3GPP TSG CN Plenary Meeting #21 **NP-030400**
17th – 19th September 2003 Frankfurt, GERMANY.

Source:	**CN4**
Title:	**3GPP TS 29.234 v1.0.0**
	3GPP System to WLAN Interworking;
	Stage 3 Description
Agenda item:	9.19
Document for:	**Information**

This document contains **3GPP TS 29.234 3GPP System to WLAN Interworking; Signalling Stage 3 Description**. It has been agreed by TSG CN WG4, and is forwarded to TSG CN Plenary meeting #21 for information.

TS 29.234 specify the protocol/s crossing several reference points of the 3GPP-WLAN IW architecture. It is initially focussed on specifying protocols used in reference points belonging to Scenario 2, such as Wr, Ws and Wx. In TS 29.234 also some of the scenario 3 related reference points are covered, but not developed so far waiting for the stabilization of the architecture work in SA2.

The open issues are:

- Further development of the protocol crossing the Wx reference point
- Development of Scenario 3 related reference points. Waiting for clearer definition in Stage 2.

3GPP TS 29.234 V1.0.0 (2003-09)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Core Network;
3GPP System to WLAN Interworking;
Stage 3 Description
(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 Wr interface between the WLAN AN and the 3GPP AAA Proxy.
- The Ws interface between the 3GPP AAA Proxy and 3GPP AAA Server.
- The Wx interface between the 3GPP AAA Server and the HSS
- The Wm interface between the 3GPP AAA Server and the PDG
- The Wn interface between the WLAN AN and the PDG

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 TS 21.905: "Vocabulary for 3GPP Specifications"

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

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

[4] 3GPP TS 23.234: "3GPP system to WLAN Interworking; System description"

[5] 3GPP TS 33.234: "WLAN Interworking Security"

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

[7] IETF Internet-Draft: "Diameter Base Protocol". draft-ietf-aaa-diameter-17.txt, work in progress

[8] IETF Draft: "Diameter Extensible Authentication Protocol (EAP) Application", draft-ietf-aaa-eap-02.txt, work in progress

[9] IEFT 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 Draft: "RADIUS Support For Extensible Authentication Protocol (EAP) ", draft-aboba-radius-rfc2869bis-22.txt, work in progress

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the [following] terms and definitions [given in ... and the following] apply.

Definition format

***<defined term>**: <definition>.*

example: text used to clarify abstract rules by applying them literally.

3.2 Symbols

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

Wb	Interface between a WLAN Access Network and a 3GPP AAAProxy (charging signalling)
Wc	Interface between a 3GPP AAA Proxy and a 3GPP AAA Server (charging signalling)
Wf	Interface between a CGw/CCF and a 3GPP AAA Server/Proxy
Wi	Interface between a Packet Data Gateway and an external IP Network
Wm	Interface between a Packet Data Gateway and a 3GPP AAA Server
Wn	Interface between a WLAN Access Network and a Packet Data Gateway
Wo	Interface between a 3GPP AAA Server and an OCS
Wr	Interface between a WLAN Access Network and a 3GPP AAA Proxy (control signalling)
Ws	Interface between a 3GPP AAA Proxy and a 3GPP AAA Server (control signalling)
Wx	Interface between an HSS and a 3GPP AAA Server
Wg	Interface between a 3GPP AAA Proxy and WAG

3.3 Abbreviations

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

AAA	Authentication, Authorisation and Accounting
CCF	Charging Collection Function
CG	Charging Gateway
EAP	Extensible Authentication Protocol
PDG	Packet Data Gateway
OCS	On-line Charging System
WAG	WLAN Access Gateway
WLAN	Wireless Local Access Network

4 Overview

Editor's Note: Provides general overview of WLAN-3GPP IW system

5 General Architecture

Editor's Note: General architecture of WLAN-3GPP IW system.

Editor's Note: The term roaming is used here when referring to roaming between 3GPP networks. However, an intermediate aggregator or a chain of intermediate networks may possibly separate the user when accessing the WLAN from the 3GPP home network.

Editor's Note: The architecture, namely network elements and reference points, is still under development in 3GPP SA2 WG.

The WLAN-3GPP IW system reference architecture is in 3GPP TS 23.234 [4]. It is compound of WLAN UE, WLAN Access Network, the Visited (Interworking) PLMN and Home PLMN.

