**3GPP TSG SA WG3 Security — S3#28** **S3-030176**
**6 - 9 May 2003**
**Berlin, Germany**

**3GPP TSG SA2 #30** **S2-030994**
**Milan, Italy, 24-28.2.2003**

**Title:** LS on Clarification of Scenario 2 and Scenario 3 architectural characteristics and stable and non-stable parts of TS 23.234
**Release:** Release 6
**Work Item:** WLAN Interworking

**Source:** SA2
**To:** SA, SA3, SA5, CN, CN1, CN4, CN3
**Cc:** SA1

**Contact Person:**
Name: Raquel Rodríguez
Tel. Number: + 358405259208
E-mail Address: Raquel.Rodríguez@nokia.com

**Attachments:** S2-030727

## 1. Introduction

Based on the query received from TSG-SA, and the fact that stage-3 WLAN Interworking Wis are being created across the relevant CN WGs, SA2 would like to clarify what are the stable and non-stable parts in the currently defined architecture (Stage 2 work) for WLAN-3GPP IW in TS 23.234. Furthermore, the Scenario 2 and Scenario 3 architectural characteristics are also clarified. The target is to ensure that other WGs that have initiated WLAN-3GPP IW work, have a clear understanding of the architecture situation, to proceed with their work.

## 2. Clarification

### ❑ SCENARIO 2 AND ITS STABILITY

The description of Scenario 2 according to SA1 is: “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 definition 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 off the WLAN AN to the 3GPP AAA Server. The 3GPP AAA server uses accounting procedures of the Wo and Wf interfaces for online and offline accounting with the OCS and the CCF/CGw, respectively.

The network elements involved to achieve Scenario 2 are: 3GPP AAA Proxy, 3GPP AAA Server, HSS/HLR, OCS and CGW/CCF

The BGW is optional in scenario 2.

The reference points involved in Scenario 2 are Wr, Wx, Wb, Wo and Wf. When pre-Release-6 HSS/HLR is used, the D´/Gr´ reference points are also involved.

Figure 1 shows the network elements that are needed to achieve authentication, access control and charging functions in Scenario 2.

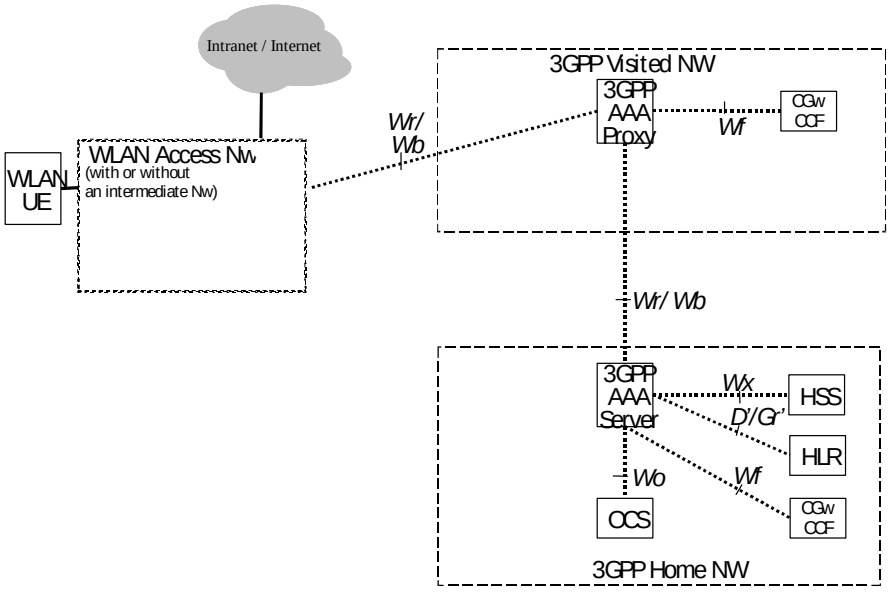



Figure 1. Roaming Reference Model with stable needed network elements and reference points to accomplish Scenario 2

The architecture of Scenario 2 shown in Figure-1 is stable already.

Network selection aspects are still under discussion.

## ❑ SCENARIO 3 AND ITS STABILITY

The goal of Scenario 3 according to SA1 is: “to make 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).”

Scenario 2 is a pre-requisite for Scenario 3. Additional implications of Scenario 3 compared to Scenario 2 are:

- Enabling user data to be tunnelled via operator network via PDGW. UE transparent tunnelling or UE initiated tunnelling.
- Charging based in service-flow differentiation performed in PDGW. SA2 is working on the overall architecture aspects for IP-flow-based bearer charging within the context of a separate WI. This work is expected to produce a stable high level architecture by 03/03, and a stable stage-2 concept by 06/03.
- Support for 3GPP IP based services via PDGW , e.g. support for IMS
- Reliable level of end to end security
- Certain level of QoS provisioning

The network elements involved to achieve Scenario 3 beyond the ones in Scenario 2: PDGW and BGW.

The additional reference points involved in Scenario 3 beyond the ones in Scenario 2 are Wn, Wi and Wm. However, certain aspects (e.g. charging) of the Scenario 3 architecture are expected to be developed further, hence new interfaces might still be added.

**The scenario 3 reference model is not yet stable. Detailed issues are:**

- UE transparent tunnelling and UE initiated tunnelling to PDGW.
- Detailed tunnel type and authorization
- Charging reference points related to scenario 3 to perform differentiated service-flow-based charging towards OCS and CGW.
- Support for 3GPP IP based services e.g. IMS, implications in PDGW.
- Level of QoS support for IMS. The relation of the PDGW and Service Based Local Policy.

## 3. Actions:

**To TSGs:**

Note the current status of the WLAN-IW stage-2 work as described above.

**To CN WGs:**

SA2 asks CN WGs to consider this informational LS to start and proceed with the WLAN-3GPP IW Stage 3 work.

**To SA WGs:**

SA2 asks SA WGs to consider this informational LS to proceed with the WLAN-3GPP security and charging aspects.

## 4. Date of Next TSG–SA WG2 Meetings:

| Meeting | Date | Location | Host |
|---|---|---|---|
| **SA2#31** | **07-11. April 2003** | **Korea** | **Samsung** |
| **SA2#32** | **12-16. May 2003** | **USA** | **-** |

# Draft 3GPP TS 23.234 V1.5x6.0 (2003-02)

*Technical Specification*

**3rd Generation Partnership Project;**
**Technical Specification Group Services and System Aspects;**
**3GPP system to Wireless Local Area Network (WLAN) Interworking;**
**System Description**
**(Release 6)**

Keywords

<keyword[, keyword]>

***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 ..... 5

Introduction ..... 5

1 Scope ..... 6

2 References ..... 6

3 Definitions, symbols and abbreviations ..... 6
3.1 Definitions ..... 7
3.2 Symbols ..... 7
3.3 Abbreviations ..... 7

4 WLAN Radio networks ..... 7
4.1 WLAN Networks Interworking with 3GPP ..... 7

5 High-level Requirements and Principles ..... 8
5.1 Access Control Requirements ..... 8
5.2 Access Control Principles ..... 9
5.3 Authentication methods ..... 10
5.3.1 General Requirements ..... **Error! Bookmark not defined.**
5.3.2 USIM based Authentication ..... **Error! Bookmark not defined.**
5.3.3 GSM SIM based authentication ..... **Error! Bookmark not defined.**
5.3.5 Re-authentication ..... 10
5.4 User Identity ..... 10
5.4.1 Home network domain name ..... 11
5.4.2 User identity ..... **Error! Bookmark not defined.**
5.4.3. Allocation of temporary identifier ..... **Error! Bookmark not defined.**
5.5 IP Network Selection ..... 11
5.5.1. IP Connectivity without Tunneling ..... 12
5.5.2 UE-Transparent Tunneling ..... 12
5.5.3 UE-Initiated Tunneling ..... 12
5.6 Charging Requirements ..... 13
5.7 Charging Principles ..... **Error! Bookmark not defined.**
5.7.1 Offline Charging ..... 13
5.7.2 Online Charging ..... 13
5.8 Network Selection Principles ..... 13
5.8.1 Case of IEEE 802.11 WLANs ..... 14
5.8.2 Case of HiperLan/2 WLANs ..... 14
5.8.3 Case of Bluetooth WLANs ..... 14

6 Interworking Architecture ..... 14
6.1 Reference Model ..... 14
6.1.1 Non Roaming WLAN Inter-working Reference Model ..... 14
6.1.2 Roaming WLAN Inter-working Reference Model ..... 15
6.2 Network elements ..... 16
6.2.1 WLAN UE ..... 16
6.2.2 3GPP AAA Proxy ..... 16
6.2.3 3GPP AAA Server ..... 17
6.2.4. HLR/HSS ..... 17
6.2.5 Border Gateway ..... 17
6.2.6 Packet Data Gateway ..... 18
6.3Reference Points ..... 18
6.3.1 Wr 18
6.3.1.1 General description ..... 18
6.3.1.2 Functionality ..... 19
6.3.1.3 Protocols 19
6.3.2 Wx 19
6.3.3 D'/Gr' 19
6.3.4 Wb 20

6.3.5 Wo 20
6.3.6 Wf 20
6.3.7 Wn 21
6.3.8 Wi 21
6.3.9 Wm 21

7 Procedures ..... 22
7.1 Authentication and Authorisation ..... 22
7.2 Subscriber Profile Update ..... 23
7.3 Canceling WLAN Registration ..... 24
7.4 Disconnecting a Subscriber by WLAN ..... 25
7.5 Disconnecting a Subscriber by Online Charging System ..... 25
7.6 Charging offline charged subscribers ..... 26
7.7 Charging online charged subscribers ..... 27

**Annex A (informative): Refererence Points Signalling Flows ..... 30**

A.1 Signalling Sequences examples for Wr Reference Point ..... 30

A.2 Signalling Sequences examples for Wx Reference Point ..... 33

A.3 Signalling Sequences examples for D' Reference Point ..... 38
Authentication Information Retrieval ..... 38
Subscriber Profile Retrieval ..... 39

A.4 Gr' Signalling Mechanisms to support WLAN service ..... 40
Introduction ..... 40
Existing GPRS parameter ..... 40
Possible WLAN use 40
infoRetrieval procedure: ..... 41
gprsLocationUpdate procedure: ..... 41

A.5 Example of Authentication procedures ..... 41

**Annex B (informative): WLAN Radio Technologies ..... 51**

**Annex C (informative): Hierarchical Roaming Principles ..... 53**

**Annex D (informative): Function Prioritisation ..... 63**

**Annex E (informative): Change history ..... 65**

# 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.

# Introduction

This document studies interworking between 3GPP systems and Wireless Local Area Networks (WLANs). For the purpose of this document the term 3GPP - WLAN interworking refers to the utilisation of resources and access to services within the 3GPP system by the WLAN UE and user respectively. The intent of 3GPP - WLAN Interworking is to extend 3GPP services and functionality to the WLAN access environment. Thus the WLAN effectively becomes a complementary radio access technology to the 3GPP system.

The WLAN provides access to services that can be located either in the WLAN itself or in a network that is connected to the WLAN.

In 3GPP - WLAN interworking, 3GPP system functionalities can be used either through a WLAN or independently of any WLAN (i.e. using 3GPP access). In the case of 3GPP system functionalities accessed via a WLAN, the interworking between 3GPP system and WLAN may include:

- Enabling usage of 3GPP system functionalities between mobile terminals and 3GPP systems via the WLAN (e.g. providing SIP calls)
- Utilising 3GPP system functionalities to complement the functionalities available in the WLAN (e.g. providing charging means, authentication, authorization, and accounting functions)

Moreover, in order to ensure transition between the WLAN access and the 3GPP access, the interworking between the systems may include

- Creation of mechanisms for selecting and switching between the WLAN and 3GPP access systems

Enabling any of these interworking cases may result in modifications or additions in 3GPP systems, in WLANs or both.

# 1 Scope

This document specifies the 3GPP WLAN subsystem. The 3GPP WLAN subsystem is assumed to provide bearer services for connecting a 3GPP subscriber via WLAN to IP based services compatible with those offered via PS domain.

# 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 TS 23.002: "Network architecture".

[3] 3GPP TS 32.225: " Telecommunication management;Charging management;Charging data description for the IP Multimedia Subsystem (IMS)."

[4] 3GPP TS 29.329: " Sh Interface based on the Diameter protocol; Protocol details."

[5] 3GPP TS 29.002: "Mobile Application Part (MAP) specification "

[6] RFC2284: ” PPP Extensible Authentication Protocol (EAP)”

[7] RFC 2486: “The Network Access Identifier”

[8] IETF Internet-Draft, "Diameter Base Protocol".

http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-12.txt

[9] J. Caron, “DNS Based Roaming”, http://www.ietf.org/internet-drafts/draft-caron-dns-based-roaming-00.txt, April 2002, (work in progress)

[10] 3GPP TS 33.234: "WLAN Interworking Security."

[11] Calhoun, P., et al, “Diameter Network Access Server Application, http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-nasreq-11.txt , February 2003, (work in progress)

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

**APN:** Access Point Name

**Environment:** The type of area to be covered by the WLAN network of a 3GPP - WLAN interworking; e.g. public, corporate and residential.

**Home WLAN:** The WLAN that is interworking with the HPLMN of the 3GPP - WLAN interworking user.

**Interworking WLAN** : WLAN that interworks with a 3GPP system**.**

**Visited WLAN:** An interworking WLAN that Interworks only with a visited PLMN.

**WLAN coverage:** an area where wireless local area network access services are provided for interworking by an entity in accordance with WLAN standards.

**WLAN roaming**: The ability for a 3GPP - WLAN interworking user (subscriber) to function in a serving WLAN different from the home WLAN

**3GPP - WLAN Interworking:** Used generically to refer to interworking between the 3GPP system and the WLAN family of standards**.** Annex B includes examples of WLAN Radio Network Technologies.

## 3.2 Symbols

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

| | |
|---|---|
| Wb | Interface between WLAN Access Network and 3GPP AAA |
| Wf | Interface between a CGw/CCF and 3GPP AAA |
| Wo | Interface between 3GPP AAA and OCS |
| Wr | Interface between WLAN Access Network and 3GPP AAA |
| Wx | Interface between HSS and 3GPP AAA |

## 3.3 Abbreviations

| | |
|---|---|
| CCF | Charging Collection Function |
| CGw | Charging Gateway |
| OCS | Online Charging System |
| PDA | Personal Digital Assistant |
| WLAN | Wireless Local Area Network |

# 4 WLAN Radio networks

Editor's notes : Provides a high-level description of WLAN technologies/standards.

## 4.1 WLAN Networks Interworking with 3GPP

Figure 4.1 illustrates WLAN networks from the point of view of 3GPP interworking. The 3GPP Authentication, Authorization and Accounting (AAA) server is a Diameter or Radius server. The Packet Data Gateway, introduced in scenario 3, is a node via which packet data networks are connected. Scenario 2 offers direct connection from the WLAN to the Internet/intranet. The WLAN includes WLAN access points and may include other devices such as routers or intermediate AAA elements. The User Equipment (UE) includes all equipment that is in possession of the end user, such as a computer, WLAN radio interface adapter etc.

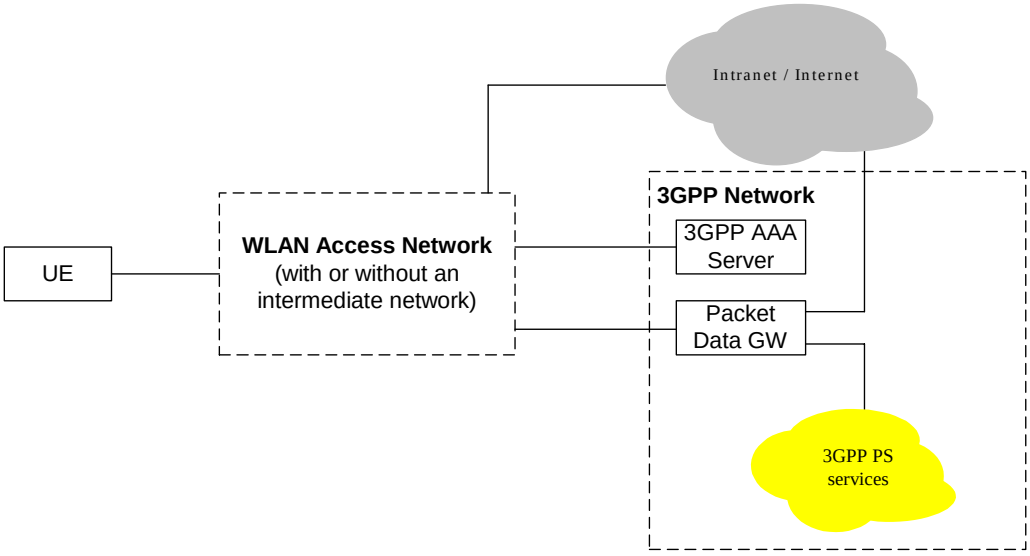



*Figure 4.1: Simplified WLAN Network Model*

- As 3GPP-WLAN interworking concentrates on the interfaces between 3GPP elements and the interface between the 3GPP system and the WLAN, the internal operation of the WLAN is only considered in order to access the impact of architecture options/requirements on the WLAN.
- 3GPP-WLAN interworking shall be independent of the underlying WLAN Radio Technology.

For IEEE 802.11 Wireless LANs, the authentication and security functionality between UE and WLAN is specified in the IEEE 802.11i standard.

[Editor's note; IEEE 802.11i is work in progress at the time of writing.]

# 5 High-level Requirements and Principles

Editor's note : Provides the high-level functional requirements for the Interworking between WLAN and 3GPP system

It is necessary to provide WLAN interconnection between WLAN Networks and pre-R6 3GPP Networks. Hence it is required that this TS is compatible with R99 Networks and onward.

