3GPP TSG SA WG3 Security — S3#29 S3-030427
15 - 18 July 2003
San Francisco, USA

3GPP TSG SA2 WLAN Ad-hoc S2-032729~~44220~~
Sophia Antipolis, France, 7th – 11th July 2003

Title: **LS on ~~PDG IP~~ address discovery using public DNS for WLAN interworking**

Release: Rel-6
Work Item: WLAN Interworking

Source: **SA2**

To: **SA3**

Contact Person:
Name : **Xin Chen**
E-mail Address: **x.chen@fle.fujitsu.com**
Tel Number: **+44(0)2086064453**

Attachment: **3GPP TS 23.234 v1.12.0**

1 Over All Description

~~'PDG Address Discovery' is the process by which the UE obtains the IP address of the PDG. It is required for the **end-to-end tunnelling**.~~

~~In more detail about the DNS proposal:~~

~~After UE is authenticated by WLAN and gets a local IP address and DNS server address from WLAN. The UE then will use a FQDN (stored in terminal or generated itself) to query the DNS server in the WLAN to get the IP address of the PDG.~~
SA2 is currently considering mechanisms for 3GPP UEs connected to WLANs to establish a tunnel towards a 3GPP network for the purposes of accessing packet based services which are currently available over GPRS.

In order to achieve this, the WLAN UE must obtain the IP address of the first point of contact (WAG or PDG) in the 3GPP network.

It has been proposed that this should be done independently from the initial WLAN Access authentication and authorization procedure (which uses EAP).

One proposal for this is that the address of this first point of contact would be available within the Public DNS based on the UE having sufficient information (e.g. MNC and MCC of the Visited PLMN) to construct an appropriate FQDN. Then the UE can use the FQDN to get the IP address of the first contact point from DNS server in the WLAN.

~~The implications of this proposal are~~Some concerns have been expressed about the security implications of this approach, specifically that ~~:~~

~~The~~ the WLAN may be provided by a third party, so the DNS server could be part of the Internet and shared by 3GPP and non-3GPP users. Therefore the DNS server is open for attacks from the Internet.

These concerns are from the comparing with the GPRS system in which the DNS Server is a private DNS Server and the GGSN address is resolved by SGSN not by the UE and the IP addresses of the GGSN and SGSN can not be derived by the UE.~~e.g.a ., e.g. a faked DNS server address could be given to the UE.~~

~~- The operators will have to give their PDG's IP addresses to the public DNS domain. Therefore un-authenticated WLAN user will be able to send packets to PDGs.~~

Others have noted that use of a third party WLAN will require Service Level Agreements between the 3GPP operator and WLAN provider, and these could include requirements with respect to the security and availability of the DNS servers.

2 Action

SA2 kindly asks SA3 to ~~comment whether this proposal is satisfactory according to 3GPP security requirements.~~answer the following questions:

Is allowing IP address of the WAG to be discovered by UE using public DNS satisfactory according to 3GPP security requirements applicable to 3GPP WLAN interworking?

Is allowing IP address of the PDG to be discovered by UE using public DNS satisfactory according to 3GPP security requirements applicable to 3GPP WLAN interworking?

3 Next meetings :

SA2 #34	18 - 22 Aug 2003	Brussels
SA2 #35	27 - 31 Oct 2003	Asia

Draft 3GPP TS 23.234 V1.1~~1~~2.0 (2003-07)

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

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 22.101: "Service principles".

[3] 3GPP TR 22.934: "Feasibility study on 3GPP system to WLAN interworking".

[4] 3GPP TS 23.002: "Network architecture".

[5] 3GPP TS 23.060: "GPRS; Service description".

[6] 3GPP TR 23.934: "3GPP system to WLAN Interworking; Functional and architectural definition"

[7] 3GPP TS 29.002: "Mobile Application Part (MAP) specification "

[8] 3GPP TS 29.329: " Sh Interface based on the Diameter protocol; Protocol details."

[9] 3GPP TS 31.102: "Characteristics of the USIM Application."

[10] 3GPP TS 32.225: " Telecommunication management;Charging management;Charging data description for the IP Multimedia Subsystem (IMS)."

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

[11] RFC2284: "PPP Extensible Authentication Protocol (EAP)"

[12] RFC 2486: "The Network Access Identifier"

[13] 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)

[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

W-APN: WLAN Access Point Name – identifies an IP network and a point of interconnection to that network (Packet Data Gateway)

Requested W-APN: The W-APN requested by the user

Selected W-APN: The W-APN selected by the network as a result of the user request

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.

PS based services: Services that are usually provided by the 3GPP PS Core Network.

Service Authorization: Authorization for a user to access the requested service according to the user's subscription.

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:

D'	Interface between a pre-R6 HSS/HLR and a 3GPP AAA Server
Gr'	Interface between a pre-R6 HSS/HLR and a 3GPP AAA Server
Wb	Interface between a WLAN Access Network and a 3GPP AAA Server/Proxy
Wf	Interface between a CGw/CCF and a 3GPP AAA Server/Proxy
Wi	Interface between a Packet Data Gateway and an external IP Network
Wm	Interface between a Packet Data Gateway and a 3GPP AAA Server
Wn	Interface between a WLAN Access Network and a ~~Packet Data~~WLAN Access Gateway
Wp	Interface between a WLAN Access Gateway and a Packet Data Gateway
Wo	Interface between a 3GPP AAA Server and an OCS
Wr	Interface between a WLAN Access Network and a 3GPP AAA Server/Proxy
Wx	Interface between an HSS and a 3GPP AAA Server

3.3 Abbreviations

APN	Access Point Name
CCF	Charging Collection Function
CGw	Charging Gateway
OCS	Online Charging System

PDA	Personal Digital Assistant
PDG	Packet Data Gateway
WAG	WLAN Access Gateway
W-APN	WLAN APN
WLAN	Wireless Local Area Network

4 WLAN Radio networks interworking with 3GPP

Editor's notes : Provides a high-level description of the WLAN interworking model.

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 server. The home network is required to support RADIUS interworking in the non-roaming case when WLAN Access Networks not providing Diameter interfaces are to be supported.

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.

