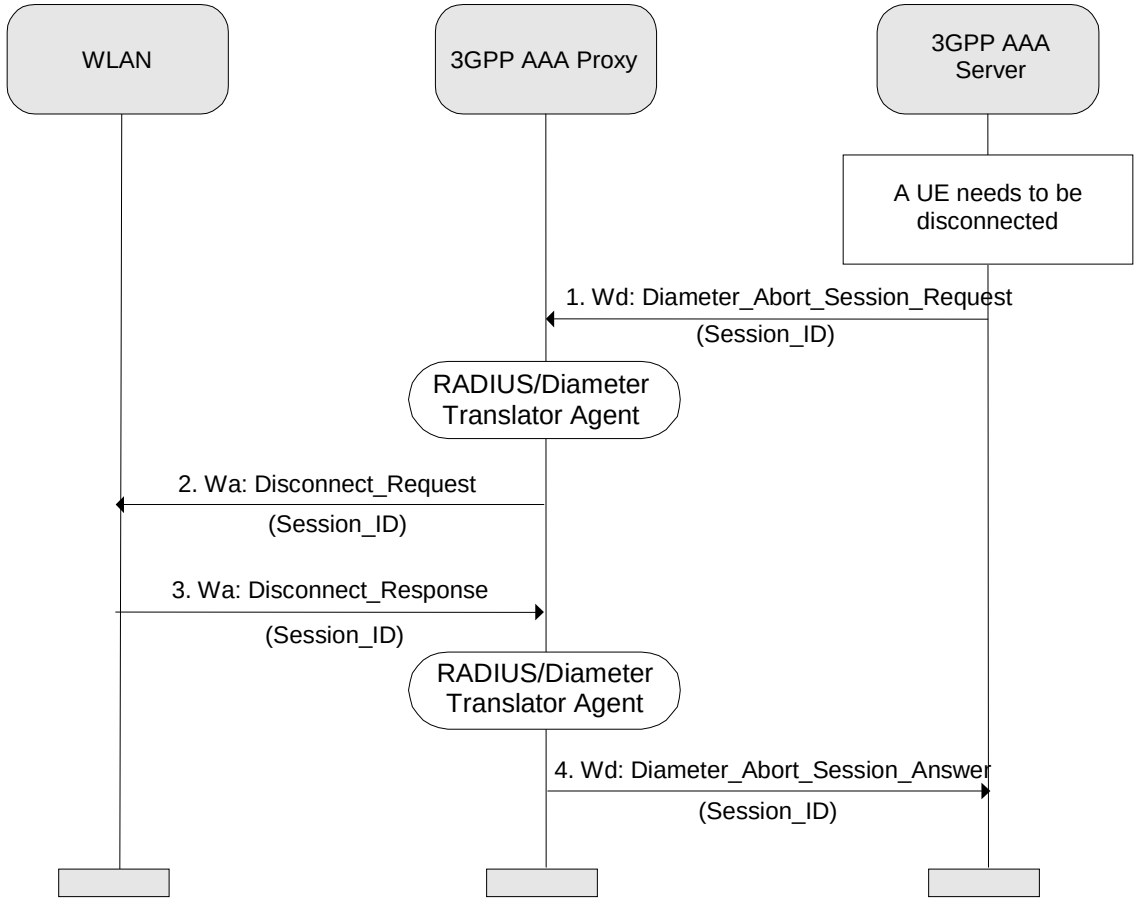

Figure A.4: Wa and Wd message flow for User Purging
Case a) Wa using RADIUS and Wd using Diameter

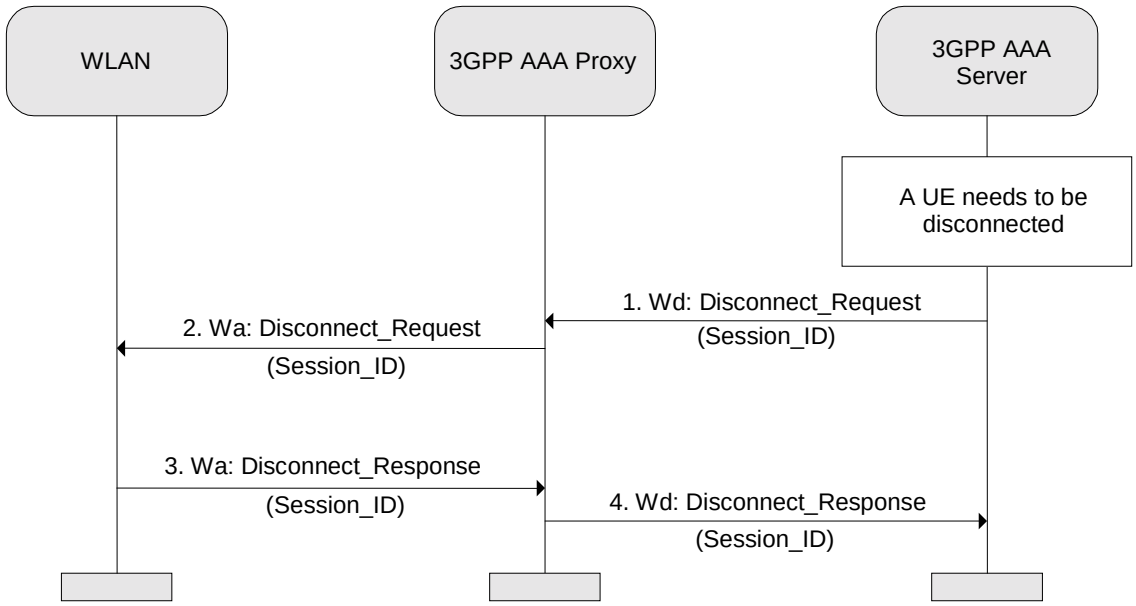

Figure A.5: Wa and Wd message flow for User Purging
Case b) Wa and Wd using RADIUS