## 5.1 Access Control Requirements

- Legacy WLAN terminals should be supported. However software upgrades may be required for e.g. security reasons.
- Minimal impact on the user equipment, i.e. client software.
- Minimal impact on existing WLAN networks.
- The need for operators to administer and maintain end user SW shall be minimized

- Existing SIM and USIM shall be supported.
- Authentication shall rely on (U)SIM based authentication mechanisms.
- R6 USIM may include new functionality if seemed necessary e.g. in order to improve privacy.
- Changes in the HSS/HLR/AuC shall be minimized.
- Methods for key distribution to the WLAN access NW shall be supported
- The WLAN connection established for a 3GPP subscriber shall have no impact to the capabilities of having simultaneous PS and CS connections for the same subscriber
- Authorization shall occur upon the success of the authentication procedure
- It shall be possible to indicate to the user of the results of authorization requests.
- It shall be possible to indicate to the user any conditions for use of an authorised service.
- Results of authorization requests shall be indicated to the WLAN, so that the WLAN can take appropriate action.
- The authorization mechanism shall be able to inform the user and WLAN immediately of any change in service provision.

Additional access control requirements for scenario 3:

- Policy control applies to the services authorized for the user.
- Access to 3GPP PS based services shall be provided via WLAN. 3GPP PS based services supported shall include IMS based services including Presence and IMS Messaging services, location based services, ~~instant messaging, presence based services,~~ MBMS and services built upon combinations of these. Among these services, prioritisation is given for information in Annex C.
- Access to PS based services normally provided by the 3GPP packet core shall be provided via WLAN. These PS based services shall include support of private addressing schemes, external address allocation, secure tunnelling to private network, ability to provide addresses of DNS and NetBios servers specific to a private network.

## 5.2 Access Control Principles

**End to End Authentication :** WLAN Authentication signalling is executed between WLAN UE and 3GPP AAA Server for the purpose of authenticating the end-user and enabling the access to the WLAN and 3GPP network.

**Transporting Authentication signalling over WLAN Radio Interface :** WLAN authentication signalling is carried between WLAN UE and WLAN AN by WLAN Access Technology specific protocols. To ensure multivendor interoperability these WLAN technology specific protocols shall conform to existing standards of the specific WLAN access technology.

**Transporting Authentication signalling between WLAN and 3GPP network** : WLAN Authentication signalling shall be transported **between WLAN and 3GPP network** by standard mechanisms, which are independent on the specific WLAN technology utilised within the WLAN Access network.

Details of end to end authentication and transport of authentication signalling over the WLAN radio interface and between the 3GPP network and WLAN is covered in 3GPP TS 33.234 [10]

Additional access control principle for scenario 3:

**Service Selection**

The end to end signalling shall include means for delivering encrypted service selection information from the UE to the 3GPP AAA server. The service selection information may contain APN and External Protocol Configuration Options as they are defined in 3GPP TS 24.008. Before admitting the user to access WLAN, 3GPP AAA server shall verify users subscription to the indicated APN against the WLAN subscriber profile retrieved from HSS.

## 5.3 Authentication methods

Authentication methods are discussed in TS 33.234 [6].

### 5.3.1 Re-authentication

On some networks, EAP authentication may be performed frequently. For such cases, EAP SIM and EAP AKA include an optional re-authentication procedure. Re-authentication causes less load on the network and is faster to execute than the full SIM/USIM authentication procedure. Re-authentication is optional to implement for both the WLAN UE and 3GPP AAA server. On each EAP authentication, either one of the entities may also fall back on full authentication if they do not want to use re-authentication. Re-authentication is based on the keys derived on the preceding full authentication.

On re-authentication, the UE protects against replays with an unsigned 16-bit counter. The server includes an encrypted server nonce (NONCE_S) in the re-authentication request. The Message Authentication Code attribute in the client's response is calculated over NONCE_S to provide a challenge/response authentication scheme. The NONCE_S also contributes to the new session keys.

Because one of the objectives of the re-authentication procedure is to reduce load on the network, the re-authentication procedure does not require the 3GPP AAA server to contact a reliable database. Therefore, the re-authentication procedure makes use of separate re-authentication user identities. Pseudonyms and the permanent IMSI-based identity are reserved for full authentication only. The network does not need to store re-authentication identities as carefully as pseudonyms. If a re-authentication identity is lost and the network does not recognize it, the 3GPP AAA server can fall back on full authentication.

If the 3GPP server supports re-authentication, it may communicate an encrypted re-authentication identity for next re-authentication to the WLAN UE during full authentication. If the client wants to use re-authentication, it uses this re-authentication identity on next authentication.

[*Editor's note: Section 5.3.5 on re-authentication may be removed once it is incorporated into TS 33.234*]

## 5.4 User Identity

### 5.4.1 General

The network authentication procedure are based on the use of EAP method, as described in clause 7, where User Identity field carries the user identity in the Network Access Identifier (NAI) format specified in RFC 2486 [7]. An NAI is composed of a username part and a realm part. For more information, the NAI username part format is specified in EAP-SIM and EAP-AKA specifications [EAPSIM], [EAPAKA].

For user identity protection a Temporary Identity username can be used. The use of a temporary identifier is necessary to replace the IMSI in radio transmissions as it protects the user against tracing from unauthorized access networks. As a working assumption, it is considered in this version of the TS that temporary identifiers are allocated ~~and stored~~ in the 3GPP AAA Server.

For reauthentication, UE shall use the previously allocated Reauthentication ID as specified in [EAP-SIM] and [EAP-AKA] as its NAI user identity.

### 5.4.2 NAI Realm Name

The NAI realm name shall be in the form of an Internet domain name as specified in RFC 1035.

On EAP-SIM and EAP-AKA full authentication,the UE shall by default derive the NAI realm from the IMSI as described in the following steps:

1. take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [27]) and separate them into MCC and MNC with "."; and
2. reverse the order of the MCC and MNC. Append to the result: "WLAN.3gppnetwork.org"

An example of a home network domain name is:

EXAMPLE: IMSI in use: 234150999999999;

- where;
- MCC: 234;
- MNC: 15;
- MSIN: 0999999999; and
- home domain name: 15.234.WLAN.3gppnetwork.org.

NOTE: Other mechanisms to retrieve a realm e.g. by having a realm configured in a R6 USIM are FFS.

## 5.5 IP Network Selection

Note that this type of IP Network Selection is only applicable in scenario 3. Scenario 2 offers direct connection from the WLAN network to Internet/intranet.

The UE can connect to different IP networks, including the Internet, an operator's IP network or an external IP network such as a corporate IP network. The user may indicate a preferred IP network with an WLAN Access Point Name (WAPN). The relationship between WAPN and the GPRS APN is FFS.

A WAPN is transmitted from the UE to the 3GPP AAA server in the end-to-end EAP/AAA signalling. The home network decides the type of IP connectivity based on for example the WAPN and user's subscription information. The home network choices are:

1. No tunnelling
2. UE-transparent tunneling
3. UE-initiated tunneling

Visited network choices are FFS.

These cases are described below.

### 5.5.1. IP Connectivity without Tunneling

When no tunnelling is used, the 3GPP AAA server does not include any tunnel attributes in Wr signalling.

### 5.5.2 UE-Transparent Tunneling

When UE-transparent tunneling is used, the UE is not involved in tunnel establishment or packet encapsulation/decapsulation to the PDGW.

In this case, the WLAN session is established as follows (assuming that the PDGW in the home network is used):

1. EAP authentication between UE and 3GPP AAA Server. WAPN information and other relevant information (username/password) may be transmitted as part of the end-to-end signalling.
2. The 3GPP AAA server decides that UE-transparent tunneling shall be used for this session.
3. Tunnel attributes are transmitted from 3GPP AAA Server to WLAN over the Wr reference point
4. The WLAN establishes a tunnel to the PDGW, e.g., binds the IEEE 802.11 MAC address to a tunnel endpoint
5. UE uses for example DHCP to get the IP address and configuration information. (For example, WLAN may tunnel DHCP packets to PDGW which includes DHCP server functionality, or a local DHCP server in WLAN may allocate an IP address that the WLAN has received via Wr.)

Because the tunnel is established as part of WLAN session set-up, the UE can only have one IP connection at a time. If the UE wishes to change to another IP network, the UE may need to re-establish the WLAN session and use different IP network selection parameters.

### 5.5.3 UE-Initiated Tunneling

In UE-initiated tunneling, the UE initiates the establishment of tunnels and may be involved in packet encapsulation/decapsulation. The detailed mechanism is FFS and outside the scope of this document, however, the following steps are performed on WLAN session set-up:

1. EAP authentication between UE and 3GPP AAA Server. A WAPN may be transmitted as part of the end-to-end signalling. The WAPN indicates that the UE wishes to use UE-initiated tunneling.
2. The 3GPP AAA server decides that UE-Initiated tunneling shall be used for this session.
3. Filtering attributes may be needed in order to enable the WLAN to enforce that the UE tunnels all traffic as required. Filtering attributes may be transmitted from 3GPP AAA Server to WLAN over the Wr reference point. The WLAN sets up appropriate packet filters.

The tunnel establishment is not coupled to WLAN session establishment. The UE may establish several tunnels in order to access several IP network simultaneously. The actual IP network selection is performed as part of the establishment of each tunnel. Tunnel establishment and tunneling may be performed for example using Mobile IP.

## 5.6 Charging Requirements

- The W-LAN access network shall be able to report the W-LAN access usage to the appropriate 3GPP system
- It shall be possible for the 3GPP system to command some operations on a specific ongoing W-LAN access session. This can be useful in the context of prepaid processing.
- It shall be possible for an operator to maintain a single prepaid account for W-LAN, PS, CS, and IMS per user.
- It shall be the role of the 3GPP system to process the W-LAN access resource usage information into 3GPP compatible format (CDR).
- Charging correlation information shall be used for correlating charging and accounting records between WLAN Access related nodes and 3GPP Network nodes.

## 5.7 Charging Mechanisms

It shall be possible to apply offline charging and online charging mechanisms for the WLAN interworking with 3GPP network.

### 5.7.1 Offline Charging

Offline charging mechanism is provided forcollection and forwarding charging information about occurred WLAN access resource and core network resource usage, etc without affecting the service rendered in real-time.

### 5.7.2 Online Charging

Online charging mechanism is provided where the service rendered is affected in real-time and is required for a direct interaction with session/service control. This allows an online charged subscriber to access WLAN.

## 5.8 Network Selection Principles

If the WLAN radio technology allows for features enabling radio access network sharing or provider selection these shall be reused for network selection in 3GPP-WLAN interworking.

### 5.8.1 Case of IEEE 802.11 WLANs

In the case of IEEE 802.11 WLANs, the WLAN network name is provided in WLAN beacon signal in so called SSID (Service Set ID) information element. There is also the possibility for a UE to actively solicit support for specific SSIDs by sending a probe request message and receive a reply if the access point does support the solicited SSID. [IEEE 802.11-01/659r0]

Once confirmed the availability of one of the preferred SSIDs either in beacon or in a probe response message, WLAN UE performs association with the particular access point using the selected preferred SSID.

WLAN acting in 3GPP reference model as a DIAMETER client for transport of authentication exchanges carried in EAP, shalluse the used SSID as information that determines the first hop routing of DIAMETER frames, according to 3GPP reference model this implies selection of 3GPP AAA proxy. In this way the user can select either his/her home operator or its preferred roaming partner's 3GPP AAA proxy. 3GPP AAA Proxy then makes further AAA routing decision based on the NAI it has received.

To enable the PLMN Selection functionality for automatic processing SSID format would have to be standardized. SSID is 0-32 octets large (see IEEE 802.11-1999).

### 5.8.2 Case of HiperLan/2 WLANs

FFS

### 5.8.3 Case of Bluetooth WLANs

FFS

# 6 Interworking Architecture

## 6.1 Reference Model

*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.*

### 6.1.1 Non Roaming WLAN Inter-working Reference Model

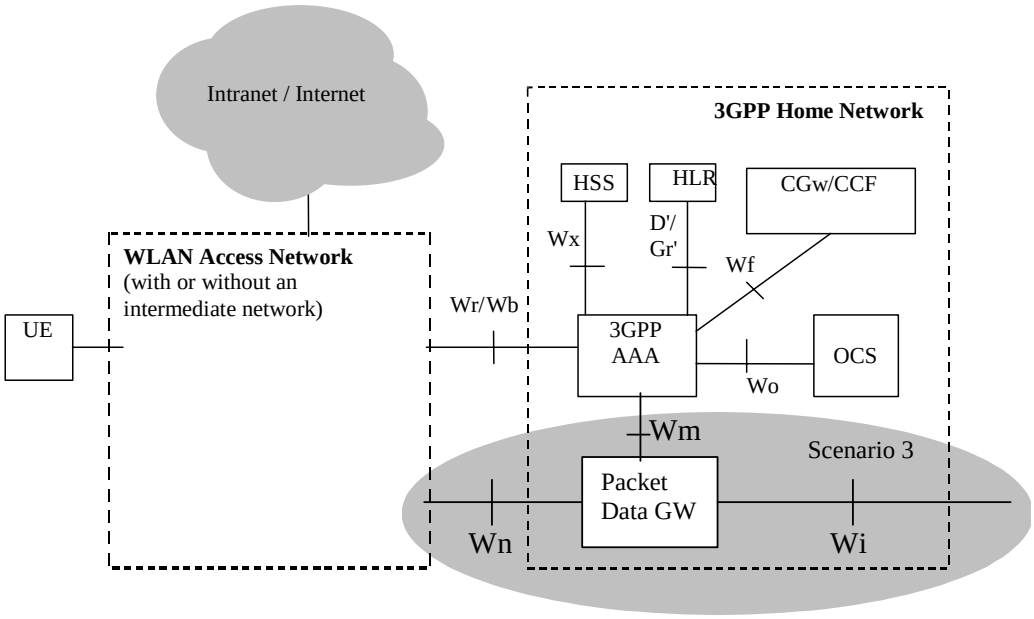



*figure 6.1 Non Roaming Reference Model. The shaded area refers to scenario 3 functionality.*

## 6.1.2 Roaming WLAN Inter-working Reference Model

### 6.1.2.1 WLAN Roaming Architecture Principles

For the delivery of 3GPP PS domain services in a roaming scenario;

- The roaming architecture shall ensure that CDRs can be generated e.g. volume and time based by the visited network
- The roaming architecture shall ensure that tunnels established are between entities that have a roaming agreement
- The roaming architecture shall ensure that the bearer path from the WLAN to 3GPP home network part of the network conforms with QoS and roaming agreement.
- The roaming architecture shall provide the ability to allow the user to access services provided by the visited network, e.g. IMS local services.
- The roaming architecture shall ensure that the home network can provide a sub-set of the 3GPP services.

### 6.1.2.2 WLAN Roaming Reference Model

The home network is responsible for access control. Charging records can be generated in the visited and/or the home 3GPP networks. The Wx and Wo interfaces are intra-operator. The 3GPP network interfaces to other 3GPP networks, WLANs, and intermediate networks via the Wr and Wb interfaces.

The 3GPP proxy AAA relays access control signalling and accounting information to the home 3GPP AAA server.

It can also issue charging records to the visited network CGw/CCF when required.

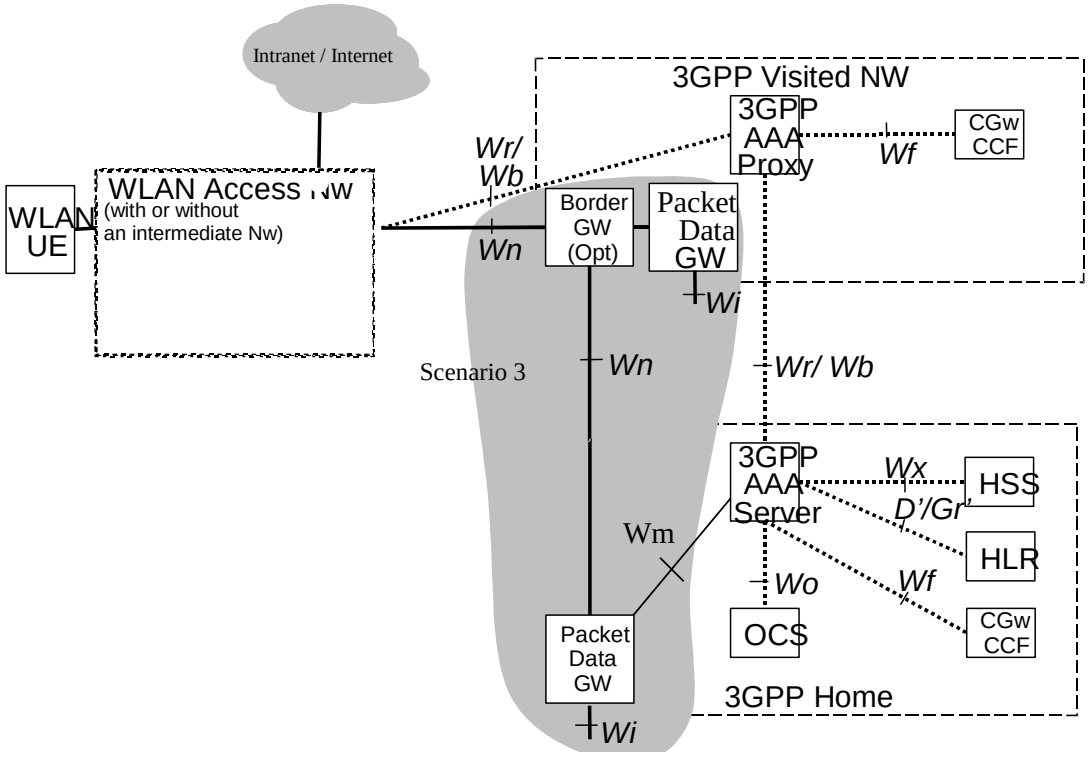



*Figure 6.2 Roaming Reference Model. The shaded area refers to scenario 3 functionality.*

## 6.2 Network elements

### 6.2.1 WLAN UE

- the UE (equipped with (U)ICC card including (U)SIM) utilised by a 3GPP subscriber to access the WLAN interworking service. The UE may be capable of WLAN access only, or it may be capable of both WLAN and 3GPP System access. Some UE may be capable of simultaneous access to both WLAN and 3GPP systems. The UE may include terminal types whose configuration (e.g. interface to a (U)ICC), operation and software environment are not under the exclusive control of the 3GPP system operator, such as a laptop computer or PDA with a WLAN card, (U)ICC card reader and suitable software applications.