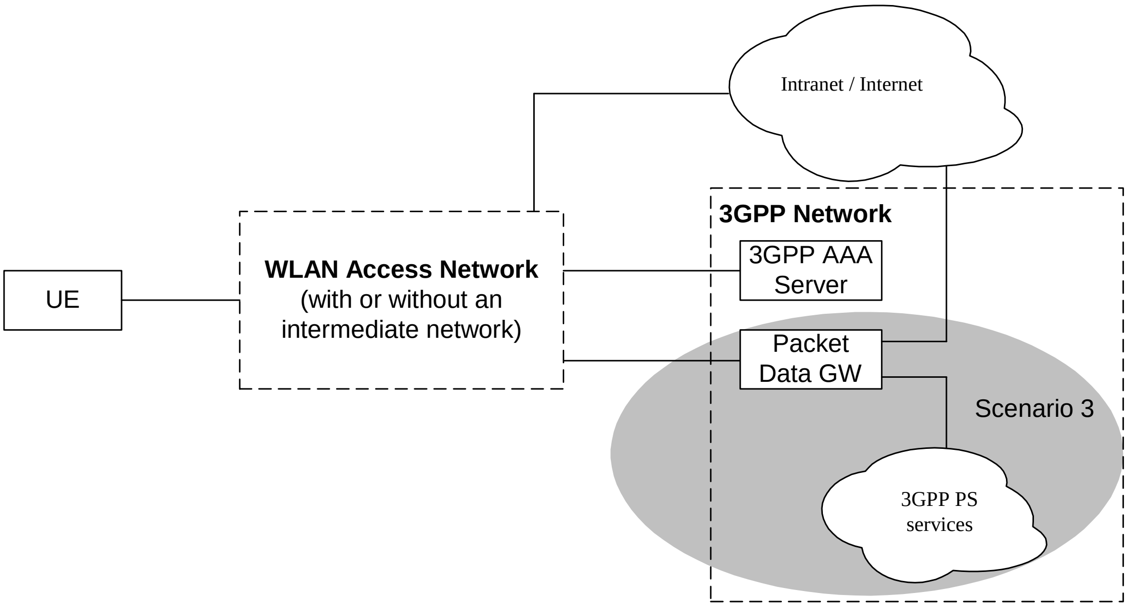


Figure 4.1: Simplified WLAN Network Model. The shaded area refers to scenario 3 functionality

- 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.

5 High-level Requirements and Principles

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

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 software 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 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 network 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
- WLAN Access 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 WLAN Access A~~a~~uthorization requests shall be indicated to the WLAN, so that the WLAN can take appropriate action.
- The WLAN Access A~~a~~uthorization mechanism shall be able to inform the user and WLAN immediately of any change in service provision.
- This TS proposes solutions for operators who want to interwork their WLAN with an existing pre-R6 HLR/HSS.

Additional access control requirements for scenario 3:

- Service Authorization shall occur after the WLAN Access Authentication/Authorization procedure.
- 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, MBMS and services built upon combinations of these. Among these services, prioriti~~s~~zation is given for information in Annex C.
- Access to PS based services normally provided by the 3GPP ~~packet core~~PS Core Network shall be provided via WLAN. These PS based services shall include support of private addressing schemes, external address allocation, secure tunnel~~l~~ing to private external network, ability to provide addresses of DNS and NetBios servers specific to a private external network. End to end Quality of Service shall be supported when accessing these services via WLAN.

  Note: some limitations may exist because of the WLAN AN.

- A scenario 3 WLAN inter-working system shall be able to support WLAN UEs operating in scenario 2, e.g.~~,~~ according to subscription.

- A scenario 2 WLAN inter-working system shall be able to indicate in the reject cause for access from a scenario 3 WLAN UE that only scenario 2 is supported.

- A scenario 3 WLAN inter-working system shall be able to mandate all flows to be routed to the HPLMN, e.g.~~,~~ according to subscription. This routing enforcement shall not rely on the WLAN UE client.

  Note: T~~t~~his may mandate additional functionality existing in the WLAN AN

5.2 Access Control Principles

End to End Authentication : WLAN Authentication signa~~l~~ling is executed between WLAN UE and 3GPP AAA Server for the purpose of authenticating the end-user and ~~enabling~~ authorizing 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]

WLAN Access Authoris~~z~~ation: This defines the process(es) in 3GPP AAA Server verifying whether ~~the~~ WLAN Access should be allowed to a subscriber and deciding what access ~~scope~~ rules/policy~~of WLAN Access~~ should be applied~~allowed~~ to a subscriber. It is the access stage after the access authentication, ~~and~~ but before service authori~~z~~sation ~~(also before the~~and transport IP address allocation~~)~~.

After the authentication process succeeds, t~~T~~here could be additional conditions for the 3GPP AAA Server to decide whether the access is allowed and what access rules/policy should be applied~~what access scope is allowed, after the authentication process success~~. These conditions may be based on the subscriber's profile, the account status, O&M rules or local agreements.

The p~~P~~rocedure for WLAN Access Authorization between the UE and the 3GPP AAA Server is combined with the WLAN Access Authentication.

~~WLAN Access scope should be specified by the operator.~~

Access ~~scope/~~rules/policy decided by the 3GPP AAA Server may be deployed in the 3GPP AAA Server, or/and ~~sent to other~~in other entities such as the WAG or the WLAN AN.

Access rules/policy may include access scope limitation, time limitation, bandwidth control values, and/or user priority.

WLAN Access rules/policy should be specified by the home and/or visited operator based on the subscriber's profile, the account status, O&M rules (e.g. blacklist, access limitation list), and local agreements. Factors such as access time and access location could also be considered in these rules.

The access scope limitation could be, for example, only/not/may “access through WAG”; only/not/may “access intranet X”.

Access scope limitation can be achieved using IP allocation scheme, VLAN allocation, Filtering, ACLs in the routers and switchers, etc.

Different access priority or the range of priorities may be authorized for different subscribers, and/or for one subscriber based on different access time or location, etc.

3GPP WLAN attach: The WLAN-attach status indicates whether the WLAN UE is now being served by the 3GPP WLAN IW network.

A UE is “WLAN-attached” after successful authentication and WLAN Access A~~a~~uthorization.

A UE is “WLAN-detached” in 3GPP network after its disconnection, or its authentication ~~and~~ or WLAN Access A~~a~~uthorization being cancelled.

The WLAN-attach status is maintained by the 3GPP AAA server.

The UE’s WLAN attach status should be obtained from the AAA Server directly or through the HSS, by other entities in the 3GPP or 3GPP connected network. Other entities in the 3GPP network obtain the UE’s WLAN-attach status directly from the AAA Server or through the HSS.

The description of the corresponding status in the UE is out of the scope of this TS.

Additional access control principle for scenario 3:

Service Selection and authorisation:

The solution shall include means for securely delivering service selection information from the UE to the 3GPP AAA server in the Home Network. The service selection information shall contain an indication of the requested W-APN to which access is requested. The 3GPP AAA Server in the Home network shall verify the users subscription to the indicated W-APN against the WLAN subscriber profile retrieved from HSS. The 3GPP AAA Server may modify the Requested W-APN based on the users subscription/local policy.