Editor's Note: The specification of WLAN Access Network is out of 3GPP scope

System and Service requirements defined for WLAN-3GPP IW System have determined up to six WLAN-3GPP interworking scenarios. Each scenario realises an additional step in integrating WLAN in the 3GPP service offering and includes the previous level of integration of the previous scenario.

The WLAN-3GPP IW Roaming reference model in 3GPP TS 23.234 [4] satisfy the architectural requirements for scenario 2 and scenario 3.

In scenario 2, the WLAN-3GPP system interworking service is defined as a wireless IP connectivity service where the radio access technology is of type WLAN. The service is subject to a 3GPP system subscription. The implications of this scenario are:

- Internet/Intranet access from WLAN AN
- Authentication and authorisation for accessing the service based on 3GPP methods
- Online and Offline charging based on accounting procedures coming of the WLAN AN to the 3GPP AAA Server

The network elements involved to achieve scenario 2 type of service are 3GPP AAA Proxy, 3GPP AAA Server, OCS, CG/CCF and HSS. Optionally WAG. The reference points involved are Wr, Ws, Wx, Wb, Wc, Wo and Wf. From these, the ones covered by this specification are Wr, Ws and Wx.

In scenario 3, the WLAN-3GPP system interworking service is defined to access to 3GPP system PS based services available to the user through the WLAN. The services available should include all services based on 3GPP System PS domain capabilities (e.g. IMS). Additional implications of scenario 3 in comparison with scenario 2:

- Enabling user data to be tunnelled via operator network via PDG
- Charging based in service-flow differentiation performed in PDG
- Support for 3GPP IP based services via PDG, e.g. support for IMS
- Reliable level of end to end security

The network elements involved to achieve scenario 3 type of service are the ones involved in scenario 2, PDG and WAG. The additional reference points involved are Wn, Wm, Wg and Wi. From these, the ones covered by this specification are Wn and Wm.

Editor's Note: Scenario 3 architecture, reference points and network elements functionality is currently instable. There might be changes in the reference model, network elements and reference points functionality.

5.1 Network Elements Entities in WLAN-3GPP IW System

The network elements involved in WLAN-3GPP IW that are related to this specification are:

- WLAN UE
- 3GPP AAA Proxy
- 3GPP AAA Server

- HSS
- PDG Editor's Note: PDG only necessary for scenario 3
- WAG Editor's Note: WAG optional for scenario 2. Currently, It is optional for scenario 3. Due to not clear situation in scenario 3 architecture definition the status might change to mandatory, but not clear yet.

For detailed description on the WLAN-3GPP IW network elements refer to 3GPP TS 23.234 [4]

5.2 Reference Points in WLAN-3GPP IW System

In this section the WLAN-3GPP IW reference points are briefly described.

5.2.1 Wr Reference point (WLAN AN - 3GPP AAA Proxy)

Wr reference point connects the WLAN access network, possibly via intermediate networks, to the 3GPP AAA Network (i.e., 3GPP AAA Proxy in the roaming case and the 3GPP AAA Server in the non-roaming case). The prime purpose of the protocols crossing this reference point is to transport WLAN session authentication, authorization and related information in a secure manner. The reference point has to accommodate also legacy WLAN access networks.

5.2.2 Ws Reference point (3GPP AAA Proxy - 3GPP AAA Server)

The reference point Ws 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 in a secure manner.

5.2.3 Wx Reference point (3GPP AAA Server - HSS)

The reference point Wx is located between 3GPP AAA Server and HSS. The prime purpose of the protocols crossing this reference point is communication between WLAN AAA infrastructure and HSS.

5.2.4 Wn Reference point (WLAN AN- WAG- PDG)

Editor's Note: Reference point necessary for scenario 3 and for scenario 2 if WAG is used. Not stable yet.

5.2.5 Wm Reference point (3GPP AAA Server – PDG)

Editor's Note: Reference point only necessary for scenario 3.Not stable yet.

6 Wr Description

Wr is the reference point that connects the WLAN AN, possibly via intermediate networks, to the 3GPP Network (i.e., the 3GPP AAA Proxy in the roaming case and the 3GPP AAA Server in the non-roaming case). The reference point has to accommodate also legacy WLAN AN(RADIUS based), i.e. has to accommodate to the protocols supported by the WLAN ANs.