### 6.2.2 3GPP AAA Proxy

- the 3GPP proxy AAA represents a Diameter proxying and filtering functionthat resides in the visited 3GPP network. The 3GPP proxy AAA functions include.:

- Relay the AAA information between WLAN and the 3GPP AAA Server.
- Enforce policies derived from roaming agreements between 3GPP operators and between WLAN operator and 3GPP operator
- Report charging/accounting information to local CCF/CGw for roaming users
- Service termination (O&M initiated termination from visited NW operator)
- Receives authorization information (Subscriber information)
- Forwarding authorization information to WLAN
- Rejection of authorization according to local policy

The 3GPP proxy AAA functionality can reside in a separate physical network node, it may reside in the 3GPP AAA server or any other physical network node.

### 6.2.3 3GPP AAA Server

- the 3GPP AAA server is located within the 3GPP network. The 3GPP AAA server :

  o retrieves authentication information and subscriber profile (including subscriber's authorisation information) from the HLR/HSS of the 3GPP subscriber's home 3GPP network;

  o authenticates the 3GPP subscriber based on the authentication information retrieved from HLR/HSS. The authentication signalling may pass through AAA proxies.

  o communicates authorisation information to the WLAN potentially via AAA proxies.

  o registers its (the 3GPP AAA server) address or name with the HLR/HSS for each authenticated and authorised 3GPP subscriber.

  o initiates the Purge procedure when the 3GPP AAA server deletes the information of a subscriber.

  o may act also as a AAA proxy (see above).

Editor's note : Clarification on the caching functionality is for further study

### 6.2.4. HLR/HSS

- the HLR/HSS located within the 3GPP subscriber's home network is the entity containing authentication and subscription data required for the 3GPP subscriber to access the WLAN interworking service.

Additional network elements in scenario 3:

### 6.2.5 Border Gateway

Support of BG in scenario 2 is optional

- The Border Gateway is an optional gateway via which the data to/from the WLAN Access Network.can be routed via a PLMN.
- The Border Gateway support is subject to local agreement between the WLAN AN and the VPLMN, in the roaming case, and between the WLAN AN and the HPLMN, in the non-roaming case.

The Border Gateway:

- Enables generation of aggregate charging for users accessing via the WLAN AN (scenario 2), e.g., to verify the charging records generated by the WLAN AN
- 
- Enables the (V)PLMN to implement portal functionality for users accessing via the WLAN AN, e.g., for scenario 2

The definition of the interface between WLAN AN and PLMN and the operation of the WLAN Border Gateway are subject to local agreement and are not specified by 3GPP. However, in order to demonstrate support for the WLAN border gateway, informative examples of such connectivity between WLAN AN and PLMN are described in an informative annex.

Editor's note : the use of the BGW in sc.3 is ffs.

~~The Border Gateway is an optional gateway via which the data between WLAN and Packet Data Gateway can be routed.~~

### 6.2.6 Packet Data Gateway

- The Packet Data Gateway is a node via which packet data networks are connected to 3GPP interworking WLAN. The location of Packet Data Gateway may be different for each specific service accessed WLAN. For some WLAN connections no Packet Data Gateway is used, for some accessed services Packet Data Gateway may be in home network and for some accessed services it may locate in visited Nw.

  The Packet Data Gateway:

  - contains routeing information for WLAN-3G connected users;
  - routes the packet data received from/sent to the PDN to/from the WLAN-3G connected user;
  - performs address translation and mapping;
  - performs encapsulation;
  - generates charging information related to user data traffic for offline and online charging purposes.

## 6.3Reference Points

### 6.3.1 Wr

#### 6.3.1.1 General description

The reference point Wr connects the WLAN access network, possibly via intermediate networks, to the 3GPP AAA Server. The prime purpose of the protocols crossing this reference point is to transport authentication, authorization and related information in a secure manner. The reference point has to accommodate also legacy WLAN access networks and thus should be DIAMETER or RADIUS-based.

#### 6.3.1.2 Functionality

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

- Carrying data for authentication signalling between WLAN UE and 3GPP AAA Server
- Carrying data for authorization signalling between WLAN AN 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

#### 6.3.1.3 Protocols

Wr reference shall be based on IETF Diameter Base protocol. EAP authentication shall be transported over *Wr* reference point by Diameter Extensible Authentication Protocol (EAP) Application.,

*[Editors note: Diameter base protocol is work in progress in IETF [draft-ietf-aaa-diameter-12.txt ]]*

*[Editors note: Diameter Extensible Authentication Protocol (EAP) Application is work in progress in IETF [draft-ietf-aaa-eap-00.txt]]*

To support legacy logical nodes outside of 3GPP scope and which terminate or proxy the Wr reference point signalling and not supporting Diameter protocol, a signalling conversion between RADIUS and Diameter may be performed. [11]. Editor's note: this issue requires further study. ~~This conversion is not specified by 3GPP.~~

It should also be noted that RADIUS does not support all the Diameter features. Therefore, this conversion might limit the usage of features existent in Diameter but not existent in RADIUS (e.g. filtering rules).

### 6.3.2 Wx

This reference point is located between 3GPP AAA Server and HSS. The prime purpose of the protocol(s) crossing this reference point is communication between WLAN AAA infrastructure and HSS. The protocol crossing this reference point is either MAP or DIAMETER-based.

The functionality of the reference point is to enable:

- Retrieval of authentication vectors, e.g. for USIM authentication, from HSS.
- Retrieval of WLAN access-related subscriber information (profile) from HSS
- Registration of the 3GPP AAA Server of an authorised WLAN user in the HSS.
- Indication of change of subscriber profile within HSS (e.g indication for the purpose of service termination).
- 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.

### 6.3.3 D'/Gr'

This reference point is located between 3GPP AAA Server and HLR. The prime purpose of the protocol(s) crossing this reference point is communication between WLAN AAA infrastructure and HLR. The protocol crossing this reference point is MAP-based.

The functionality of the reference point is to enable:

- Retrieval of authentication vectors, e.g. for USIM authentication, from HLR.
- Retrieval of online/offline function address from HLR.

D'/Gr' include a subset of D/Gr Reference Point.

### 6.3.4 Wb

The reference point Wb is located between WLAN access network and 3GPP network. The prime purpose of the protocols crossing this reference point is to transport charging-related information in a secure manner. The reference point has to accommodate also legacy WLAN access networks and thus should be DIAMETER or RADIUS-based.

The functionality of the reference point is to transport RADIUS/DIAMETER frames with:

- Charging signalling per each WLAN user

To minimize the requirements put on the WLAN Access Network and to protect the confidentiality of the subscribers charging status the fact whether a user is offline or online charged by his 3GPP subscription provider shall be transparent for the WLAN AN and thus for the Wb reference point.

### 6.3.5 Wo

Reference point Wo is used by a 3GPP AAA server to communicate with 3GPP Online Charging System (OCS). The prime purpose of the protocol(s) crossing this reference point is to transport online charging related information so as to perform credit control for the online charged subscriber.

The protocol(s) crossing this interface shall be DIAMETER-based.

The functionality of the reference point is to transport:

- Online charging data

Wo reference point should be similar to Ro interface currently used in 3GPP OCS.

### 6.3.6 Wf

The reference point Wf is located between 3GPP AAA Server and 3GPP Charging Gateway Function (CGF)/Charging Collection Function (CCF). The prime purpose of the protocols crossing this reference point is to transport/forward charging information towards 3GPP operator's Charging Gateway/Charging collection function located in the visited network or home network where the subscriber is residing.

The information forwarded to Charging Gateway/Charging collection function is typically used for:

- Generating bills for offline charged subscribers by the subscribers' home operator
- Calculation of inter-operator accounting from all roaming users. This inter operator accounting is used to settle the payments between visited and home network operator and/or between home/visited network and WLAN.

The protocol(s) crossing this interface is DIAMETER-based.

The functionality of the reference point is to transport:

- WLAN access-related charging data per each WLAN user

Additional reference points in scenario 3:

### 6.3.7 Wn

Reference point *Wn* indicates the reference point for transporting tunneled WLAN user data towards 3GPP system. Routing of *Wn* reference point is service specific. For accessing home network services the *Wn* may be routed directly between WLAN and Home 3GPP Network or forced to go via Border Gateway functionality within the Visited Network.

When the Packet Data GW is not provided for accessing the external IP networks, data can be directly routed from the WLAN access network towards the external IP network without passing 3GPP network.

### 6.3.8 Wi

This is the reference point between Packet Data GW and a packet data network. The packet data network may be an operator external public or private packet data network or an intra operator packet data network, e.g. the entry point of IMCN subsystem, RADIUS Accounting or Authentication, DHCP.

*Wi* reference point is similar to the *Gi* reference point provided by the PS domain. Interworking with packet networks is provided via the Wi reference point based on IP. Mobile terminals offered services via the Wi reference point may be globally addressable through the operators public addressing scheme or through use of a private addressing scheme. When 3GPP network is provided for IM CN subsystem, Wi reference point is used for policy control interface. It is ffs whether Wi or other reference point is used or not.

### 6.3.9 Wm

This reference point is located between 3GPP AAA Server and Packet Data Gateway. The functionality of this reference point is to enable:

- The 3GPP AAA Server to retrieve tunneling attributes and UE's IP configuration parameters from/via Packet Data Gateway.

The protocol crossing this reference point is Diameter.

# 7 Procedures

## 7.1 Authentication and Authorisation

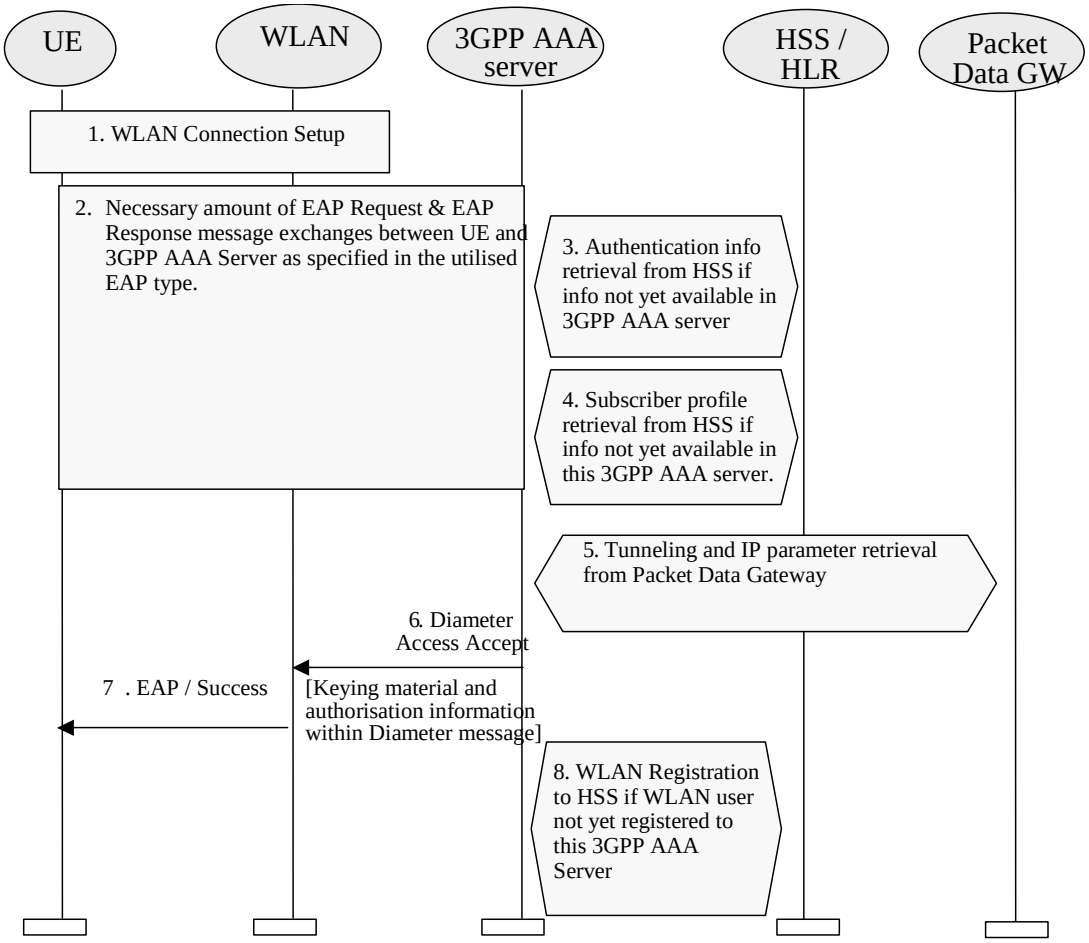



*Figure 7.1Authentication and authorisation procedure*

1. WLAN connection is established with a Wireless LAN technology specific procedure (out of scope for 3GPP).

2. The EAP authentication procedure is initiated in WLAN technology specific way.

All EAP packets are transported over the Wireless LAN interface encapsulated within a Wireless LAN technology specific protocol.

All EAP packets are transported over the Wr reference point encapsulated within Diameter messages as specified in Diameter EAP application .

*[Editors note: Diameter Extensible Authentication Protocol (EAP) Application is work in progress in IETF [draft-ietf-aaa-eap-00.txt]]*

A number of EAP Request EAP Response message exhanges is executed between 3GPP AAA Server and UE. The amount of round trips depends e.g. on the utilised EAP type. Information stored in and retrieved from HSS may be needed to execute certain EAP message exchanges.

3 Information to execute the authentication with the accessed user is retrieved from HSS. This information retrieval is needed only if necessary information to execute the EAP authentication is not already available in 3GPP AAA Server. To identify the user the *username* part of the provided NAI identity is utilised.

4 Subscribers WLAN related profile is retrieved from HSS. This profile includes e.g. the authorisation information and permanent identity of the user. Retrieval is needed only if subscriber profile information is not already available in 3GPP AAA Server.

5 Tunneling and IP parameters may be retrieved from/via Packet Data Gateway over the Wm reference point. Note that this only applicable to scenario 3.

6 If the EAP authentication was successful, then 3GPP AAA Server sends Diameter Access Accept message to WLAN. In this message 3GPP AAA Server includes EAP Success messge, keying material derived from the EAP authentication as well as connection authorisation information (e.g. NAS Filter Rule or Tunneling attributes ) to the WLAN.

WLAN stores the keying material and authorisation information to be used in communication with the authenticated UE.

7 WLAN informs the UE about the successful authentication with the EAP Success message.

8 3GPP AAA server registers the WLAN users 3GPP AAA Server to the HSS. In registration messages the subscriber is identified by his permanent identity. This registration is needed only if the subscriber is not already registered to this 3GPP AAA Server.

## 7.2 Subscriber Profile Update

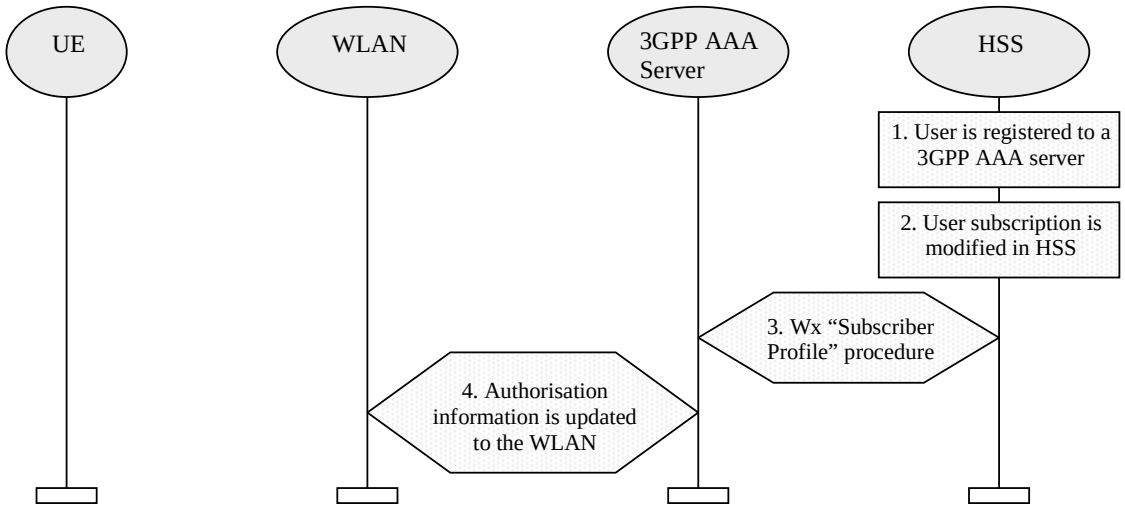



*Figure 7.2 Subscriber Profile Update Procedure*

1. User is registered to a 3GPP AAA server

2. Subscribers subscription is modified inthe HSS e.g. via O&M.

3. HSS updates the profile information stored in the registered 3GPP AAA server by Wx reference point procedure "Subscriber Profile".