The service request shall be indicated by a tunnel establishment request from the UE to the WAG or PDG (whether the request is sent to the WAG or to the PDG is ffs). The WAG or PDG shall then seek authentication/authorisation from the 3GPP AAA Proxy or Server in the same network.

The results of the authorisation decision shall be communicated to the Visited Network. All subscription-based authorisation decisions are made in the Home network.

In the case of a request for access to services provided in the Visited Network, the 3GPP AAA Proxy shall also authorise access based on local policy.

5.3 Authentication methods

Authentication methods are discussed in TS 33.234 [6].

5.4 User Identity

5.4.1 General

The network authentication procedure is 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 [12]. A NAI is composed of a username part and a realm part. For more information, the NAI username part format is specified in IETF EAP-SIM and EAP-AKA specifications.

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 in the 3GPP AAA Server.

For re-authentication, UE shall use the previously allocated Reauthentication ID as specified in the IETF EAP-SIM and EAP-AKA specifications 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 [9]) 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 Service Authorization Principles for scenario 3

The home network decides whether visited service is allowed or not based on e.g. W-APN, the user subscription information, visited network capabilities and roaming agreement.

5.5.1 Accessing Home Network provided services

- It shall be possible to support multiple service authorizations after a successful authentication (i.e. EAP success)...
- Service authorization information shall be protected
- The Access Point Name (APN) concept defined in 3GPP TS 23.003 shall be used for WLAN interworking authorization (namely W-APN). In a service authorization procedure:
  - W-APN selection and authorization is an end-to-end procedure between the UE and the HPLMN (the service authorization decision is made by the 3GPP AAA Server).

    Editor's note: the use of subscription information is FFS.
  - WLAN UE shall use W-APN to indicate to the network the service or set of services it wants to access.
  - The PDG selection is under control of the 3GPP Home Network. The selection is based on the requested W-APN and user subscription information. The mechanism to select the PDG by the home network is for further study.
  - The PDG needs to know the authorized W-APN to select the Wi interface.

[Editor's note: The definition of W-APN is for further study]

5.5.2 Accessing Visited Network provided services

When accessing visited network provided services, additional principles below apply:

- If the home network determines that the services are to be provided by the Visited Network in the roaming case, the 3GPP AAA Server needs to pass to the 3GPP AAA Proxy the authorized W-APN and service related information which is required by the Visited Network to perform the service.
- The W-APN needs to be understood by both the Home and the Visited Networks.
- The V-PDG selection is under control of the 3GPP Visited Network. The selection is based on the authorized W-APN and service related information. The mechanism to select the V-PDG by the Visited Network is for further study.
- The selected PDG in the Visited Network needs to know the authorized W-APN to select the Wi interface.

5.6 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 a requested WLAN Access Point Name (W-APN). The Requested W-APN may also indicated a point of connection to the IP network (i.e. WAG or PDG).

A W-APN is indicated by the UE in the tunnel establishment procedure between the UE and an initial WAG or PDG (whether the request is sent to the WAG or to the PDG is FFS). It is then forwarded to the 3GPP AAA server (whether this request is routed via the 3GPP AAA Proxy is FFS).

Since scenario 3 mandates that some additional functionality exists in the VPLMN, in scenario 3 the VPLMN shall be able to communicate with the HPLMN across the Ws reference point whether it can support the various tunnelling options.

The home network decides the type of IP connectivity based on e.g. the requested W-APN, user's subscription information and VPLMN information and may determine an alternative W-APN, the Selected W-APN indicating the same network, but a different point of interconnection. The home network choices are:

1. No tunnelling, for supporting a scenario 2 WLAN UE
2. UE-transparent tunnelling
3. UE-initiated tunnelling

The 3GPP Home Network may also determine that the user should be given access to the same IP Network but via a different point of interconnection.

Editor's note: compatibility between scenario 2 and scenario 3 functional elements requires further study.

These cases are described below.

5.6.1. IP Connectivity without Tunnelling

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

5.6.2 UE-Transparent Tunnelling

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

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

1. EAP authentication between UE and 3GPP AAA Server. W-APN 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 tunnelling 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 PDG, 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 PDG 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.

5.6.3 UE-Initiated Tunnelling

5.6.3.1. UE-Initiated Tunnelling Requirements

The requirements that a UE-Initiated tunnel protocol should meet are:

- Minimal requirements to the underlying IP connectivity network, i.e. UE initiated tunnelling and tunnel establishment signalling can be deployed on top of generic IP connectivity networks
- Minimal impacts to the WLAN
- Establishment of trusted relationships (e.g. mutual authentication for both tunnel end-points) shall be possible
- Tunnel IP configuration of the UE may be obtained from/through the remote tunnel endpoint
- Set up secure tunnels between UE and remote tunnel endpoint. Especially support encryption and integrity protection during tunnel establishment and while transporting user data packets, if enabled.
- User data IP addresses (inner IP):
    - The transport of IPv4 packets shall be supported
    - The transport of IPv6 packets shall be supported (e.g. in order to support IPv6 services like IMS)
- Transport IP addresses (outer IP)
    - Tunnel shall be able to support IPv4 and IPv6 transport addresses
    - Non-routable in the public internet (e.g. private)~~Non-public routable~~ transport IP addresses shall be supported
- The protocol should be fully specified and 3GPP should define its usage to enable multi-vendor inter-operability

5.6.3.2. UE-Initiated Tunnelling Mechanism

In UE-initiated tunnelling, 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. UE indicates that it wishes to use UE-initiated tunnelling. A W-APN may be transmitted as part of the end-to-end signaling.
2. The 3GPP AAA server decides that UE-Initiated tunnelling shall be used for this session.
3. Mutual tunnel authentication shall be applied between UE and tunnel endpoint.
4. 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 networks simultaneously. The actual IP network selection is performed as part of the establishment of each tunnel. Tunnel establishment and tunnelling may be performed for example using Mobile IP.

UE-Initiated, HPDG-Terminated Tunnelling shall be supported (at least for the non roaming case).

Routing towards the Home PLMN in the Visited PLMN, as well as its impacts on the WLAN AN, are for further study.

5.7 Charging Requirements

- The WLAN Access Network shall be able to report the WLAN access usage to the appropriate 3GPP system
- It shall be possible for the 3GPP system to command some operations on a specific ongoing WLAN 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 WLAN, PS, CS, and IMS per user.
- It shall be the role of the 3GPP system to process the WLAN 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 nodes.

5.8 Charging Mechanisms

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

5.8.1 Offline Charging

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

5.8.2 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.

5.9 3GPP Network Advertisement and Selection

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

In addition to radio network selection, the WLAN UE may need to select a VPLMN through which to authenticate, if more than one is available through the chosen radio network.