6.1 Functionality

The functionality of the reference point is to transport in RADIUS/Diameter frames:

- Carrying data for WLAN session authentication signalling between WLAN UE and 3GPP Network
- Carrying data for WLAN session authorization signalling between WLAN AN and 3GPP Network
- Carrying keying data for the purpose of radio interface integrity protection and encryption

- When such functionality is supported by the WLAN AN, used for purging a user from the WLAN access for immediate service termination

- Enabling the identification of the operator networks amongst which the roaming occurs

6.2 Protocols

Wr reference point inteworks with WLAN ANs. In early deployments of WLAN-3GPP IW, a significant amount of WLAN ANs will provide RADIUS-based interfaces. On the other hand, WLAN ANs will migrate gradually towards Diameter-based interfaces.

Therefore, in order to interwork with the two kind of WLAN ANs, 3GPP AAA Proxy in the roaming case and the 3GPP AAA Server in the non-roaming case, has to support Diameter-based and RADIUS-based protocols in the Wr reference point towards the WLAN ANs.

Wr reference point shall contain the protocols :

1) RADIUS based. RFC 2869 [9] shall be used. It provides RADIUS extensions to support EAP frames transport

2) Diameter based. Diameter EAP Application [8] shall be used. It provides a Diameter application to support EAP frames transport

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

WLAN ANs depending on their characteristics will use either 1) or 2) over Wr reference point

6.3 Requirements in 3GPP AAA Proxy for Radius/Diameter "Translation Agent"

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

WLAN-3GPP IW system assumes interworking of legacy WLAN AN(RADIUS based) with PLMNs. Legacy WLAN ANs are broadly deployed supporting RADIUS as the AAA protocol. Therefore, RADIUS is the de-facto AAA protocol when interworking those kind of WLAN ANs. However, it is likely that in the future WLAN ANs will support Diameter as AAA protocol.

Ws interface is Diameter based and Wr have two possibilities either Diameter or RADIUS based. When Wr interface interworks with a WLAN AN that is RADIUS based, 3GPP AAA Proxy needs to implement a " Translation Agent" to perform the function of translating between RADIUS and Diameter messages.

A RADIUS/Diameter Translation Agent has the following requirements:

- Receive RADIUS requests (send 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.

6.3.1 Conversion of RADIUS Request to Diameter Request

When receiving a RADIUS Request on the Wr interface, the 3GPP AAA Proxy Translation Agent shall translate it into a Diameter Request to be forwarded on the Ws interface, as describe 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.

6.3.2 Conversion of Diameter Response to RADIUS Response

When receiving a Diameter Response on the Ws interface, the 3GPP AAA Proxy Translation Agent shall translate it into a RADIUS Response to be forwarded on the Ws interface, 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.

6.3.3 3GPP AAA Proxy advertisement of RADIUS or Diameter client to 3GPP AAA Server

The 3GPP AAA Proxy is required to be able to handle clients that are Diameter based and clients that are RADIUS based. When a client attached to the 3GPP AAA Proxy is Diameter based, Diameter messages can be passed on to the 3GPP AAA Server through the 3GPP AAA Proxy transparently. When a client attached to the 3GPP AAA Proxy is RADIUS based, the RADIUS messages sent by the client shall be translated by the 3GPP AAA Proxy Translation Agent into Diameter messages which can be sent on to the 3GPP AAA Server by the 3GPP AAA Proxy.

Between the 3GPP AAA Proxy and 3GPP AAA Server, Ws reference point is Diameter based (see section 7.2). Therefore the information on whether the client is Diameter or RADIUS is known by the 3GPP AAA Proxy and this one shall indicate it to 3GPP AAA Server over Ws.

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 Wr interface, it may use these AVP's in the Diameter message it sends to the 3GPP AAA Server on the Ws interface to indicate to the 3GPP AAA Server that the client 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 client.

3GPP AAA Proxy shall indicate to the 3GPP AAA Server the case that the client 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
- NAS-Identifier AVP
- State AVP
- Termination-Cause AVP

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

6.3.4 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 [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 [NASREQ]:

- RADIUS Identifier Field [6] in the RADIUS-Request
- Source IP address of the RADIUS-Request message
- Source UDP port of the RADIUS-Request message
- RADIUS Proxy-State [6] in the RADIUS-Request

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 [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.

6.4 Procedures Description

6.4.1 WLAN Access Authentication and Authorisation

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

Diameter usage in Wr:

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

See Annex A.1.1 for signalling flow reference.

RADIUS usage in Wr:

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

See Annex A.1.1 for signalling flow reference.

6.4.2 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 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 [6] 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 ANs.

Diameter usage in Wr:

- This procedure is mapped to the Diameter command codes Diameter-Abort-Session-Request and Diameter-Abort-Session-Answer specified in [7].