4. The authorisation information of the associated connection is updated to WLAN as necessary.

## 7.3 Canceling WLAN Registration

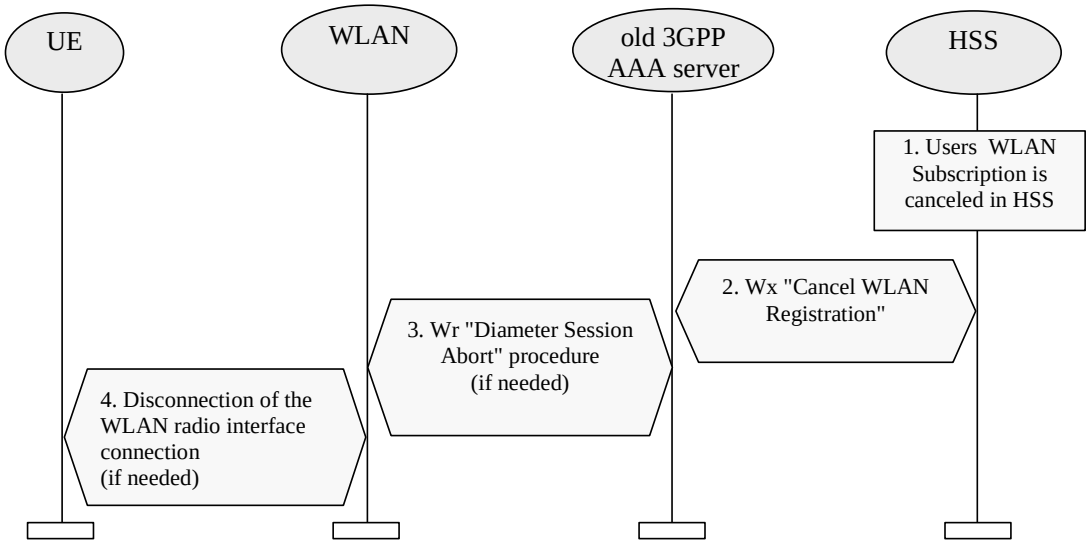



*Figure 7.3 Cancellation of WLAN Registration Procedure*

1. The 3GPP subscribers WLAN subscription is canceled in HSS.

2. HSS cancels subscribers WLAN registration in the 3GPP AAA Server by Wx reference point procedure "Cancel WLAN Registration". In the messages subscriber is identified by his permanent identity.

3. If the subscribers connection still exists, Wr reference point procedure "Diameter Session Abort" procedure is executed towards WLAN.

4. If the radio connection still exists, WLAN disconnects the radio interface connection by WLAN technology specific mechanisms.

## 7.4 Disconnecting a Subscriber by WLAN

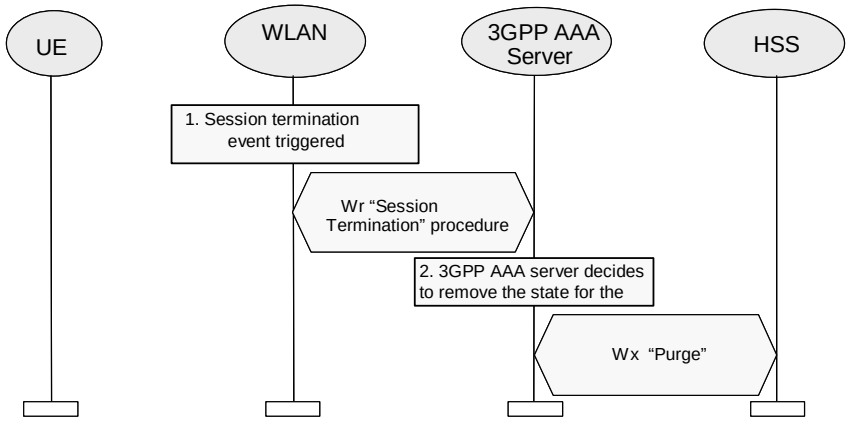



*Figure 7.4 WLAN initiated disconnection procedure*

1. WLAN detects that a Session related to a UE should be terminated towards the 3GPP AAA Server, e.g. when the UE has disappeared from WLAN coverage.

WLAN initiates Wr Session Termination procedure towards 3GPP AAA server.

In case when the 3GPP AAA server decides to remove the UEs state from the 3GPP AAA server, the 3GPP AAA server notifies HSS using Wx procedure "Purge" that the WLAN registration in the 3GPP AAA Server has been cancelled. HSS removes the state related to that 3GPP AAA server, e.g., the address of the serving 3GPP AAA server for the identified subscriber.

## 7.5 Disconnecting a Subscriber by Online Charging System

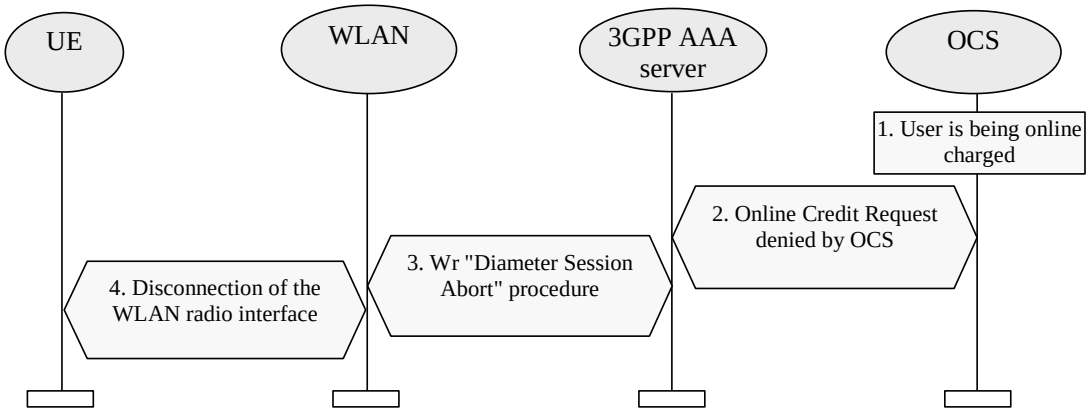



*Figure 7.5 OCS Initiated Disconnection Procedure*

1. A subscriber is being online charged by 3GPP AAA server.

2. OCS (online Charging System) denies credit request from the 3GPP AAA server for WLAN access. The possibly already retrieved online credit runs out.

3. To disconnect the subscribers connection, *Wr* reference point procedure "Diameter Session Abort" procedure is executed towards WLAN.

4. WLAN disconnects the radio interface connection by WLAN technology specific mechanisms

## 7.6 Charging offline charged subscribers

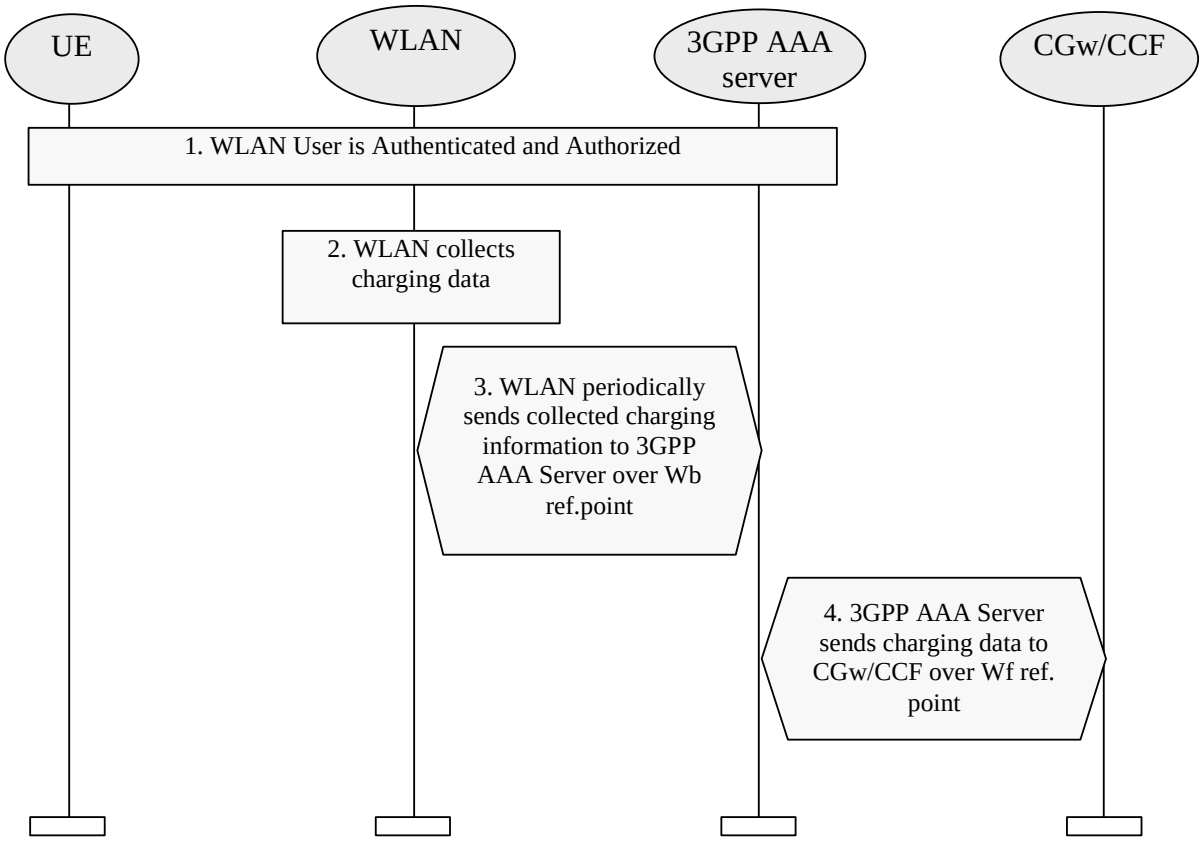



*Figure 7.6 Charging Procedure for Offline Charged Subscribers*

1. WLAN user is authenticated and authorized for WLAN access. User profile is downloaded into 3GPP AAA server. Part of the profile is information that the user is to be offline charged.

2. WLAN access network collects charging data related to access or services locally consumed.

3. WLAN access network periodically forwards collected charging information to the 3GPP AAA server over Wb reference point.

4. 3GPP AAA server forwards charging information to the CGw/CCF over the Wf reference point.

*Note: In visited network the 3GPP AAA Proxy may also periodically report the usage of resources to the local CGw/CCF over Wf reference point.*

# 7.7 Charging online charged subscribers

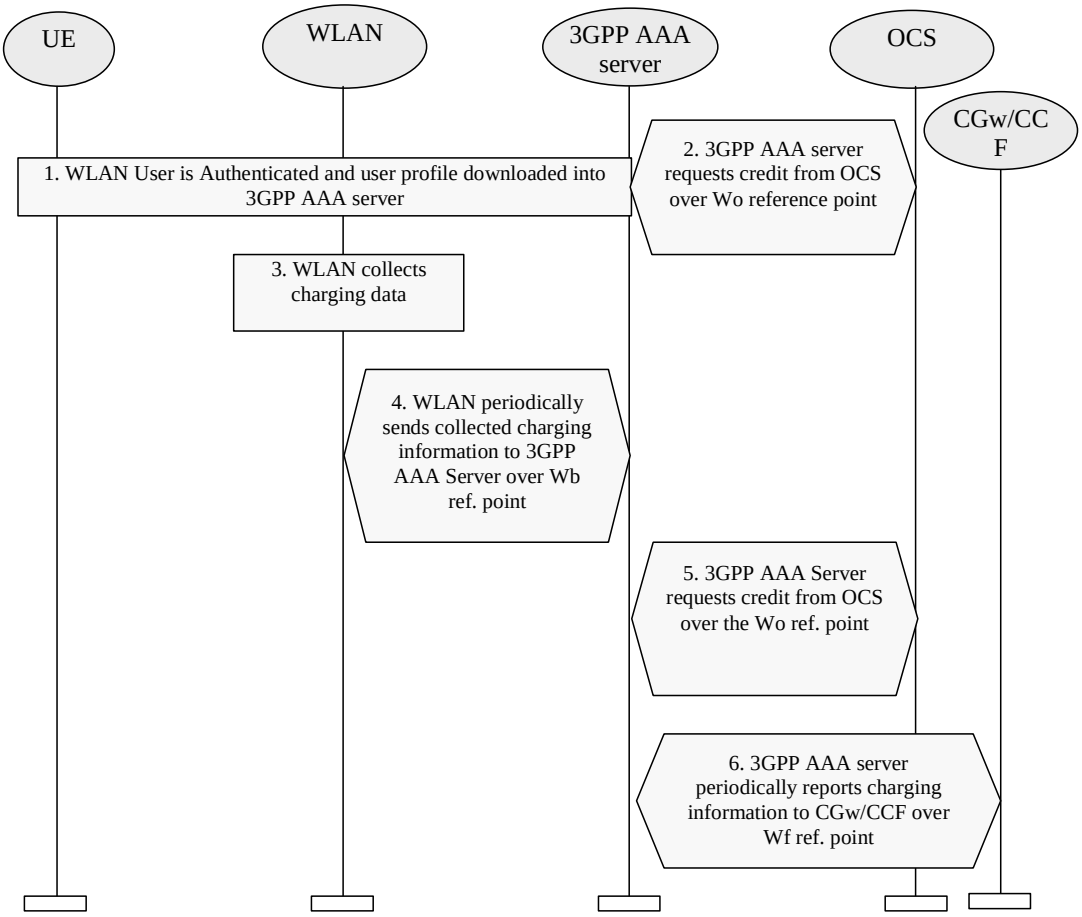



*Figure 7.7 Charging Procedure for Online Charged Subscribers*

1. WLAN user is authenticated and authorized for WLAN access. User profile is downloaded into 3GPP AAA server. Part of the profile is information that the user is to be online charged.

2. 3GPP AAA server obtains online charging credit from the OCS.

3. WLAN access network collects charging information.

4. WLAN access network periodically forwards collected charging information to the 3GPP AAA server over Wb reference point. WLAN access network does not request charging credit as the fact whether a user is online of offline charged is transparent for it.

5. If the credit is to be exceeded, 3GPP AAA server requests further credit from OCS over the Wo reference point.

6. 3GPP AAA server periodically reports to usage of resources to the CGw/CCF over Wf reference point. The purpose of this reporting is to enable inter-operator clearing.

*Note: In visited network the 3GPP AAA Proxy may also periodically report the usage of resources to the local CGw/CCF over Wf reference point.*

# Annex A (informative): Refererence Points Signalling Flows

## A.1 Signalling Sequences examples for Wr Reference Point

### A.1.1 Authentication, Authorisation and Session Key delivery

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

This Wr 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.

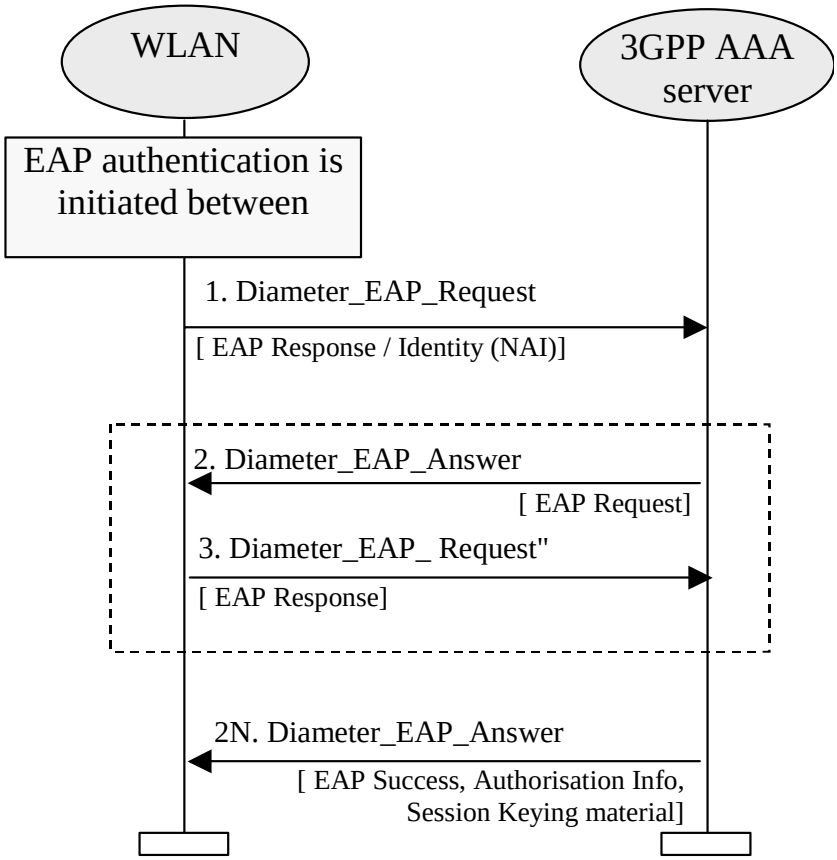



*Figure A.1.1 Signalling example on Wr Reference Point for Authentication and Authorisation*

1. The WLAN initiates authentication procedure towards 3GPP network by sending Diameter_EAP_Request message to 3GPP AAA Server. This Diameter message 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. 3GPP AAA Server performs the authentication procedure based on information retrieved from HSS/HLR. 3GPP AAA Server sends message Diameter_EAP_Answer to WLAN. This message carries encapsulated EAP Request message. The content of the EAP Request message is dependent on the EAP type being used. WLAN conveys the EAP Request message to the UE.

3. UE responds to WLAN by a EAP Response message. WLAN encapsulates it into Diameter_EAP_Request message and sends it to 3GPP AAA Server. The contents of the EAP Response message is dependent on the EAP type being used.

The number of roundtrip Diameter signalling exchanges similar to the signal pair 2 and 3 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 to WLAN. 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 Tunneling 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 the 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 canceled 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.

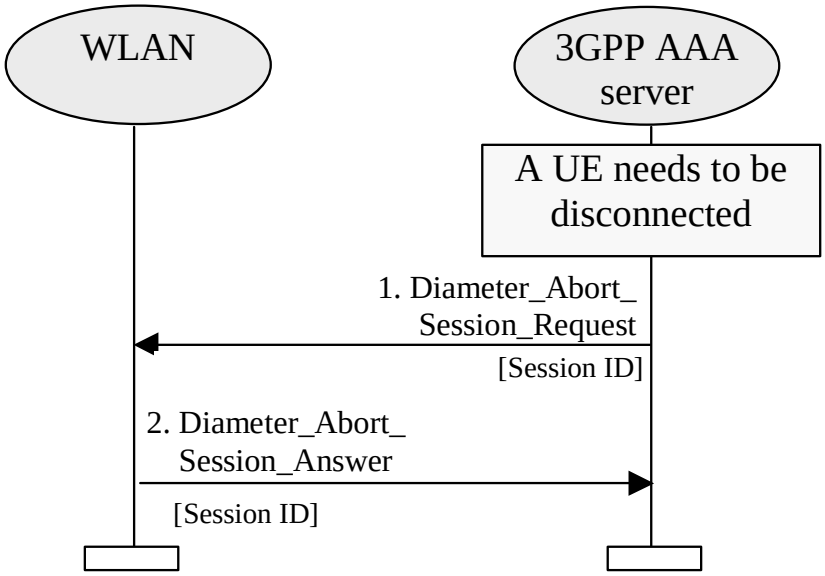



*Figure A.1.2 Signalling example on Wr Reference Point for User Purging*

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 WLAN . This message contains the Session ID by which the session is identified within WLAN.