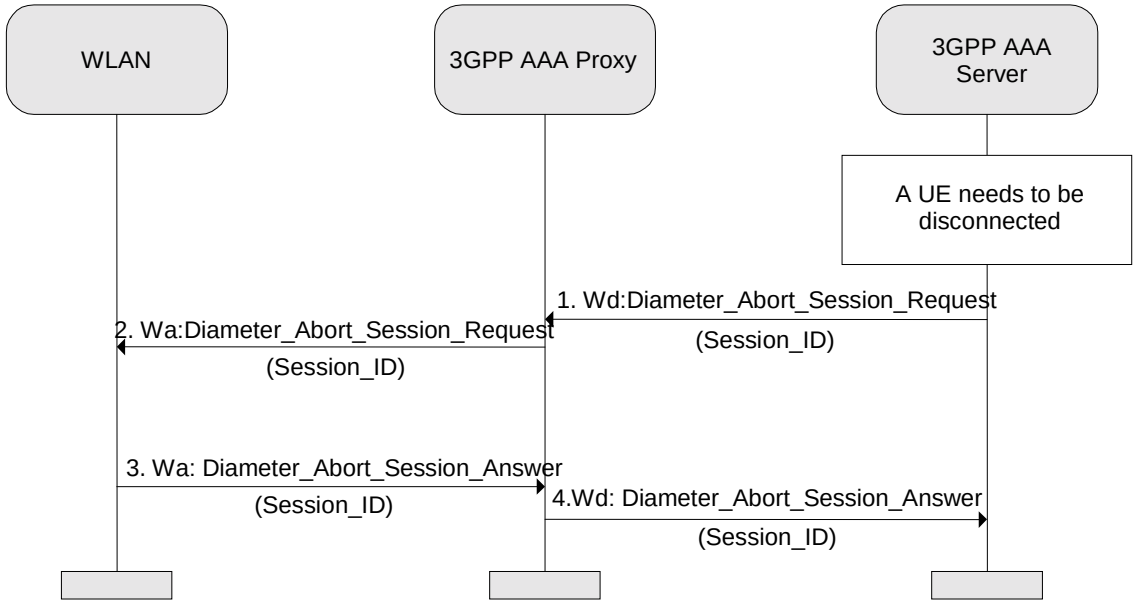

Figure A.6: Wa and Wd message flow for User Purging
Case c) Wa and Wd using Diameter

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.

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
09/2003	*CN#21*	*NP-030400*			*version 0.2.0 presented for information at CN#21*	*0.2.0*	*1.0.0*
12.11.03	*CN4#21*				*New version after CN4#21.* *Incorporates the changes from Tdocs: N4-031368, N4-031370 and N4-031386.*	*1.0.0*	*1.1.0*
9.03.04	*CN4#22*				*Incorporates Tdocs N4-040098, N4-040291, N4-040295, N4-040298, N4-040299. General architecture & Overview sections removed*	*1.1.0*	*1.2.0*
14.04.04	CN4#22bis				Incorporates Tdocs N4-040458, N4-040459, N4-040460, N4-040397, N4-040464, N4-040461, N4-040417, N4-040418	1.2.0	1.3.0
16.04.04	CN4#22bis				Incorporate Tdoc N4-040475	1.3.0	1.3.1
04-2004					Editorial corrections based by 3GPP TS 21.801	1.3.1	1.3.2
05-2004	CN4 #23				Incorporates Tdocs N4-040688, N4-040728, N4-040730	1.3.2	1.4.0
06-2004	CN4 #23bis	N4-040855			Incorporates Tdocs N4-040847, N4-040849, N4-040850, N4-040852, N4-040853, N4-040854. Also rebased according to 3GPP template and corrected chapter ordering problem. Corrections to formatting in Table 4.5.1. Correcting "AAA-Server" and "AAA-Proxy" mislabelling to "3GPP AAA Server" and "3GPP AAA Proxy".	1.4.0	1.5.0
08-2004	CN4#24	N4-041200			Incorporates N4-040980, N4-040984, N4-040986, N4-041139, N4-041140, N4-041141, N4-041142, N4-041143, N4-041146, N4-041144; N4-041198	1.5.0	1.6.0
08-2004	CN4#24				Editorial corrections from final CN4 session in Sophia Antipolis	1.6.0	1.7.0
08-2004	CN4#24				Sent to CN#25 for approval	1.7.0	2.0.0