See Annex A.1.2 for signalling flow reference.

RADIUS usage in Wr:

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

6.5 Information Elements Contents

void

7 Ws Description

Ws is the reference point that 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 in a secure manner.

7.1 Functionality

The functionality of the reference point is to transport in Diameter frames:

- Carrying data for WLAN session authentication signalling between 3GPP AAA Proxy and 3GPP AAA Server
- Carrying data for WLAN session authorization signalling between 3GPP AAA Proxy and 3GPP AAA server
- Carrying keying data for the purpose of radio interface integrity protection and encryption
- Used for purging a user from the WLAN access for immediate service termination
- Enabling the identification of the operator networks amongst which the roaming occurs

7.2 Protocols

Ws reference point shall be based on a single AAA protocol. Diameter based protocol shall be used.

Ws protocol is:

- Diameter based. Diameter EAP Application [8] shall be used. It provides a Diameter application to support EAP (RFC 2284 [10] and [11]) frames transport, as well as the basic operation of Diameter Base [7]

7.3 3GPP AAA Server behaviour when Interworking with RADIUS/Diameter clients

The 3GPP AAA Server is serving RADIUS and/or Diameter based clients, as clients can be located in either type of WLAN ANs. The 3GPP AAA Server needs to be aware of what kind of client it is serving in order to adapt its operation to the client capabilities.

The 3GPP AAA Proxy is the only network element in direct contact with the WLAN ANs and therefore, it is aware of whether the client is RADIUS or Diameter based. The 3GPP AAA Proxy shall indicate over the Ws interface to the 3GPP AAA Server the case of client being RADIUS, otherwise the 3GPP AAA Server shall assume the client to be Diameter-based *(see section 6.3.3)*

Once the Diameter 3GPP AAA Server is aware of client type, it shall adapt its operation over Ws.

When the client is Diameter based, the operation mode of the Diameter 3GPP AAA Server is the normal behaviour described in Diameter EAP[8] and Diameter Base[7].

When the client is RADIUS based, the operation mode of the Diameter 3GPP AAA Server is the normal behaviour described in Diameter EAP[8] and Diameter Base[7], but shall be modified as follows to ensure RADIUS compatibility:

- Diameter AVPs to RADIUS attributes compatibity:
    - 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

7.4 Procedures Description

7.4.1 WLAN Access Authentication and Authorisation

This procedure is used to transport the WLAN Access Authentication and Authorisation 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]

7.4.2 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 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 [7].

7.5 Information Elements Contents

void

8 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

8.1 Functionality

The functionality of the reference point is to enable:

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

8.2 Protocols

Wx reference point shall use a Diameter based protocol(s)

8.3 Procedures Description

void

8.3.1 Authentication Procedures

void

8.3.2 Location Management Procedures

void

8.3.2.1 WLAN Registration/DeRegistration Notification

void

8.3.2.2 Network Initiated De-Registration by HSS, Administrative

void

8.3.3 User Data Handling

void

8.3.3.1 User Profile Download

void

8.3.3.2 HSS Initiated Update of User Profile

void

8.4 Information Elements Contents

void

9 Wn Description

Editor's Note: Reference point necessary for scenario 3.Not stable yet.

FFS

10 Wm Description

Editor's Note: Reference point only necessary for scenario 3.Not stable yet.

FFS

:

Annex A.1 (normative): Wr & Ws Procedures Signalling Flows

A.1.1 Authentication, Authorisation and Key Delivery

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

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

The signalling sequence shown is based on Diameter. For signalling to WLANs using RADIUS the conversion defined in Diameter specification shall be used.