2. WLAN responds by Diameter_Abort_Session_Answer as defined in Diameter.

# A.2 Signalling Sequences examples for Wx Reference Point

## A.2.1 Authentication Information Retrieval

This signalling sequence is initiated by a 3GPP AAA Server when a new set of authentication information for a given subscriber is to be retrieved from an HSS/HLR.

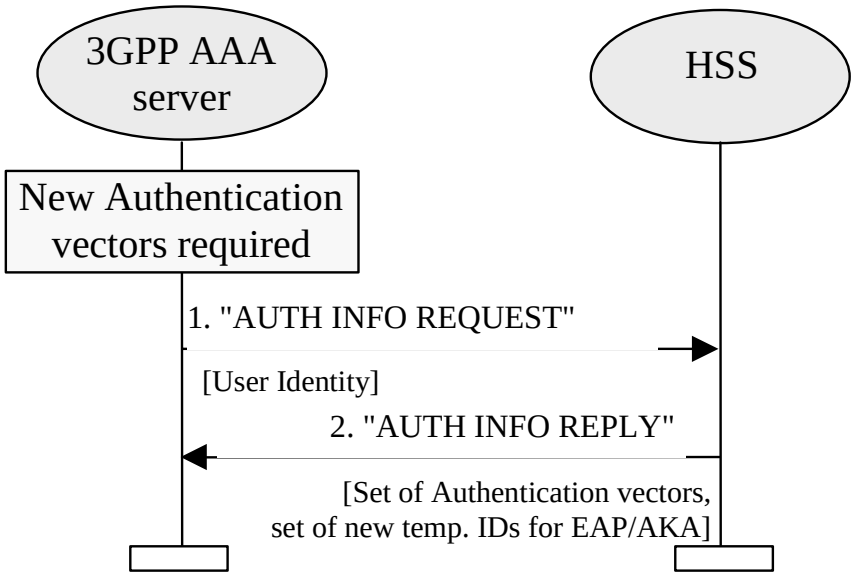



*Figure A.2.1 Signalling example on Wx Reference Point for Authentication Information Retrieval*

1. 3GPP AAA server detects that it requires new authentication vectors for a given 3GPP subscriber. 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.

   3GPP AAA server sends "AUTH INFO REQUEST" message to the HSS/HLR requesting a set of authentication vectors. In the message the subscriber is identified by a unique identifier which is used as the username part of the NAI identity.

   In case of USIM authentication (EAP/AKA) the utilised unique identifier shall be the pseudonym (associated with the IMSI) allocated in a previous authentication or, in case of the very first authentication, the IMSI.

*Note : For USIM authentication (EAP/AKA) it is ffs whether the temporary identifiers should instead of HSS/HLR be allocated in the 3GPP AAA Server, i.e. whether IMSI or Temporary identifier Is used as user identity over Wx.*

2. HSS/HLR replies by a "AUTH INFO REPLY" message containing the requested authentication vectors.

   For USIM authentication (EAP/AKA) HSS/HLR has also allocated a new set of pseudonyms for the subscriber to be given to the subscriber in each subsequent authentication.

*Note: It is ffs whether the temporary identifiers should instead of HSS/HLR be allocated in the 3GPP AAA Server*

   In case of UMTS AKA authentication, each authentication vector consists of RAND, XRES, AUTN, CK, and IK.

   3GPP AAA Server stores the authentication vectors and pseudonyms to be used in future authentication procedures for the subscriber.

### A.2.2 Subscriber Profile Retrieval

This signalling sequence is initiated by a 3GPP AAA Server when a new subscriber has accessed the 3GPP AAA server and the subscription profile information of that subscriber is not available in the 3GPP AAA server. This signalling sequence can also be used if for some reason the subscription profile of a subscriber is lost. Subscription profile contains e.g. authorisation information.

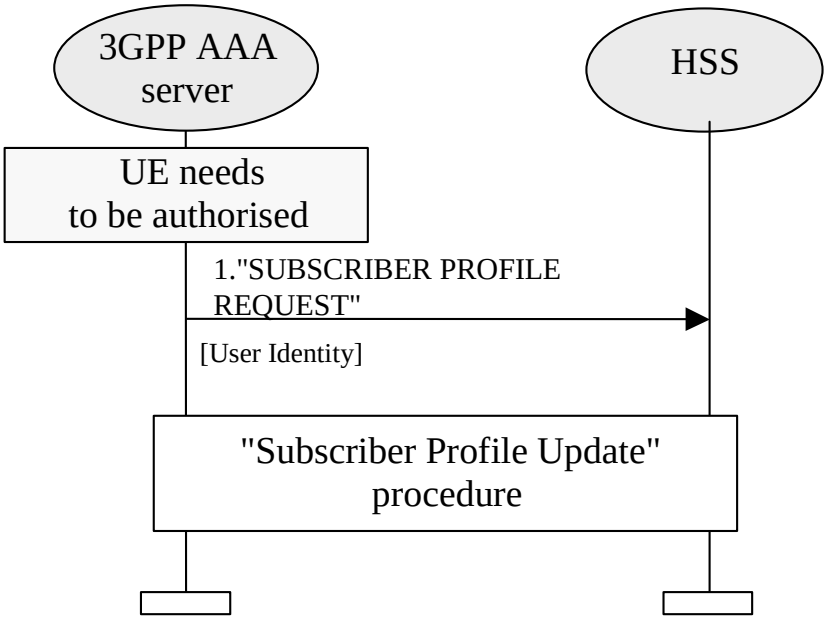



*Figure A.2.2 Signalling example on Wx Reference Point for Subscriber Profile Retrieval*

1. 3GPP AAA server detects that it requires the subscription profile for a given 3GPP subcriber. For example. this can happen when a new subscriber has accessed the 3GPP AAA Server for authentication.

   3GPP AAA server sends "SUBSCRIBER PROFILE REQUEST" message to the HSS/HLR requesting the

subscriber's profile to be downloaded to the 3GPP AAA server. In the message the subscriber is identified by a unique identifier which is used as the username part of the NAI identity.

In case of USIM authentication (EAP/AKA) the utilised unique identifier shall be the pseudonym (associated with the IMSI) allocated in the previous authentication or, in case of the very first authentication, the IMSI.

*Note : it is ffs whether the temporary identifiers should instead of HSS/HLR be allocated in the 3GPP AAA Server, i.e. whether IMSI or Temporary identifier Is used as user identity over Wx.*

2. At reception of "SUBSCRIBER PROFILE REQUEST" message, the HSS/HLR initiates a Subscriber Profile Update procedure towards the 3GPP AAA Server. The Subscriber Profile Update procedure is explained in the following subchapter.

### A.2.3 Subscriber Profile Update

This signalling sequence is initiated by the HSS/HLR when subscriber profile needs to be sent to a 3GPP AAA server. This can be due to an explicit request from the 3GPP AAA Server or due to a modification or cancellation of subscription in the HSS/HLR.

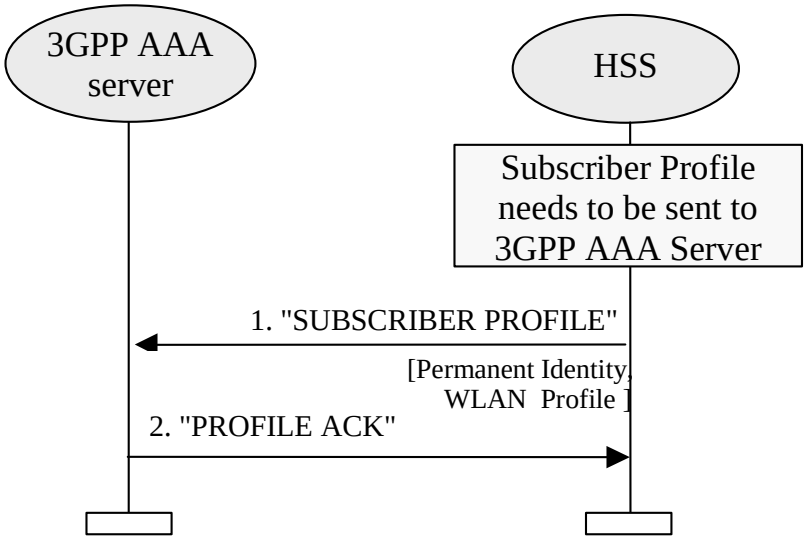



*Figure A.2.3 Signalling example on Wx Reference Point for Subscriber Profile Update*

1. HSS/HLR initiates the signalling when a subscriber profile needs to be sent to a 3GPP AAA server. This can be due to an explicit request from the 3GPP AAA Server or due to a modification or cancellation of subscription in the HSS/HLR.

   HSS/HLR sends "SUBSCRIBER PROFILE" message to 3GPP AAA Server. For example. this message includes
   - Users permanent unique identifier. In case of USIM authentication (EAP/AKA) the utilised

unique identifier shall be the IMSI,
- service authorisation information,

- charging mechanism (offline / online),
- in case of online charging. the DNS name of the subscribers online charging system

3GPP AAA Server stores the subscriber profile information.

2. 3GPP AAA Server acknowledges the reception of the subscriber profile information by sending "PROFILE ACK" message to the HSS/HLR.

### A.2.4 WLAN Registration

This signalling sequence is initiated by the 3GPP AAA Server when a new subscriber has been authenticated and authorised by the 3GPP AAA server. The purpose of this procedure is to register the current 3GPP AAA Server address in the HSS/HLR.

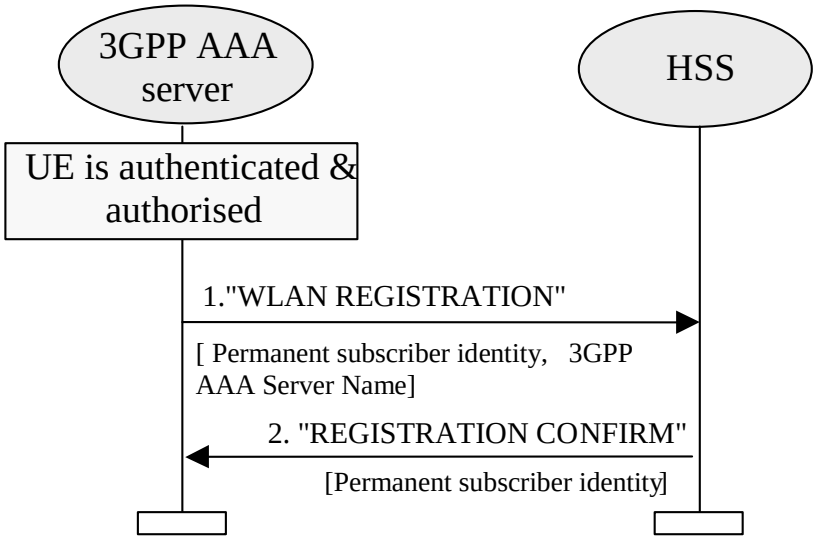



*Figure A.2.4 Signalling example on Wx Reference Point for Subscriber Registration*

1. 3GPP AAA server initiates the signalling when a new 3GPP subscriber has been authenticated and authorised by the 3GPP AAA server. 3GPP AAA server sends WLAN REGISTRATION message to the HSS/HLR. This message contains the address/name of the 3GPP AAA Server and the permanent subscriber identifier. In case of USIM authentication (EAP/AKA) the utilised unique identifier shall be the IMSI.

2. HSS/HLR confirms the reception of the WLAN REGISTRATION message by REGISTRATION CONFIRM message.

## A.2.5 Cancel Registration

This signalling sequence is initiated by a HSS when subscription has to be removed from 3GPP AAA Server. This can happen when the subscription is cancelled in HSS.

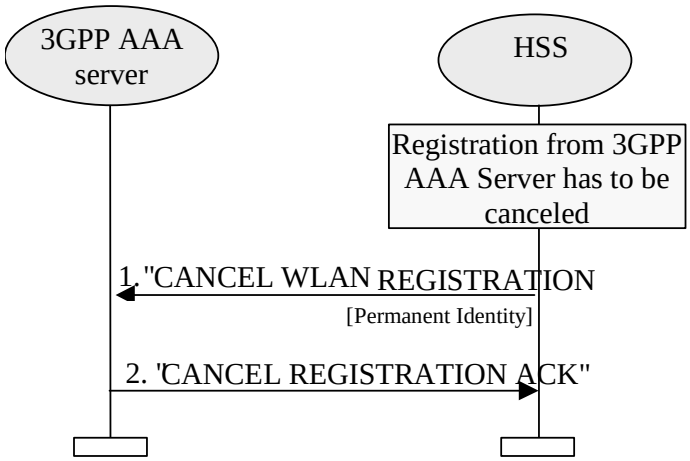



*Figure A.2.5 Signalling example on Wx Reference Point for Registration Cancellation*

1. HSS/HLR initiates the signalling when the registration of a 3GPP subscriber has to be canceled from a 3GPP AAA server. Subscriber is identified by his permanent user identity.

2. 3GPP AAA Server confirms the reception of the CANCEL WLAN REGISTRATION message by CANCEL REGISTRATION ACK message.

## A.2.6 Purge Function for WLAN inter-working

The Purge function allows a 3GPP AAA server to inform the HSS that it has deleted the information of a disconnected (either logged off or exceptionally disconnected from the WLAN inter-working service) subscriber. The 3GPP AAA server may, as an implementation option, delete the information of a subscriber immediately after the implicit or explicit logging off of the subscriber. Alternatively, the 3GPP AAA server may keep the information of the disconnected subscriber for some time, such as the subscriber profile and the authentication information retrieved from the HSS, so that the information can be reused at a later connection period without accessing the HSS.

When the 3GPP AAA server deletes the information of a subscriber, it shall initiate the Purge procedure as illustrated in the following figure. Each step is explained in the following.

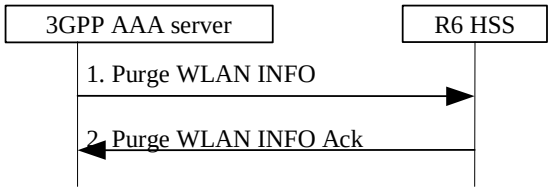



*Figure A.2.6 Signalling example on Wx Reference Point for Purge Procedure*

1) After deleting the information of a disconnected subscriber, the 3GPP AAA server sends a Purge WLAN INFO message to the -HSS.

2) The HSS record a “WLAN INFO Purged” value and acknowledges with a Purge WLAN INFO Ack message.

# A.3 Signalling Sequences examples for D' Reference Point

## Authentication Information Retrieval

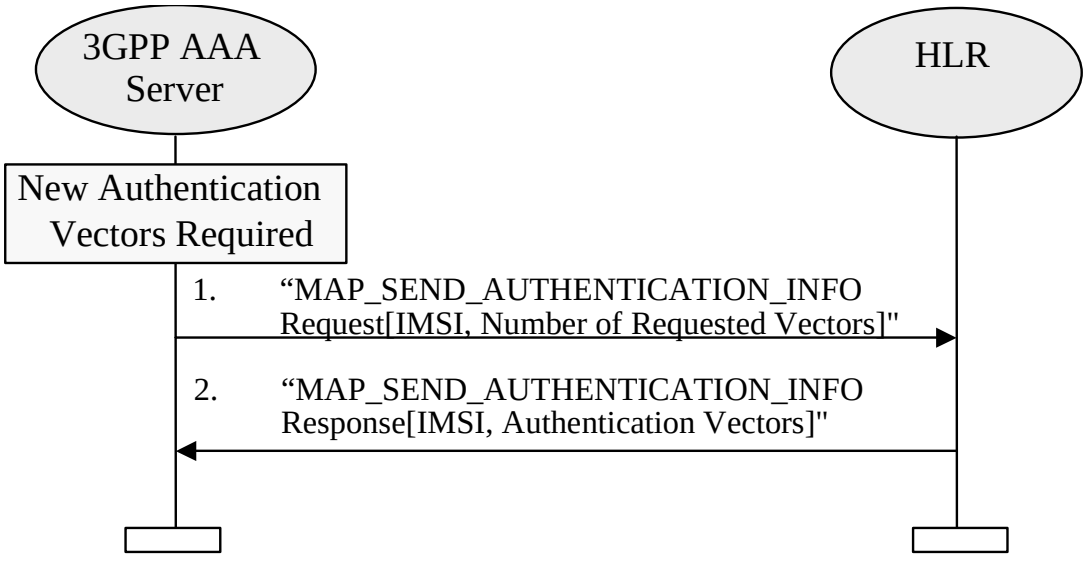



*Figure A.3.1 Authentication Information Retrieval using D' interface*

1. 3GPP AAA server detects that it requires new authentication vectors for a given 3GPP subscriber. 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.

3GPP AAA server sends "MAP_SEND_AUTHENTICATION_INFO Request" message to the HSS/HLR requesting a set of authentication vectors. In the message, the subscriber is identified by a unique identifier, IMSI.

2. HSS/HLR replies by a " MAP_SEND_AUTHENTICATION_INFO Response" message containing the requested authentication vectors.

In case of UMTS AKA authentication, each authentication vector consists of RAND, XRES, AUTN, CK, and IK.