Radio network advertisement and selection depends on the particular WLAN technology.

VPLMN advertisement and selection is independent of WLAN technology.

The generic Network Advertising and Selection scenario is illustrated in figure 5.1.

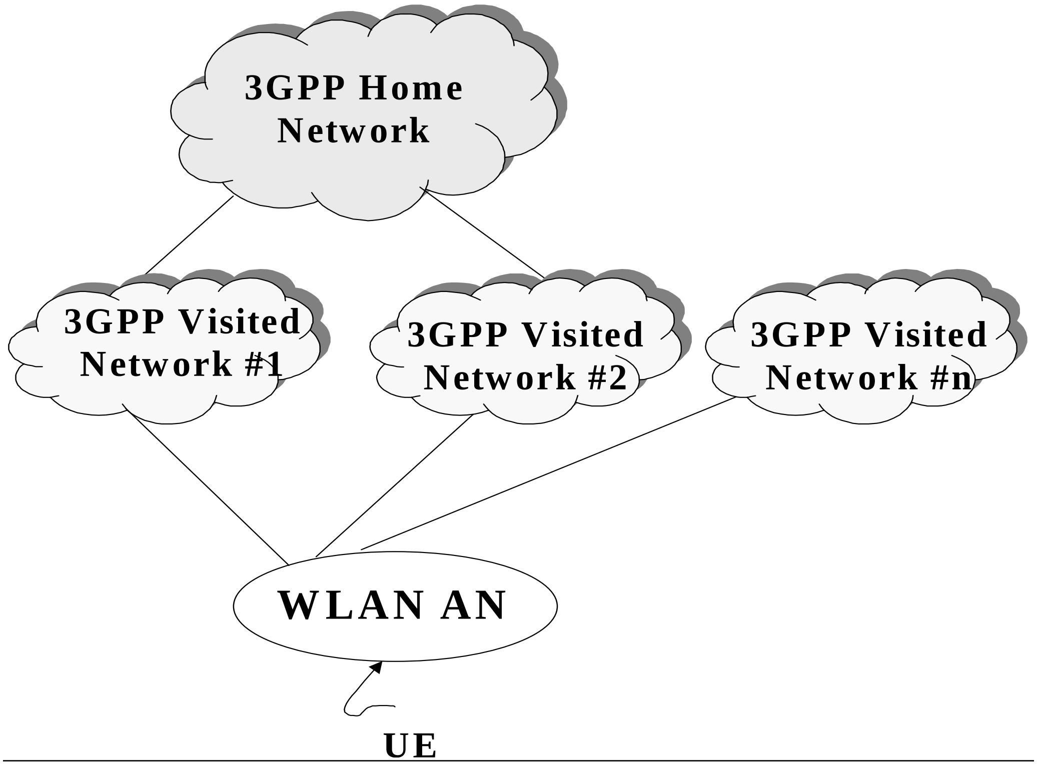


figure 5.1 Network Advertising and Selection Scenario

An area is shown covered by a a WLAN Access Networks (WLAN AN) having a set of roaming agreements with different 3G networks (3GPP Visited Network #1,#2,…,#n). A UE entering the WLAN AN wants to connect to his own 3GPP Home Network to which he is a subscriber (as shown in Figure 1).

Referring to the figure the user subscribing to the services provided to the 3GPP Home Network can reach the associated home network in two different ways, e.g. via either of 3GPP Visited Network #1 or 3GPP Visited Network #2.

5.9.1 Radio Network Selection

5.9.1.1 Case of IEEE 802.11 WLANs

~~5.9.1.1 Basic Principles~~

The following principles shall apply:

- Require no modifications of existing legacy APs.
- Have no impact on existing legacy clients (implies no modification of current broadcast SSIDs).
- Have low latency and overhead.
- Allow but not require support for multiple SSIDs.

A 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]

Support for 3GPP interworking by a WLAN may be indicated by the support of a I-WLAN SSID value by the WLAN. This SSID may either be the Broadcast SSID or may be probed for by the UE.

If the Broadcast SSID doesn't contain the I-WLAN SSID value the 3GPP WLAN UE client may probe for it. If this I-WLAN SSID is not available, the client shall select the available Broadcast SSID instead.

The I-WLAN SSID value for 3GPP interworking WLANs is defined in TS xx.yyy

Editors note: the TS number is to be replaced by reference to appropriate Stage 3 specification.

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

5.9.1.2 Case of HiperLan/2 WLANs

FFS

5.9.1.3 Case of Bluetooth WLANs

FFS

5.9.2 VPLMN Advertisement and Selection

The following principles shall be used in VPLMN ~~Network~~ Advertisement and Selection:

- The user shall be able to select the Visited Network
- Use the NAI for routing of AAA messages.
- ~~Require no modifications of existing legacy APs.~~
- ~~Have no impact on existing legacy clients (implies no modification of current broadcast SSIDs).~~
- Have low latency and overhead.
- Use existing EAP mechanisms, if possible.
- ~~Allow but not require support for multiple SSIDs.~~
- Be extensible to permit advertisement of WLAN characteristics other than the PLMNIDs of roaming partners.

5.9.2~~1~~.~~2~~1 Network Advertisement

Network advertisement information shall be provided~~ by a TBD mechanism~~which enumerat~~ing~~es the roaming partners and associated NAI realms. A single mechanism shall be used to provide that information. This information shall be ~~delivered to the WLAN UE via a FFS EAP based mechanism and shall be~~ provided to the WLAN UE when the WLAN has no direct roaming relationship with the subscribers HPLMN.

5.9.~~1~~2.~~3~~2 Network Selection

~~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]~~

~~Support for 3GPP interworking by a WLAN may be indicated by the support of a well-known SSID value by the WLAN. This SSID may either be the Broadcast SSID or will be probed for by the UE.~~

~~If the Broadcast SSID doesn't contain the well-known value the 3GPP WLAN UE client shall probe for it. If this well-known SSID is not available, the client shall select the available Broadcast SSID instead.~~

~~The well-known SSID value for 3GPP interworking WLANs is defined in TS xx.yyy~~

~~Editors note: the TS number is to be replaced by reference to appropriate Stage 3 specification.~~

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

The WLAN UE shall provide an initial NAI, constructed according to Section 5.4.2 indicating the UE's Home Network, in response to the EAP-Request/Identity. If the WLAN AN recognizes the realm of the initial NAI (i.e. has a direct roaming relationship with the UE's Home ~~that~~ operator), then no special processing for network advertisement/selection is needed.