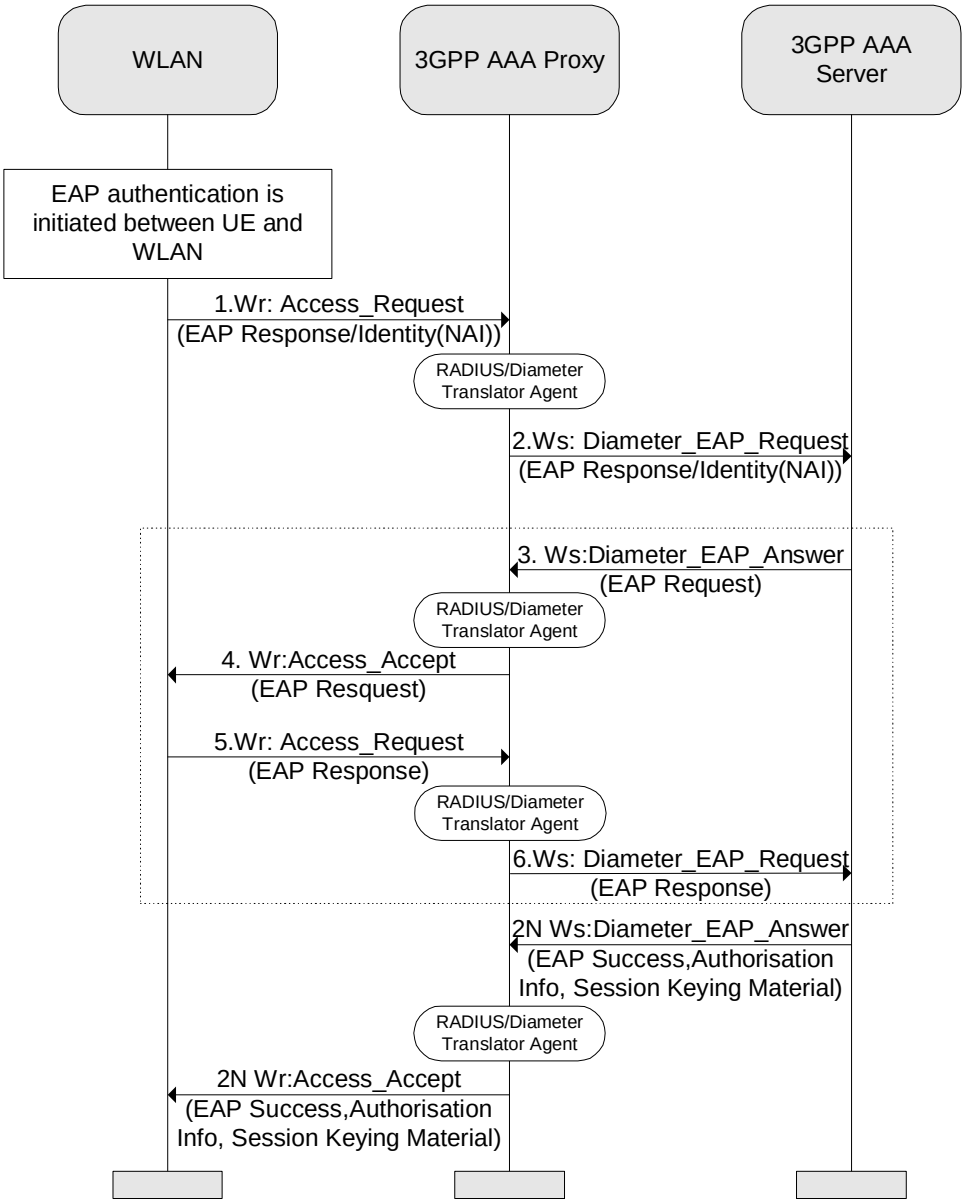

Figure 1. Wr and Ws message flow for WLAN Session Authentication and Authorisation. Case a) Wr with Radius mandatory implementation

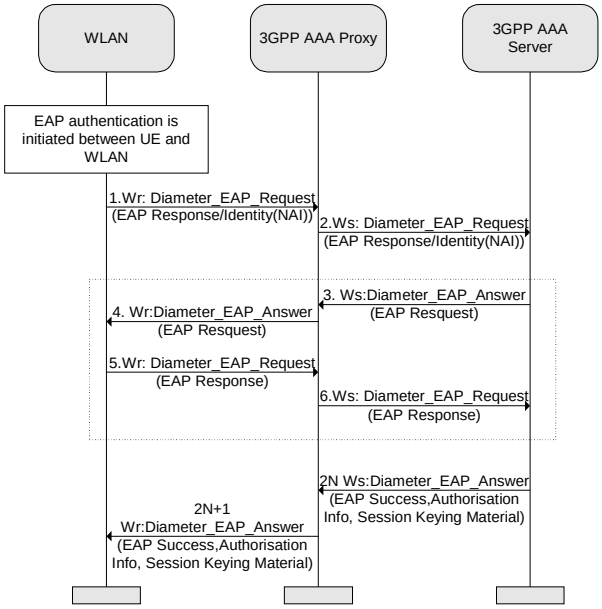

Figure 2. Wr and Ws message flow for WLAN Session Authentication and Authorisation. Case b) Wr with Diameter optional implementation

1. The WLAN initiates authentication procedure towards 3GPP network by sending to 3GPP AAA Proxy

- "Access_Request" message in case a) or

  - Diameter_EAP_Request message in case b)

3GPP AAA Proxy sends to 3GPP AAA Server a Diameter_EAP_Request message that carries encapsulated EAP Response/Identity message to 3GPP AAA Server. Message also carries a Session-ID used to identify the session within the WLAN.