## Subscriber Profile Retrieval

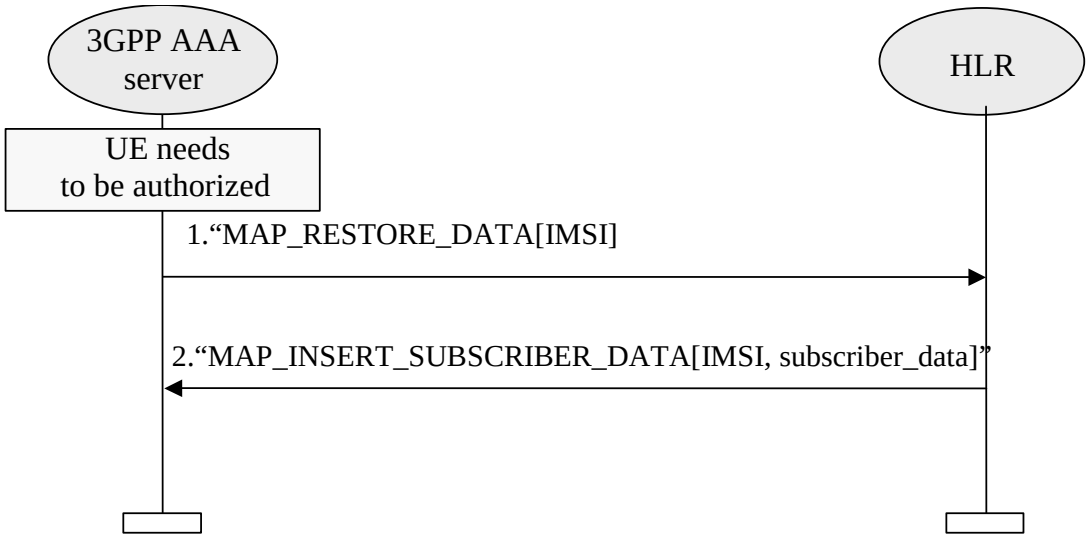



*Figure A.3.2 Subscriber Profile Retrieval using D' interface*

1. 3GPP AAA server detects that it requires the subscription profile for a given 3GPP subscriber. For example, this can happen when a new subscriber has accessed the 3GPP AAA Server for authentication.

   3GPP AAA server sends "MAP_RESTORE_DATA" message to the HSS/HLR requesting the subscriber's profile to be downloaded to the 3GPP AAA server. In the message the subscriber is identified by IMSI.

2. At reception of "MAP_RESTORE_DATA" message, the HSS/HLR initiates a MAP_INSERT_SUBSCRIBER_DATA procedure towards the 3GPP AAA Server.

Since pre-R6 Subscriber Data records in HLR do not have any standardized information related to WLAN subscription, the choice and interpretation of the retrieved data is left up to the operator.

# A.4 Gr' Signalling Mechanisms to support WLAN service

## Introduction

**The following sections describe the use of existing GPRS parameters and signaling mechanisms to support the WLAN services when interworking with legacy HLRs.**

The table shows a list of parameters in existing HLR and suggests possible use in context of WLAN operation. However actual use and interpretation is left to the operator.

| Existing GPRS parameter | Possible WLAN use |
|---|---|
| IMSI | Subscribers Identity |
| PDP Context subscription record | Services Subscriber has access to |
| VPLMN Address Allowed | Subscriber's ability to use service while roaming |
| SGSN Number, SGSN Address | Indicate the serving 3GPP AAA Server |
| Authentication Vectors | Authentication and ciphering |

**Following procedures are relevant between 3GPP AAA Server and HLR with respect to the information identified above. These messages are exchanged over the Gr' interface..**

- **Authentication information retrieval via infoRetrieval procedure**
- **Subscriber Information retrieval via gprsLocationUpdate procedure**
- **Deletion of subscription via cancelLocation procdeure.**

**It is important to note that use of gprsLocationUpdate procedure from WLAN will detach the subscriber from GPRS.**

Further proprietary work with possible impact to existing HLR and/or SGSNs is necessary to support simultaneous connections when Gr' signaling is used for WLAN purposes.

### infoRetrieval procedure:

**Using this procedure the 3GPP AAA server can request for the Authentication Vectors for the user (IMSI) by initiating SEND-AUTHENTICATION-INFO message to HLR. HLR/AuC validates the user (IMSI) and generates Authentication Vectors and responds back with SEND-AUTHENTICATION-INFO-ACK message that contains the generated Authentication Vectors.**

**The infoRetrieval (Authentication) procedure is illustrated in Figure X below.**

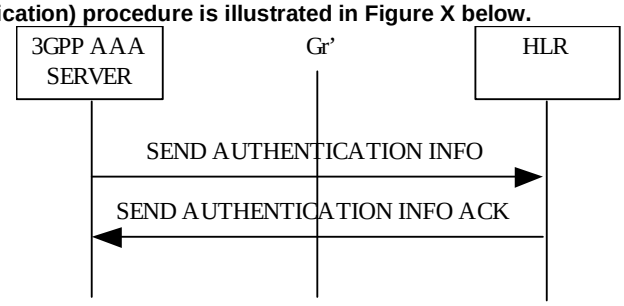



**Figure X. infoRetrieval procedure**

### gprsLocationUpdate procedure:

**Using this procedure the 3GPP AAA server can update the HLR with the local storage area information of the user and request HLR for the subscriber information (services, roaming, etc). 3GPP AAA server initiates this procedure by sending UPDATE-LOCATION message with the local storage area information. HLR sends the subscriber information through INSERT-SUBSCRIBER-DATA, which 3GPP AAA server acknowledges . HLR repeats the above procedure until all the data is sent. On successful completion of above procedure HLR responds with UPDATE-LOCATION-ACK message.**

**The gprsLocationUpdate (Subscriber Information retrieval) procedure is illustrated in Figure X.1 below.**

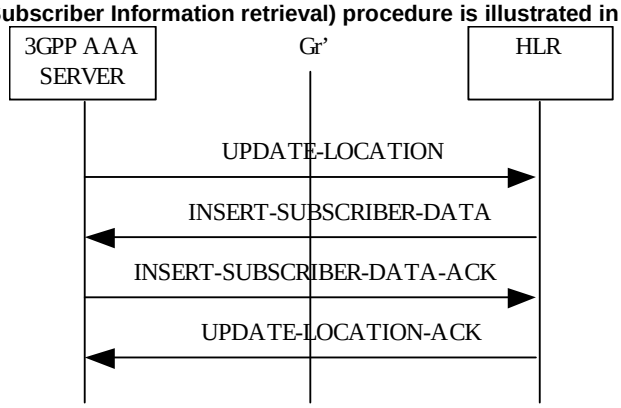



**Figure X.1. gprsLocationUpdate procedure**

## A.5 Example of Authentication procedures

### A.5.1 EAP/AKA Procedure

USIM based authentication may be based on existing AKA method. In the case of WLAN-3GPP system interworking, this method should be supported by a generic authentication mechanism (independently of the underlying WLAN standard), e.g. EAP. EAP/AKA authentication mechanism is described in Internet Draft draft-arkko-pppext-eap-aka.

The current version is 05 (draft-arkko-pppext-eap-aka-05.txt). The following procedure is based on EAP/AKA authentication mechanism:

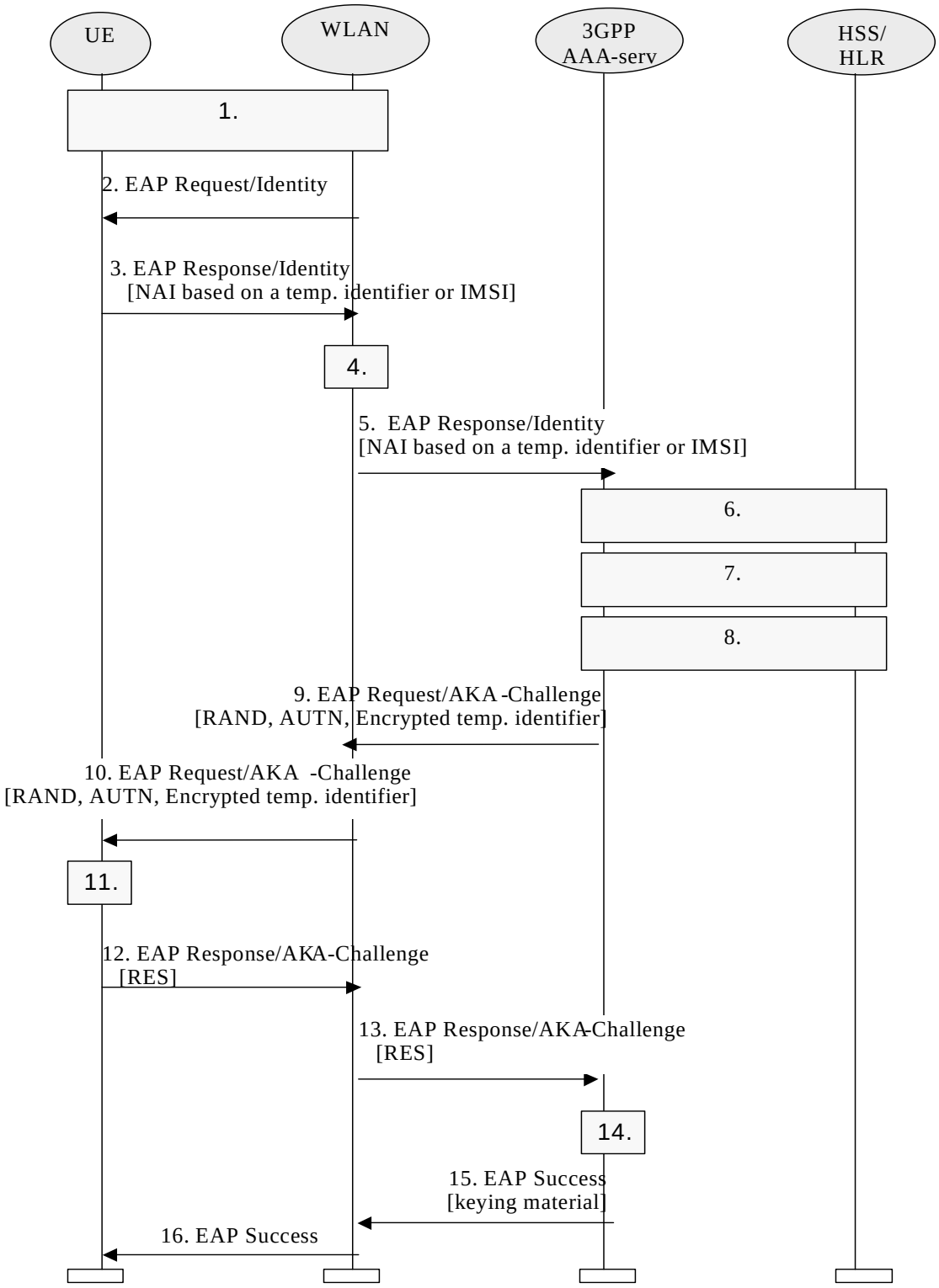



*Figure A.4.1 Authentication based on EAP AKA scheme*

1. After WLAN connection establishment, Extensible Authentication Protocol is started with a Wireless LAN technology specific procedure (out of scope for 3GPP).

2. The WLAN sends an EAP Request/Identity to the UE.

EAP packets are transported over the Wireless LAN interface encapsulated within a Wireless LAN technology specific protocol.

3. The UE starts EAP AKA authentication procedure by sending an EAP Response/Identity message. The UE sends its identity complying to Network Access Identifier (NAI) format specified in RFC 2486. NAI contains the temporary identifier allocated to UE in previous authentication if available and valid. Otherwise, the NAI shall contain the IMSI.

Note : generating an identity conforming to NAI format from IMSI is defined in EAP/AKA draft (draft-arkko-pppext-eap-aka-05.txt).

4. The 3GPP AAA Server is chosen based on the NAI.

Note : diameter/radius proxy chaining and/or diameter referral can be applied to find the AAA server.

5. The 3GPP AAA server receives the EAP Response/Identity packet that contains the subscriber identity.

6. 3GPP AAA Server checks that it has an authentication vector available (RAND, AUTN, XRES, IK, CK) for the subscriber from previous authentication. If not, a set of authentication quintuplets is retrieved from HSS/HLR. If a temporary identifier is provided, it is mapped to the corresponding IMSI.

7. 3GPP AAA server checks that it has the WLAN access profile of the subscriber available. If not, the profile is retrieved from HSS/HLR. 3GPP AAA Server verifies that the subscriber is authorized to use the WLAN service.

Although this step is presented after step 6 in this example, it could be performed at some other point, however before step 14. (This will be specified as part of the Wx interface.)

8. New keying material is derived from IK and CK. The extra keying material is required in order to pass the encrypted and integrity protected temporary identifier to the UE. The keying material may also be used for WLAN technology specific confidentiality or integrity protection.

A new temporary identifier is chosen and encrypted. Temporary identifier format is FFS.

9. 3GPP AAA Server sends RAND, AUTN, and encrypted temporary identifier to WLAN in EAP Request/AKA-Challenge message.

10. The WLAN sends the EAP Request/AKA-Challenge message to the UE

11. UE runs UMTS algorithm on the USIM. The USIM verifies that AUTN is correct and hereby authenticates the network. If AUTN is incorrect, the terminal rejects the authentication (not shown in this example). If the sequence number is out of synch, terminal initiates a synchronization procedure (not shown in this example). If AUTN is correct, the USIM computes RES, IK and CK.

UE derives required additional keying material from IK and CK. UE decrypts temporary identifier and saves it to be used on next authentication.

12. UE sends EAP Response/AKA-Challenge containing calculated RES to WLAN

13. WLAN sends the EAP Response/AKA-Challenge packet to 3GPP AAA Server

14. 3GPP AAA Server compares XRES and the received RES.

15. If the comparison in step 14 is successful, then 3GPP AAA Server sends the EAP Success message to WLAN. The 3GPP AAA Server includes the derived keying material in the message. WLAN stores the keying material to be used in communication with the authenticated UE.

16. WLAN informs the UE about the successful authentication with the EAP Success message. Now the EAP AKA exchange has been successfully completed, and the UE and the WLAN share session key material.

Note 1: The 3GPP AAA Server that is referred to in this diagram is the one that actually realises the authentication. If AAA Proxies are used between the WLAN Access Network and the AAA Server, they are not referred to in this diagram.

Note 2: Temporary identifier is only used for authentication purpose. User identification on the data path is done by the Access Point in a way that is proper to the WLAN.

### A.5.2 EAP SIM procedure

SIM based authentication shall be based on existing GSM AKA method but shall include enhancements for network authentication. In the case of WLAN-3GPP system interworking, this method should be supported by a generic authentication mechanism (independently of the underlying WLAN standard), e.g. EAP.

EAP SIM authentication mechanism is described in Internet Draft draft-haverinen-pppext-eapsim. The current version is 06 (draft-haverinen-pppext-eap-sim-06.txt).

The following procedure is based on EAP SIM authentication mechanism:

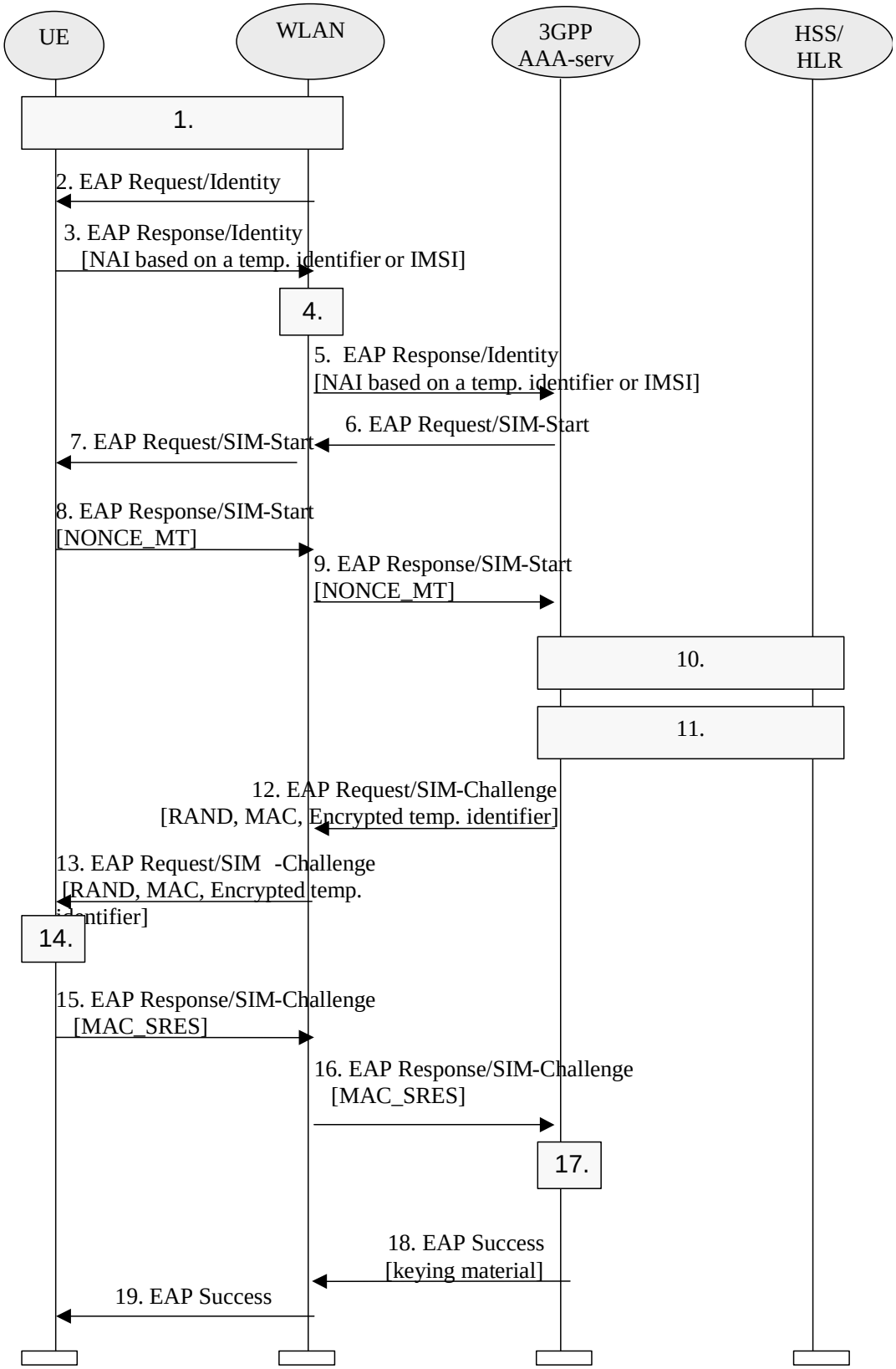



*Figure A.4.2 Authentication based on EAP SIM scheme*

1. After WLAN connection establishment, Extensible Authentication Protocol is started with a Wireless LAN technology specific procedure (out of scope for 3GPP).