If the WLAN AN has no direct roaming relationship with the initial realm, the WLAN AN shall deliver the network advertisement information to the UE. The UE processes this information according to its internal roaming preference policies or prompts the user to select a VPLMN preference. It uses the result to determine how to construct a new NAI indicating the selected VPLMN, according to Section 5.4.2.

The realm portion of the new NAI shall be constructed according to Section 5.4.2 based on the chosen Visited Network MCC and MNC. The information about the Home Network shall be inserted in the username part of the new NAI.

The construction of the username part of the new NAI is FFS.

~~Note: the manner in which the selected VPLMN is indicated in the new NAI is ffs.~~

After the network advertisement information is delivered, the ~~WLAN AN shall initiate a second EAP-Request/Identity message. The~~ UE attempts to authenticate with~~responds to this message~~ ~~with~~ the new NAI determined in the prior step.

The WLAN A~~AA proxy~~N shall use the NAI to route the EAP traffic to the appropriate VPLMN AAA Proxy.

~~5.9.2 Case of HiperLan/2 WLANs~~

~~FFS~~

~~5.9.3 Case of Bluetooth WLANs~~

~~FFS~~

5.10 Scenario 3 Routing Enforcement

Scenario 3 requires that all packets sent to/from a WLAN UE are routed via a ~~PDG~~ WAG in a 3GPP network.

In order to ensure operator policies, e.g. QoS, Charging can be applied to user traffic ~~users cannot circumvent routing via a PDG~~, scenario 3 requires routing policy enforcement to be implemented in the 3GPP-WLAN interworking system ~~and for the WLAN UE not to be involved in such a process~~.

5.10.1 Routing Enforcement in the WLAN AN

When operating in scenario 3, the WLAN AN needs to ensure that all packets sent to/from a WLAN UE are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case). In addition, it shall be possible for the 3GPP network to provide the WLAN with routing enforcement information to restrict the destinations the UE's packets can be sent to. When the WLAN receives packets sent from an UE against the routing policy defined by 3GPP network, it could be possible for the WLAN to discard those packets before they are routed into 3GPP network

~~5.10.2 Enforcement in the last hop router~~

~~When operating in scenario 3, the operator of the last hop router (either the WLAN AN or VPLMN) may need to ensure that users cannot circumvent routing through the PDG by re-configuring their IP address.~~

5.10.2~~3~~ Policy Enforcement in the HPLMN

When operating in scenario 3 and the HPLMN decides that access is via a PDG in the HPLMN, the HPLMN shall be able to provide the VPLMN with suitable policy enforcement information. The HPLMN may also provide suitable routing enforcement policy information to WLAN.

5.10.3~~4~~ Policy Enforcement in the VPLMN

When operating in scenario 3, the VPLMN shall be able to implement policy enforcement on traffic sent to/from a WLAN UE according to policy enforcement information provided by the HPLMN. The VPLMN may also provide suitable routing enforcement policy information to WLAN.

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

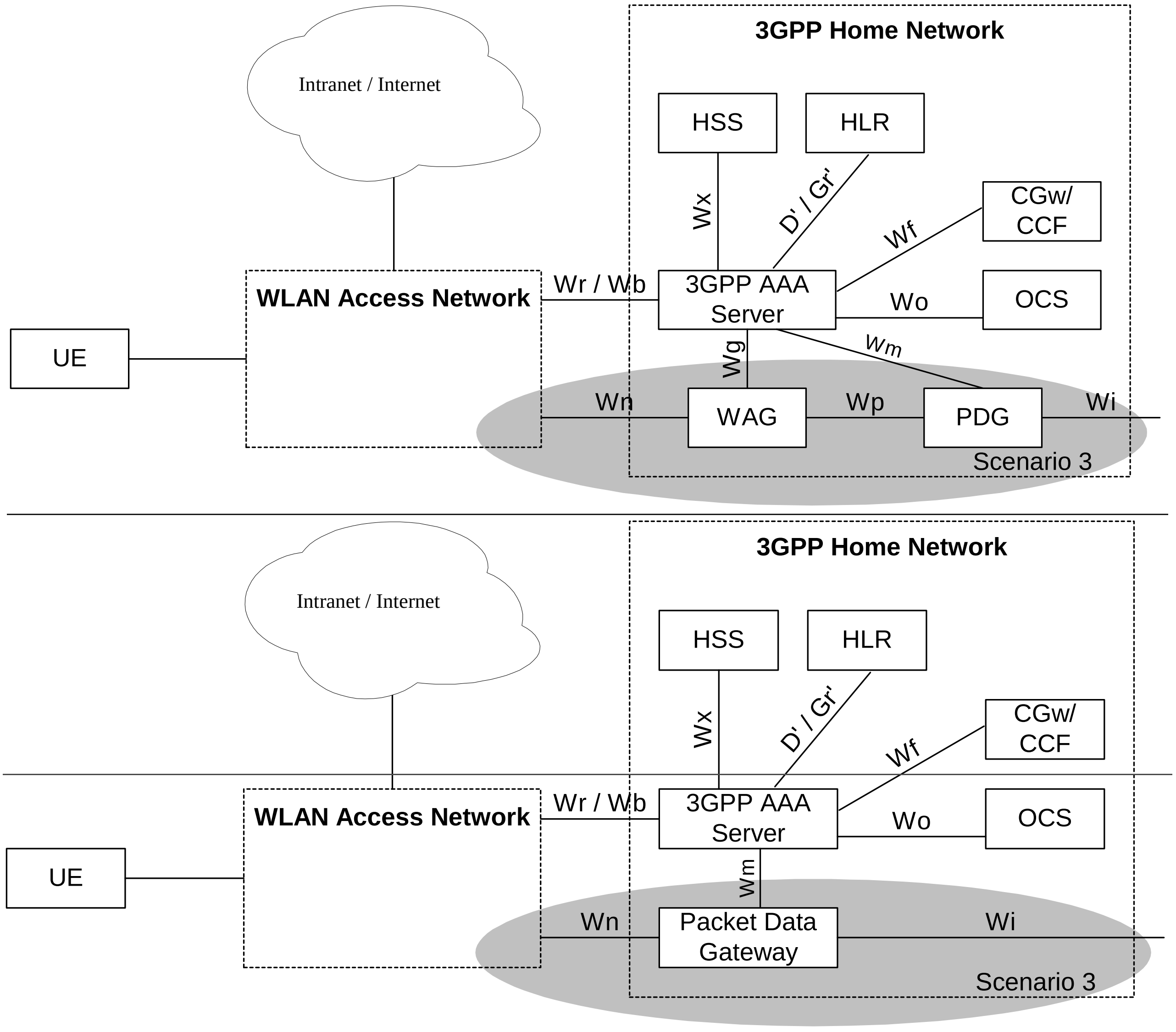


figure 6.1 Non Roaming Reference Model. The shaded area refers to scenario 3 functionality.