2. The Diameter_EAP_Request message sent by 3GPP AAA Server can be generated in two ways:

   - Outcome of the conversion by the 3GPP AAA Proxy “Translator Agent” from the RADIUS Access_Request to Diameter_EAP_Message in case a)

   - Outcome of the proxying by the 3GPP AAA Proxy of the Diameter_EAP_Message originated in WLAN in case b)

3. 3GPP AAA Server performs the authentication procedure based on information retrieved from HSS/HLR. 3GPP AAA Server sends message Diameter_EAP_Answer to 3GPP AAA Proxy. This message carries encapsulated EAP Request message. The content of the EAP Request message is dependent on the EAP type being used.

4. 3GPP AAA Proxy may act in two different ways:

   - Conversion of the “Diameter_EAP_Answer” message to “Access_Accept” by the “Translator Agent” in case a) and sending “Access_Accept” to the WLAN

   - Proxying the “Diameter_EAP_Answer” message to the WLAN in case b)

WLAN conveys the EAP Request message to the UE.

5. UE responds to WLAN by an EAP Response message. WLAN encapsulates it into:

   - Access_Request message in case a) and send it to 3GPP AAA Proxy

   - Diameter_EAP_Request message in case b) and sends it to 3GPP AAA Proxy

6. 3GPP AAA Proxy will:

    - Convert “Access_Request” to “Diameter_EAP_Request” by using the “Translator Agent” in case a) and send it to the 3GPP AAA Server
    - Proxy “Diameter_EAP_Request” message to 3GPP AAA Server in case b)

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 3GPP AAA server has successfully authenticated the 3GPP subscriber, the 3GPP AAA Server sends final Diameter_EAP_Answer message carrying encapsulated EAP Success message.

2N+1. 3GPP AAA Proxy may act in two ways:

- Convert “Diameter_EAP_Answer” message to “Access_Accept” by the “Translator Agent” in case a) and sends it to the WLAN
- Proxy “Diameter_EAP_Answer” message to the WLAN in case b)

WLAN forwards the EAP Success message to the UE.

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

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

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

This signalling sequence is initiated by the 3GPP AAA Server when a UE needs to be disconnected from accessing WLAN interworking service. For example, a 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 is based on Diameter. For signalling to WLANs using RADIUS the conversion defined in Diameter specification shall be used.

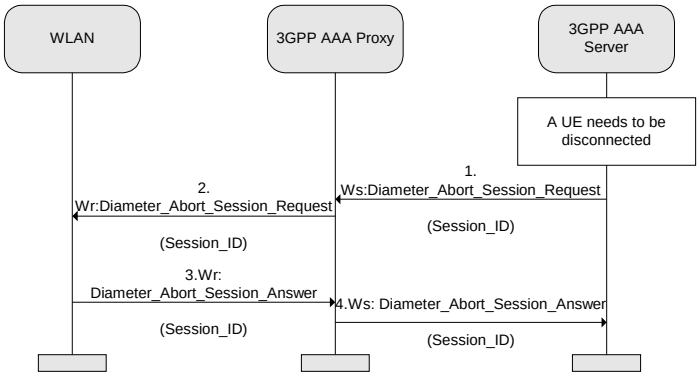

Figure 3. Wr and Ws message flow for User Purging. Case b) Wr with Diameter optional implementation

1. When 3GPP AAA Server needs to disconnect (e.g. after receiving an external trigger) a 3GPP subscriber from the WLAN access service, the 3GPP AAA Server sends a Diameter_Abort_Session_Request to 3GPP AAA Proxy. This message contains the Session ID by which the session is identified within the WLAN.

2. 3GPP AAA Proxy proxies to WLAN the “Diameter_Abort_Session_Request Message”.proxied by 3GPP AAA Proxy.

3. 4. WLAN responds to 3GPP AAA Server via 3GPP AAA Proxy by Diameter_Abort_Session_Answer as defined in Diameter Base[7].

Editor´s Note: It is needed to define also the message flow when “Wr” is RADIUS based.

It is FFS the implementation of this procedure when Wr is RADIUS based.

Annex <B> (informative): <Informative annex title>

Annex <X> (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