2. The WLAN sends an EAP Request/Identity to the UE.

EAP packets are transported over the Wireless LAN interface encapsulated within a Wireless LAN technology specific protocol.

3. The UE starts EAP SIM authentication procedure by sending an EAP Response/Identity message. The UE sends its identity complying to Network Access Identifier (NAI) format specified in RFC 2486. NAI contains the temporary identifier allocated to UE in previous authentication if available and valid. Otherwise, the NAI shall contain the IMSI.

Note : generating an identity conforming to NAI format from IMSI is defined in EAP/SIM (draft-haverinen-pppext-eap-sim-06.txt).

4. The 3GPP AAA Server is chosen based on the NAI.

Note : diameter/radius proxy chaining and/or diameter referral can be applied to find the AAA server.

5. The 3GPP AAA server receives the EAP Response/Identity packet that contains the subscriber identity.

6. The 3GPP AAA Server guesses, based on the NAI, that the subscriber is a GSM user; hence it sends the EAP Request/SIM-Start packet to WLAN.

7. WLAN sends the EAP Request/SIM-Start packet to UE

8. The UE chooses a fresh random number NONCE_MT. The random number is used in network authentication.

The UE sends the EAP Response/SIM-Start packet, containing NONCE_MT, to WLAN

9. WLAN sends the EAP Response/SIM-Start packet to 3GPP AAA Server

10. 3GPP AAA Server checks that it has N (usually two or three) available authentication triplets (RAND, SRES, Kc) for the subscriber from previous authentication. Several triplets are required in order to generate longer session keys. If N triplets are not available, a set of authentication triplets is retrieved from HSS/HLR. If a temporary identifier is provided, it is mapped to the corresponding IMSI.

Although this step is presented after step 9 in this examples, it could be performed at some other point, for example after step 5, however before step 12. (This will be specified as part of the Wx interface.)

11. 3GPP AAA server checks that it has the WLAN access profile of the subscriber available. If not, the profile is retrieved from HSS/HLR. 3GPP AAA Server verifies that the subscriber is authorized to use the WLAN service.

Although this step is presented after step 10 in this example, it could performed at some other point, however before step 18. (This will be the specified as part of the Wx interface.)

12. New keying material is derived from NONCE_MT and N Kc keys. The extra keying material is required in order to calculate a network authentication value and to pass the encrypted and integrity protected temporary identifier to the UE. The keying material may also be used for WLAN technology specific confidentiality or integrity protection.

A message authentication code (MAC) is calculated over the RAND challenges using a newly derived key. This MAC is used as a network authentication value.

A new temporary identifier is chosen and encrypted.

3GPP AAA Server sends RAND, MAC, and encrypted temporary identifier to WLAN in EAP Request/SIM-Challenge message.

13. The WLAN sends the EAP Request/SIM-Challenge message to the UE

14. UE runs the GSM A3/A8 algorithms N times, once for each received RAND.

This computing gives N SRES and Kc values.

The UE derives additional keying material from N Kc keys and NONCE_MT.

The UE calculates its copy of the network authentication MAC and checks that it is equal with the received MAC. If the MAC is incorrect, the network authentication has failed and the UE cancels the authentication (not shown in this example). The UE continues the authentication exchange only if the MAC is correct.

UE decrypts temporary identifier and saves it to be used on next authentication.

UE calculates a combined response value MAC_SRES from the N SRES responses.

15. UE sends EAP Response/SIM-Challenge containing calculated MAC_SRES to WLAN

16. WLAN sends the EAP Response/SIM-Challenge packet to 3GPP AAA Server

17. 3GPP AAA Server compares its copy of the MAC_SRES with the received MAC_SRES.

18. If the comparison in step 17 is successful, then 3GPP AAA Server sends the EAP Success message to WLAN. The 3GPP AAA Server includes the derived keying material in the message. WLAN stores the keying material to be used in communication with the authenticated UE.

19. WLAN informs the UE about the successful authentication with the EAP Success message. Now the EAP SIM exchange has been successfully completed, and the UE and the WLAN share session key material.

Note 1: The 3GPP AAA Server that is referred to in this diagram is the one that actually realises the authentication. If AAA Proxies are used between the WLAN Access Network and the AAA Server, they are not referred to in this diagram.

Note 2: Temporary identifier is only used for authentication purpose. User identification on the data path is done by the Access Point in a way that is proper to the WLAN

Note 3 : the derivation of the value of N is for further study

### A.5.3 Alternative EAP initialisation.

The following figure shows an example where the realm identifying the 3GPP AAA server is retrieved by a method linked with the WLAN technology. Once the Diameter connection is initialized, the 3GPP AAA server can start the EAP identity request phase if necessary.

Editor’s Note : the application of this procedure to IEEE 802.11 needs to be studied further.

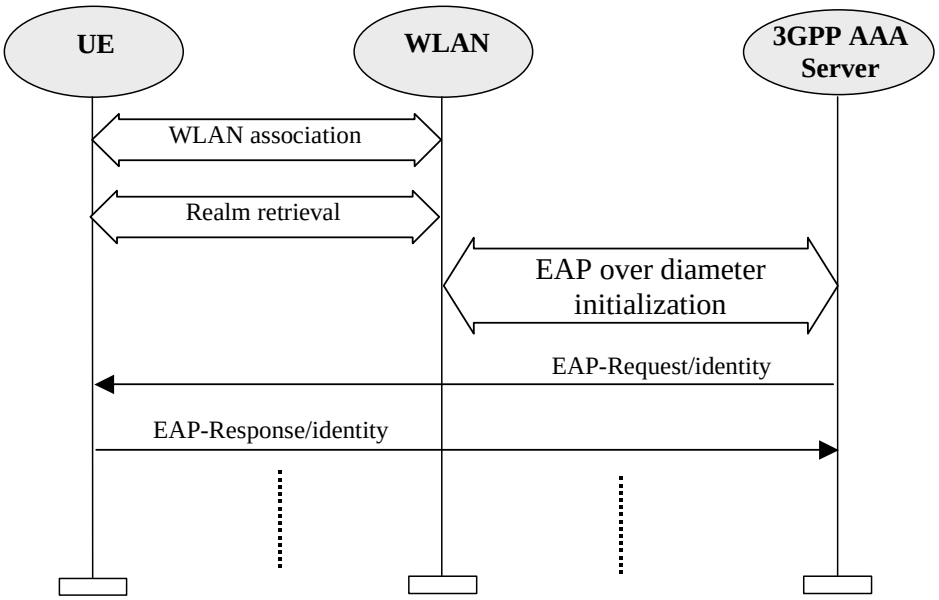



*Figure A.4.3 End-to-end EAP initialisation session*

## A.5.4 Re-authentication message sequence chart

The message sequence chart below illustrates the operation on re-authentication.

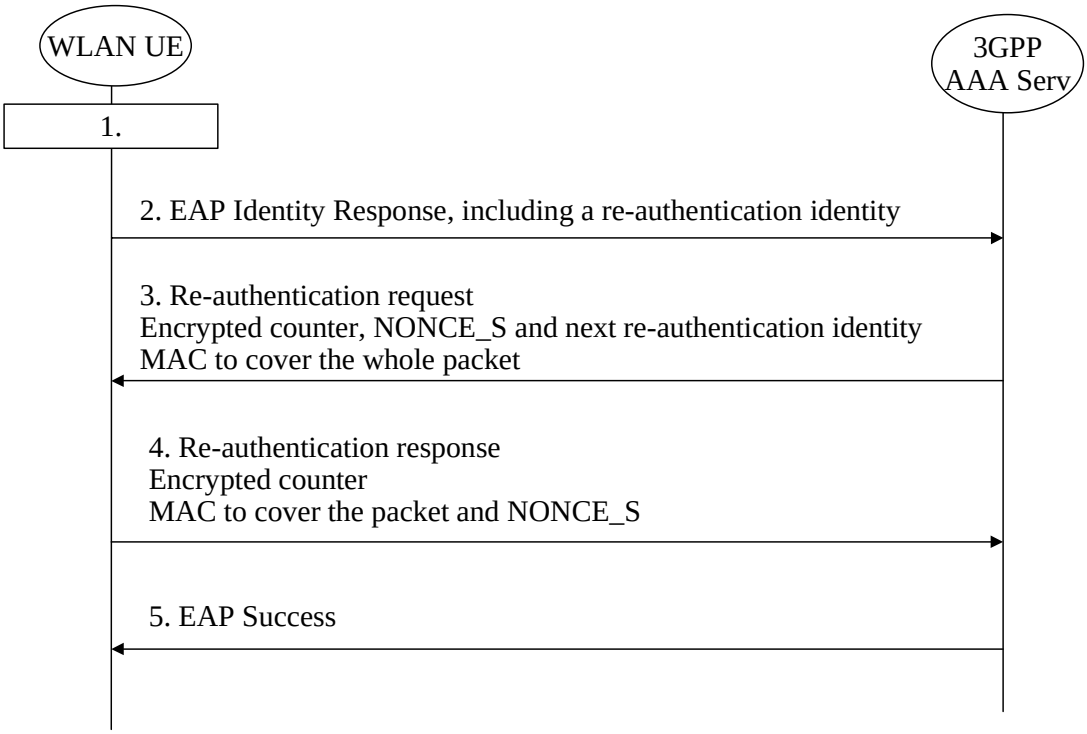



*Figure A.4.4 Re-authentication signalling sequence*

1. Either the UE or the WLAN initiates the authentication procedure with wireless LAN technology specific means. The WLAN UE is requested to send its identity

2. WLAN UE wishes to use the re-authentication procedure and therefore uses a re-authentication identity

3. 3GPP AAA server recognizes the re-authentication identity and agrees on using re-authentication. The 3GPP AAA server sends a re-authentication request (of the EAP type EAP/SIM or EAP/AKA) to the UE. The request contains an encrypted counter, an encrypted server challenge (NONCE_S) and a Message Authentication Code to cover the whole packet. The packet may also include an encrypted next re-authentication identity for next re-authentication

4. WLAN UE verifies the Message Authentication Code and checks that the counter value is fresh. If successful, the WLAN UE responds with a re-authentication response packet that includes the counter value encrypted and a Message Authentication Code that covers the EAP packet and the server challenge NONCE_S

5. 3GPP AAA server verifies the Message Authentication Code and the counter. If successful, the 3GPP AAA server sends EAP Success to the WLAN UE.

WLAN UE and 3GPP AAA Server derive new session keys. 3GPP AAA Server sends the session keys to WLAN.

# Annex B (informative): WLAN Radio Technologies

| Attribute | 802.11b | Bluetooth | 802.11a | HiperLan/2 | 802.11g |
|---|---|---|---|---|---|
| Frequency | 2.4 GHz | 2.4 GHz | 5 GHz | 5 GHz | 2.4 GHz |
| Physical Layer | Direct Sequence Spread Spectrum (DSSS) | Frequency Hopping Spread Spectrum (FHSS) | Orthogonal Frequency Division Multiplexing (OFDM) | OFDM | Orthogonal Frequency Division Multiplexing/Complementary Code Keying OFDM/CCK |
| Channel Width | 22 MHz | 1MHz | 22 MHz | 22 MHz | 22 MHz |
| Range | 150 ft (indoors) 300 ft (outdoors) | 30 ft (with 1mW) | 100 ft (indoors) 200 ft(outdoors) | Expected to be same as 802.11a | 150 ft (indoors) (speed varies as distance from Access Point) |
| Data Throughputs | 1,2,6,11 Mbps | 720 Kbps | 6,9,12,18,36,54 Mbps (speed varies as distance from Access Point) | Same as 802.11a | Up to 54 Mbps |
| MAC | CSMA/CA in Distributed Coordinated Function Mode (DCF) (optional) Polling Based in Point Coordination Function (PCF) | Time Division Duplex (TDD) with a Master/Slave Polling Mechanism | Same as 802.11b | TDMA with TDD | Same as 802.11b |
| Miscellaneous | High Speed Data Applications Susceptible to interference from Bluetooth and other devices | Wire Replacement; Inexpensive Low component count Low Power | Improve Spectral Efficiency over 802.11b | Products not available yet | Backwards compatible with 802.11b |

*Table B.1 WLAN Technology Comparison*

# Annex C (informative): Hierarchical Roaming Principles

3GPP-WLAN Interworking allows an indirect relationship between the WLAN AN and the HPLMN, with an intermediate VPLMN at least being able to act as an AAA proxy.

3GPP-WLAN roaming is an unrestricted environment which does not preclude the operator of a WLAN Access Network to have agreements with multiple 3GPP network operators who can act as intermediaries, or roaming brokers. In such a scenario, the WLAN AN must decide how to route AAA messages. The decision where to route messages may have implications on the Inter operator tarifing. Figure 1 shows a scenario where a WLAN Access Network has direct relationships with 3 different 3GPP networks offering 3GPP AAA Proxy service, Visited Network A, B and C. A WLAN UE from a home network wishes to use the WLAN service offered by the WLAN Access Network. Visited Network C does not have a roaming agreement with the home network.

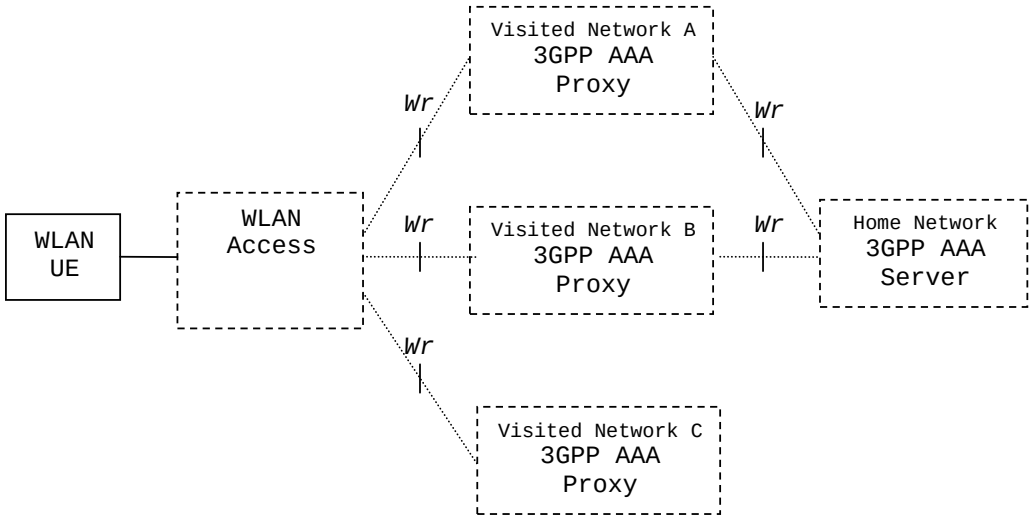



**Figure 1: AAA Routing with Hierarchical Roaming**

In the above scenario, the WLAN Access Network must decide where to route the AAA request. The WLAN AN may use static prefix or suffix tables to "route" the request, based on the realm part of NAI and optionally network ID (e.g. SSID, NOP_ID) (e.g., if multiple network IDs are supported), towards the appropriate home network.

Alternatively, if the WLAN AN has several possible other nodes which it can send the request, but no prior configuration enables it to pick one, then the WLAN can use "dynamic routing" of the AAA request, according to techniques agreed between WLAN AN, home operators and intermediate visited networks, e.g., using DNS based techniques [9].

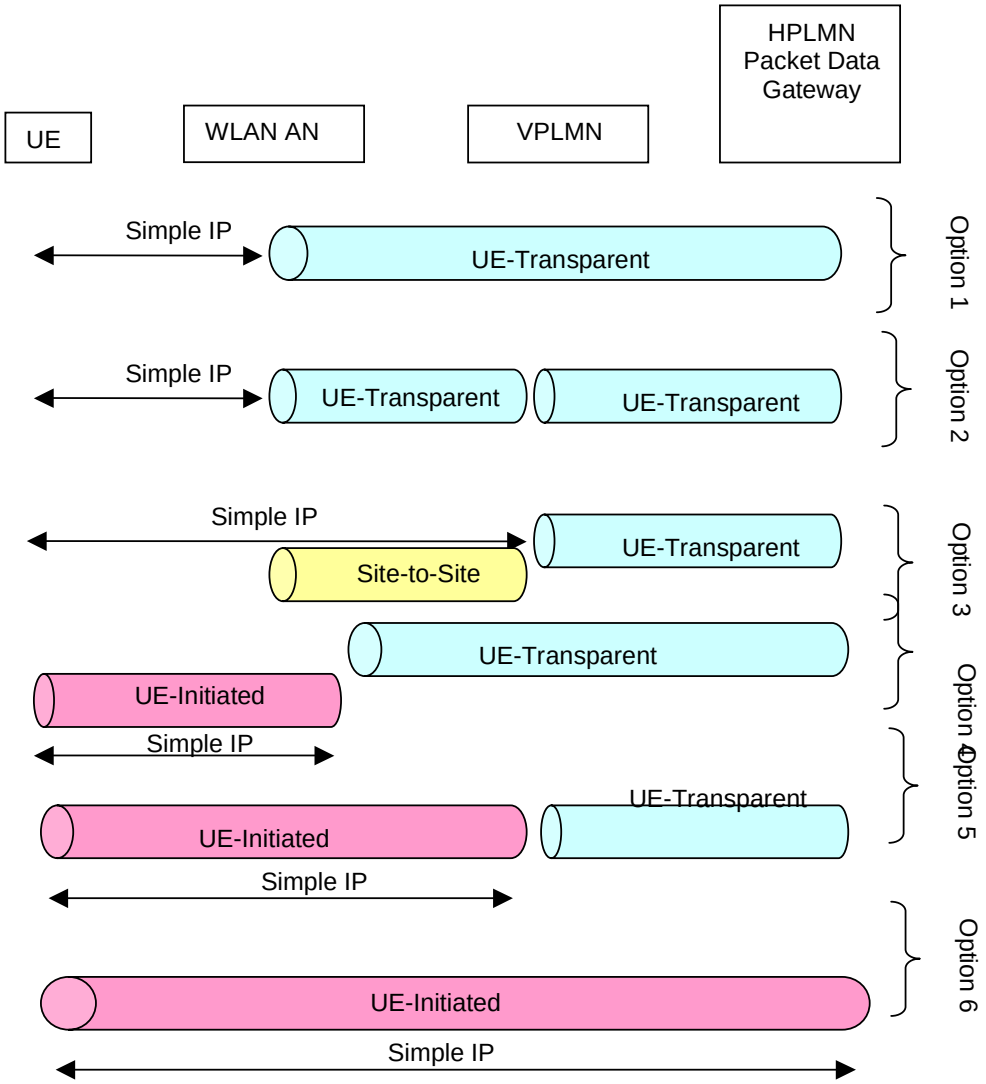
The ability of a WLAN UE to influence the routing of AAA requests, e.g., by using a specific realm part of the NAI, is FFS.