6.1.2 Roaming WLAN Inter-working Reference Model

6.1.2.1 WLAN Roaming Architecture Principles

For the delivery of 3GPP PS based 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.

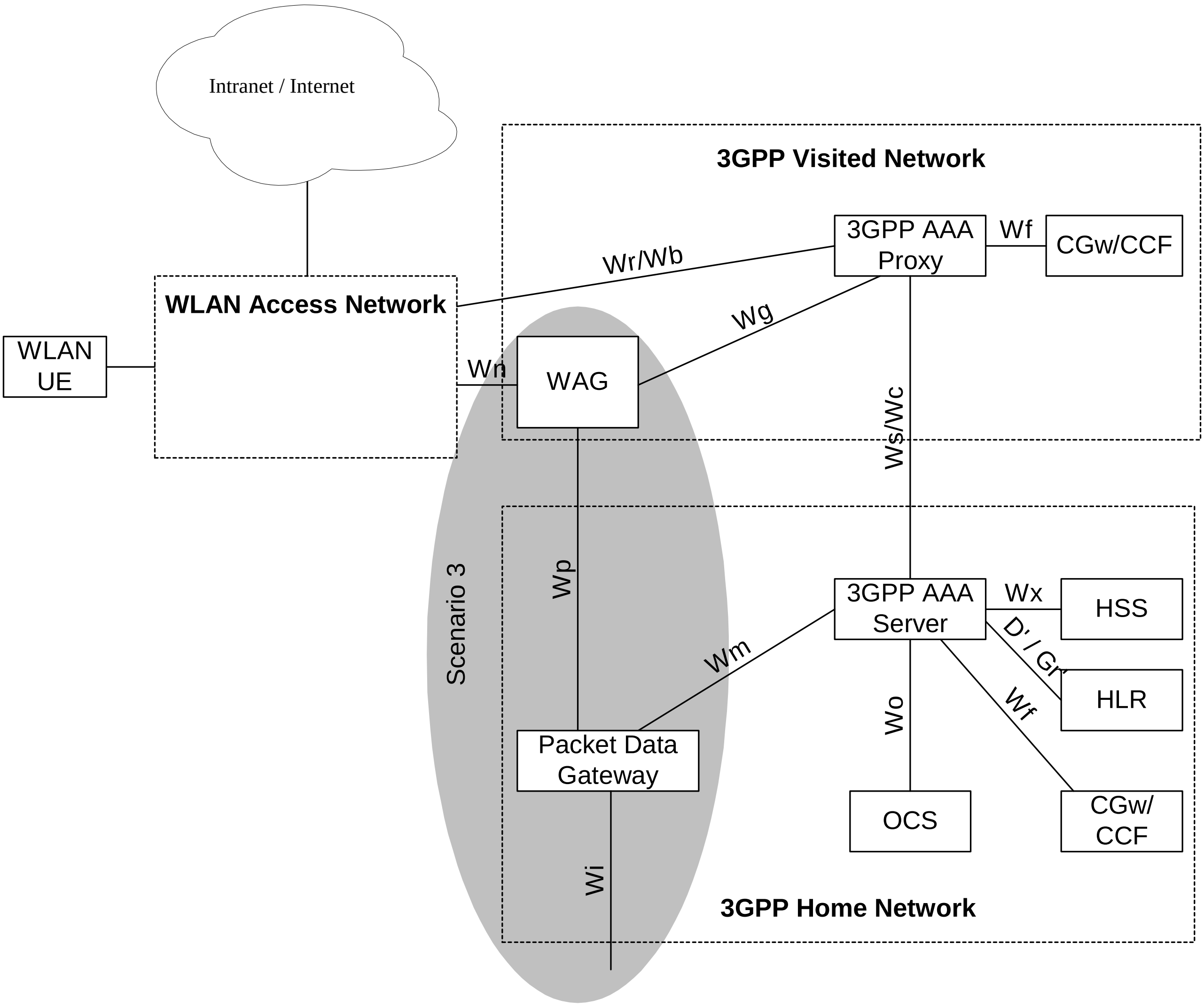
- The roaming architecture shall provide the ability to allow the user to access services provided by the visited network, e.g. IMS local services.
- The roaming architecture shall ensure that the home network can provide a sub-set of the 3GPP services.

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 home 3GPP network interfaces to other 3GPP networks via the inter-operator Ws and Wc interfaces.

The 3GPP AAA proxy relays access control signalling and accounting information to the home 3GPP AAA Server using the Ws and Wc interfaces.

It can also issue charging records to the visited network CGw/CCF when required. The 3GPP network interfaces to WLAN Access Networks via the Wr and Wb interfaces.


Intranet / Internet
3GPP Visited Network
3GPP AAA Proxy
Wf
CGw/CCF
Wr/Wb
Wg
WLAN Access Network
WLAN UE
Wn
WAG
Ws/Wc
Scenario 3
Wp
3GPP AAA Server
Wx
HSS
D' / Gr
HLR
Wm
Wf
Wo
Packet Data Gateway
OCS
CGw/ CCF
Wi
3GPP Home Network

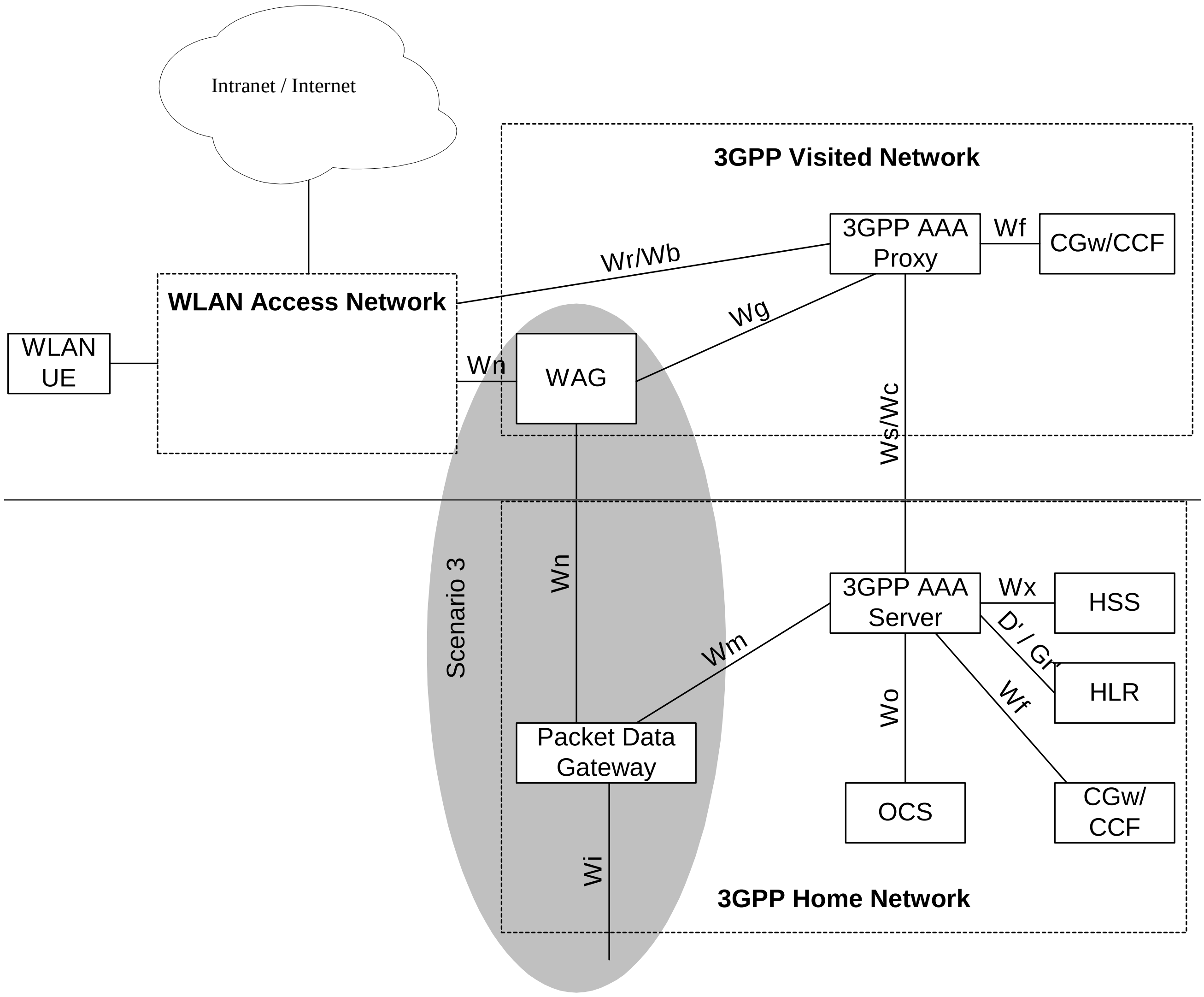
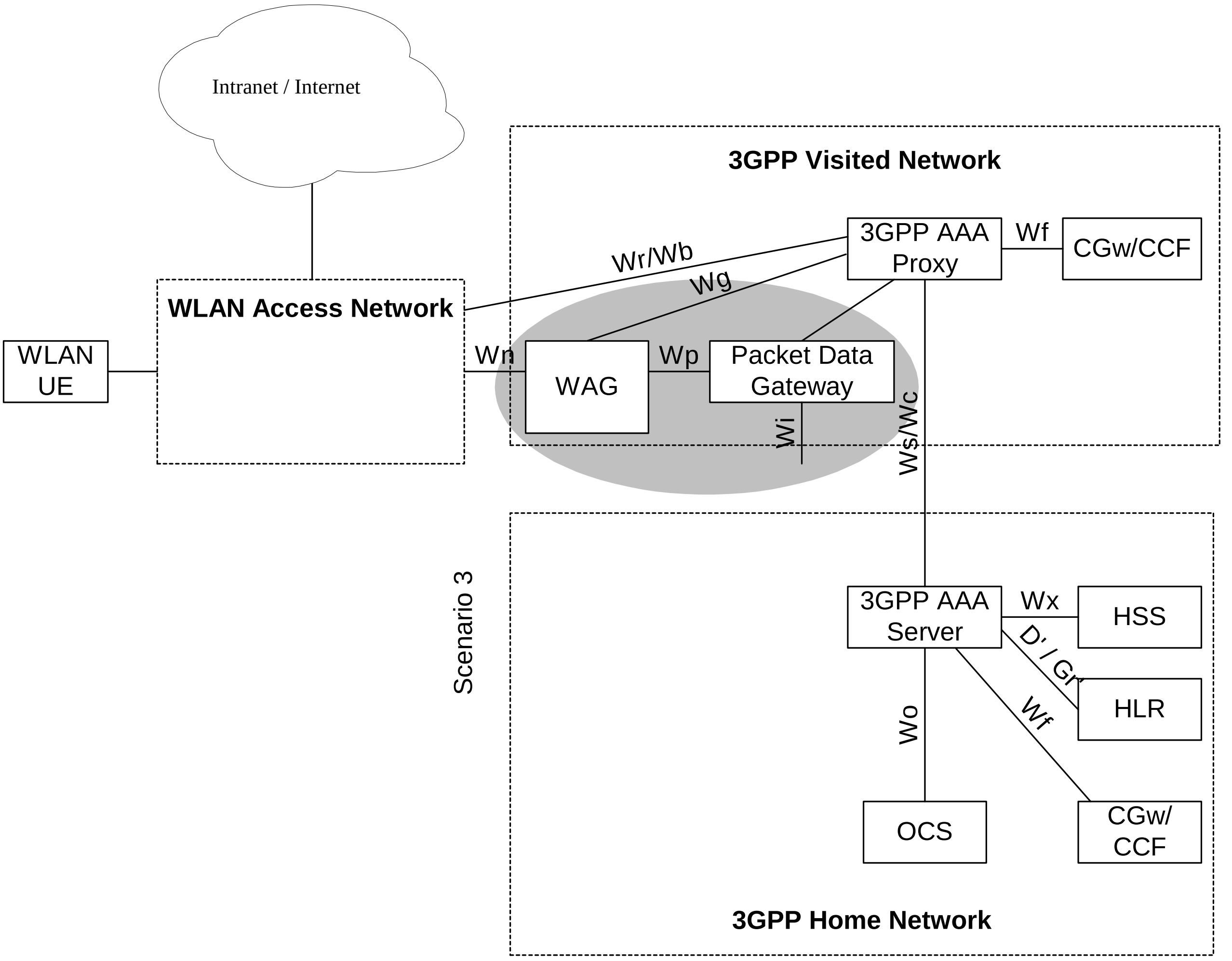


Figure 6.2.a. Roaming Reference Model- 3GPP PS based services provided via the 3GPP Home Network (the shaded area refers to scenario 3 functionality)


Intranet / Internet
3GPP Visited Network
3GPP AAA Proxy
Wf
CGw/CCF
Wr/Wb
Wg
WLAN Access Network
WLAN UE
Wn
WAG
Wp
Packet Data Gateway
Wi
Ws/Wc
Scenario 3
3GPP AAA Server
Wx
HSS
D' / Gr'
HLR
Wf
Wo
OCS
CGw/ CCF
3GPP Home Network