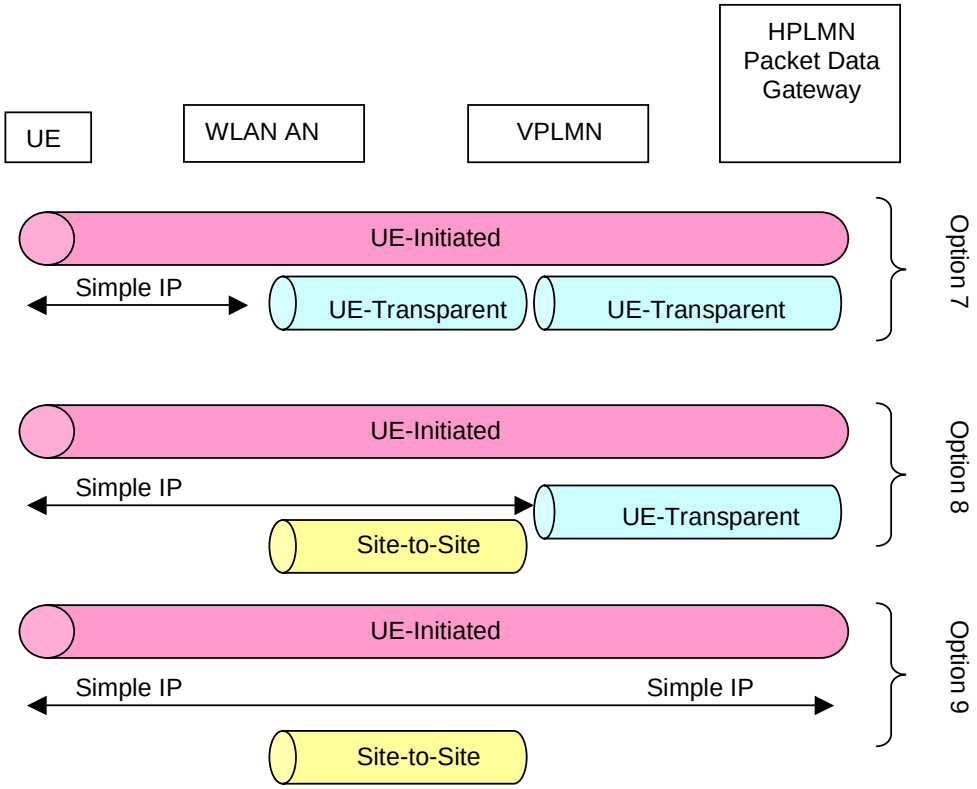
# Annex D (informative): WLAN Tunnelling Options

## Introduction

There are various different scenario options for UE-transparent and UE-initiated tunnelling. This contribution describes the different options and compares them with high level requirements and proposes to reduce the options to be considered further.

## Options


HPLMN
Packet Data
Gateway
UE
WLAN AN
VPLMN
Simple IP
UE-Transparent
Option 1
Simple IP
UE-Transparent
UE-Transparent
Option 2
Simple IP
UE-Transparent
Site-to-Site
UE-Transparent
UE-Initiated
Simple IP
Option 3
Option 4
Option 5
UE-Transparent
UE-Initiated
Simple IP
Option 6
UE-Initiated
Simple IP




Note:

Site-to-site tunnel aggregated flows

UE-transparent tunnels per user – a single tunnel per user

UE-initiated supports multiple tunnels per user

---

## Review of Each Option for VPLMN Support

Option 1: Does not meet requirement to have tunnel between “trusted partners” – not considered further

Option 2: Tunnel switch in VPLMN. Per user tunnelling requirements in WLAN AN. Meets VPLMN requirements.

Option 3: Tunnel endpoint in the VPLMN. Site-to-site tunnelling and DHCP relay in WLAN AN. Meets VPLMN requirements.

Option 4: Does not meet requirement to have tunnel between “trusted partners” – not considered further

Option 5: Tunnel switch in VPLMN. Meets VPLMN requirements.

Option 6: Does not meet requirement for monitoring by VPLMN

Option 7: Meets VPLMN requirements

Option 8: Meets VPLMN requirements

Option 9: Meets VPLMN Requirements

## Review of Remaining Options for WLAN AN impact

Option 2: Per user tunnel endpoint required

Option 3: Site-to-Site tunnel required

Option 5: No additional requirements on WLAN AN

Option 7: Per user tunnel endpoint required

Option 8: Site-to-Site tunnel required

Option 9: Site-to-Site tunnel required

## Review of Remaining Options for UE impact

Option 2: No impact

Option 3: No impact

Option 5: UE tunnelling client required

Option 7: UE tunnelling client required

Option 8: UE tunnelling client required

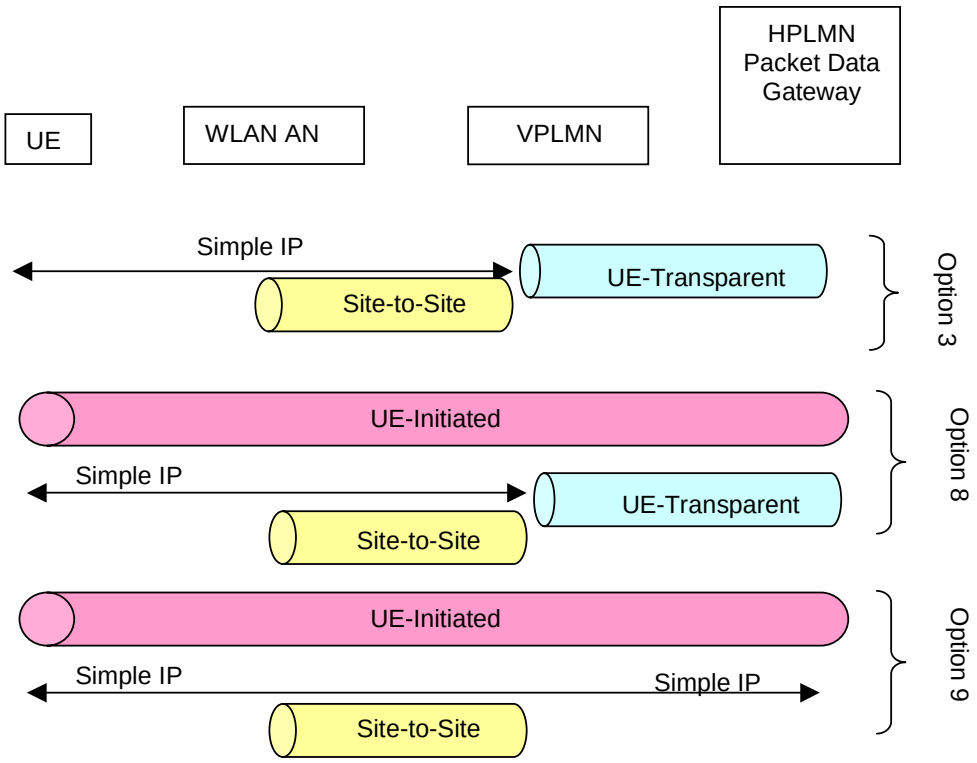
Option 9: UE tunnelling client required

**Option 7 deleted due to high impacts in WLAN AN and UE compared to option 8**

**Option 2 deleted due to high impacts in WLAN AN compared to option 3**

**Option 5 has a dependency on UE-initiated and UE-transparent – stage 3 work will be more complex, e.g., UE initiated tunnel failure scenarios, UE does not have a relationship with VPLMN, will require transitive trust mechanisms to be defined in stage 3 – Option 5 deleted.**

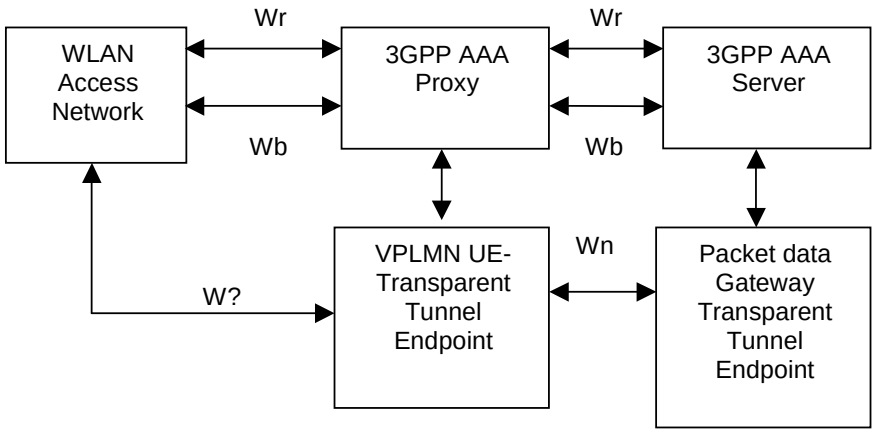
## Tunnel Types to be discussed further:




Note: Option 9 degrades from Scenario 3 to Scenario 2 when UE client not present

## Binding users to tunnel endpoints in the VPLMN

The above options include the use of a per-user tunnel endpoint in the VPLMN without such a network entity terminating pre-user tunnels on the interface to the WLAN. In order to achieve this functionality, the VPLMN needs to be able to identify the users IP address, create state for such users and to initiate a network based tunnel for such users. Such functionality places requirements on the various different reference points.




---

Only a single VPLMN is shown above. Multiple VPLMNs can be supported by using separate VLANs in the WLAN AN.

The minimum requirement on the W? interface is that it is a point-to-point link between the WLAN AN and the VPLMN., This point to point link may be for examples an ATM PVC, a PPP serial link, a layer 3 VPN.

The VPLMN UE-Transparent Tunnel Endpoint (VUTTE) needs to establish flows on behalf of the user. A users flow is identified in the VUTTE is identified by the users IP address. The VPLMN needs to correlate IP flows with AAA signalling proxied over the Wr interface.

Using RADIUS as an example, the HPLMN 3GPP AAA server can include RADIUS compulsory tunnelling attributes in the access accept. These tunnelling attributes are only of interest to the VPLMN and will be removed from the RADIUS message in the 3GPP AAA proxy. Hence the RADIUS access accept sent to the WLAN AN will not include any tunnelling attributes.

The VPLMN now can initiate a tunnel on the users behalf but cannot bind this tunnel to a users IP flow. This is because IP address allocation may be performed using DHCP and hence the Framed-IP-Address attribute cannot be used to indicate a WLAN-UE IP address in either the Access Request or Access Accept messages.

In this instance, the VPLMN must wait for the first RADIUS message containing a users IP address. Such a RADIUS message will contain the users MAC address and IP address.

The RADIUS Access Accept contains the per user tunnel establishment for a particular MAC address. The reception of a RADIUS accounting message with an allocated IP address will also contain the users MAC address, e.g., received over Wb. This allows functionality in the VPLMN to build a tunnel for the user and to perform per subscriber accounting generation on this tunnel endpoint.

## Requirements on the WLAN Access Network

All three scenarios require the VPLMN to be able to build per user state. In Option 3 and Option 8 the state is linked to an AAA signalled compulsory tunnel.

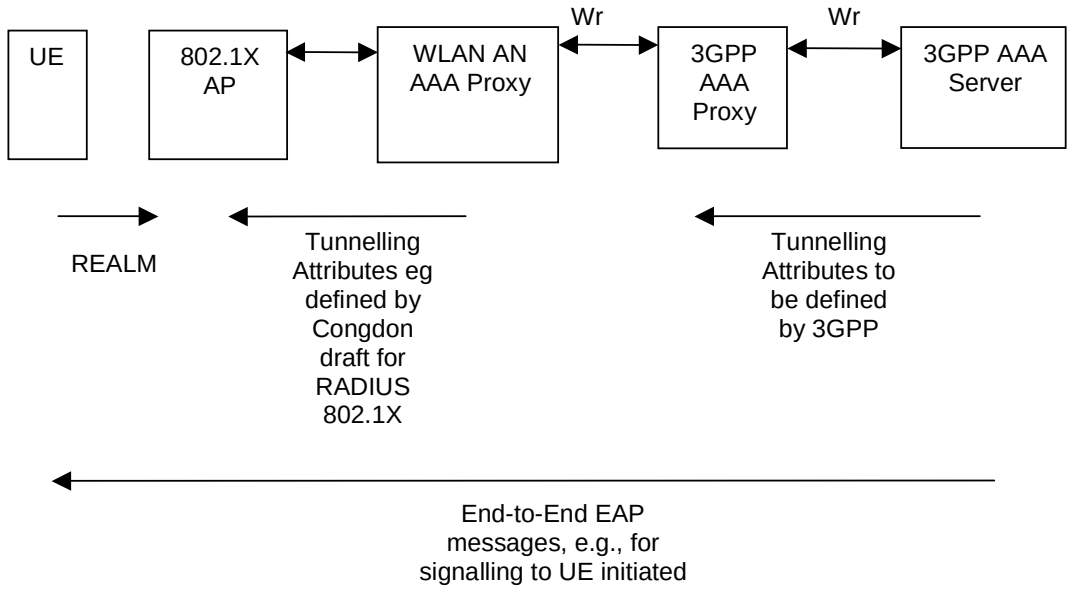
In Option 9, no compulsory tunnel is built but the VPLMN is still able to build per user state.

The above description indicates that the WLAN AN is required to support a site-to-site link with the VPLMN, e.g., to ensure packets are policy routed to the VPLMN.

Regarding the triggering of a RADIUS accounting packet containing the users IP address, this may be originated in the WLAN AN, e.g., by the WLAN Access point or by the WLAN AN DHCP server, or may be originated in the VPLMN, e.g., from a DHCP server in the VPLMN if DHCP relay is supported in the WLAN AN.

## Requirements on AAA/EAP Signalling

The AAA signalling is used to transport tunnelling information and EAP messages. The Requirements seems to fit the overall AAA and EAP architectures.



## Summary

Various options for tunnelling support have been analysed. Rough analysis has managed to eliminate three candidates. :

Option 1, 4, 6.

# Annex D (informative): Function Prioritisation

| Topic | Scenario | Overall priority (to March 2003) | SA2 WLAN group priority (to March 2003) | Comment |
|---|---|---|---|---|
| Access control architecture | 2 | High | High | |
| Interworking architecture | 2 | High | High | Consideration of roaming and interworking scenarios |
| Addressing | 2 | High | High | IP address allocation – basic capabilities need to be defined |
| Security protocols | 2 | High | Low | Detailed work on authentication and authorisation should now be undertaken by SA3 |
| Charging | 2 | High | Low | Charging related architecture should be transferred to SA5 once this spec is stable enough until 1Q 2003 |
| Network selection | 2 | Medium / Low | Medium / Low | Does this need to be standardised for R6? Liaison to SA1 |
| SMS | 3 | Medium | Medium | No contributions have yet been made on this. May need architecture changes in other areas outside the scope of WLAN group (liaison needed) |
| MMS | 3 | Medium | Medium | No contributions have yet been made on this. May need architecture changes in other areas outside the scope of WLAN group (liaison needed T2 & SA1) |
| IMS access | 3 | High | High | IMS compatibility with R5 IMS is important to operators |
| MBMS interworking | 3 | Low | Low | Propose for R7 as MBMS not yet stable |
| Presence | 3 | Low | Low | Propose for R7 - IMS access should provide support for presence services |
| Location services | 3 | **Low** | Low | Propose for R7 - Integration of WLAN and location services needs further consideration |
| Instant messaging | 3 | Low | Low | Propose for R7 - IMS access should provide support for messaging services |

| | | | | |
|---|---|---|---|---|
| Policy control information | 3 / 4 | High | Low | For R6 work on IMS access independence & policy control is ongoing in other groups within SA2 |
| Mobility | 4 / 5 | Low | Low | This is of high importance but is already agreed to be outside the scope of R6, it is therefore considered to be part of R7 |
| Editorial aspects | All | Low | Low | At this stage, priority should be given to technical rather than editorial aspects |

*Table C.1 Function Prioritisation*

# Annex E (informative): Change history

| Change history | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **Old** | **New** |
| *2002-08* | | | | | *Converted TR23.934v0.5.0 into this TS* | *0.0.0* | *0.1.0* |
| 2002-09 | | | | | Raised to v.1.0.0 for presentation at SA#17 (same content as v.0.1.0) | 0.1.0 | 1.0.0 |
| | | | | | | | |
| | | | | | | | |