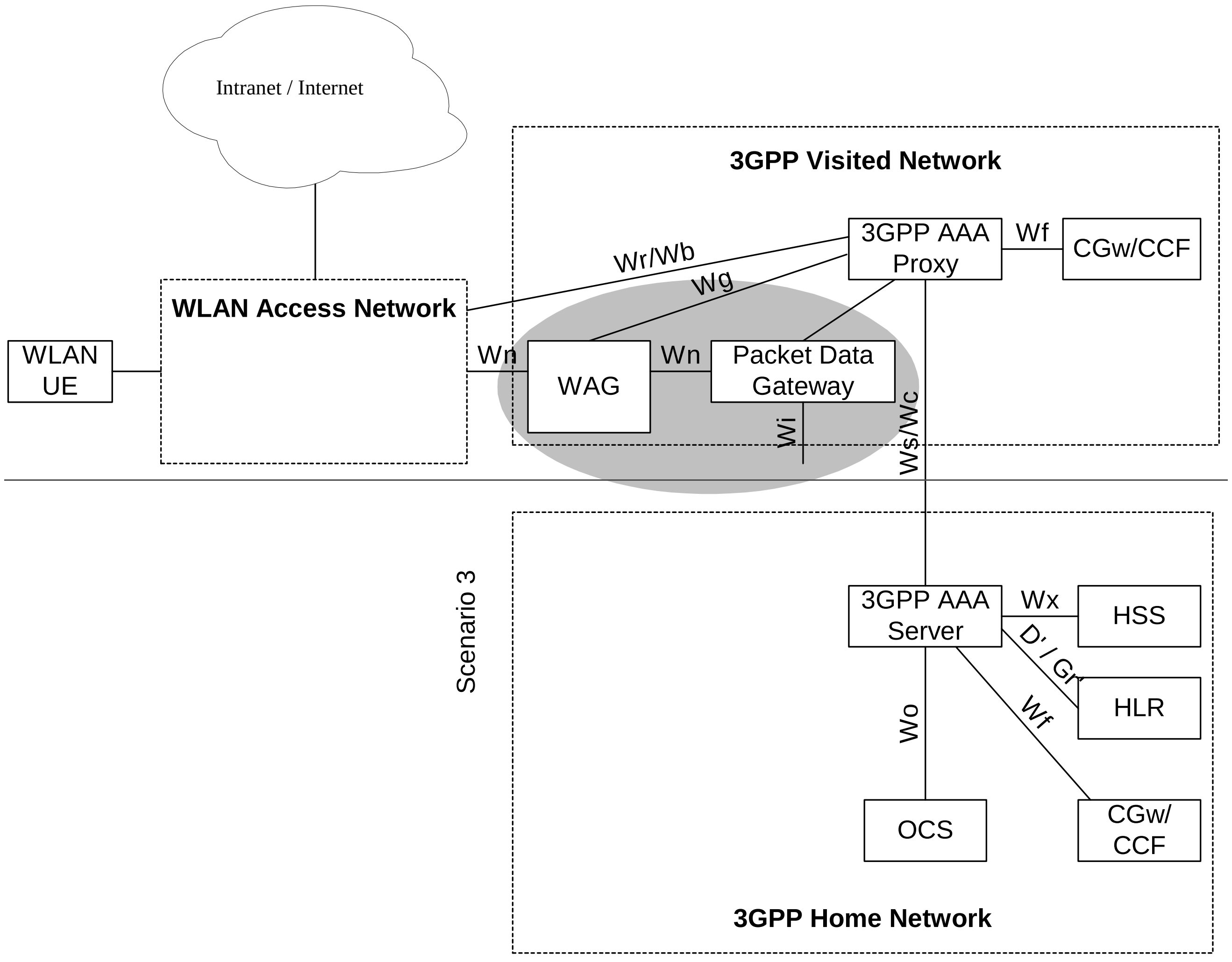


Figure 6.2.b. Roaming Reference Model- 3GPP PS based services provided via the 3GPP Visited Network (the shaded area refers to scenario 3 functionality)

6.2 Network elements

6.2.1 WLAN UE

- The WLAN UE is the UE (equipped with UICC card including (U)SIM) utilized by a 3GPP subscriber to access the WLAN interworking. The UE may be capable of WLAN access only, or it may be capable of both WLAN and 3GPP System accesses. 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 UICC), 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, UICC card reader and suitable software applications.

6.2.2 3GPP AAA Proxy

- The 3GPP AAA Proxy represents a Diameter proxying and filtering function that resides in the Visited 3GPP Network. The 3GPP AAA Proxy functions include:

    - Relaying the AAA information between WLAN and the 3GPP AAA Server.
    - Enforcing policies derived from roaming agreements between 3GPP operators and between WLAN operator and 3GPP operator
    - Reporting charging/accounting information to local CCF/CGw for roaming users
    - Service termination (O&M initiated termination from visited network operator)

    For Scenario 3 only:

    - Receiving authorization information related to subscriber requests for services in the Home or Visited network
    - Authorization of access to Visited network services according to local policy
    - RADIUS/Diameter conversion when the Wr and Ws or Wb and Wc interfaces do not use the same protocol

The 3GPP AAA Proxy 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 authorization 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 authorization 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 authorized 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).

    o Maintains the UE’s WLAN-attach status.

    o Provides the UE’s WLAN-attach status to other entities.

    o Generates and reports charging/accounting information to CCF/CGw for users.

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.
- The HSS also provides access to the UE's WLAN-attach status for other entities, e.g. answers or relays the WLAN-attach status query from other entities.

Additional network elements in scenario 3:

6.2.5 WLAN Access Gateway

Support of WAG in scenario 2 is optional.

- The WLAN Access Gateway is an optional gateway via which the data to/from the WLAN Access Network can be routed via a PLMN.
- The WLAN Access 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 WLAN Access 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.
  - Enforces routing of packets through the PDG.

Per-user charging generation in the WAG is FFS.

Note 1: per-user charging generation is provided by the 3GPP AAA proxy in scenario 2 and can be used for mediation into TAP3 tickets including binding to a user's 3GPP identity.

Note 2: per-user charging generation in the WAG is not required when the WAG and PDG are in the same network.

Support of WAG in scenario 3 is mandatory for the roaming case~~. In~~ and for the non-roaming case~~, whether the WAG is mandatory is for further study~~.

- In Scenario 3 the WAG shall provide routing policy enforcement.

  If service is provided through a PDG in the HPLMN the WAG:

  - Ensures that all packets from the UE are routed to the HPLMN.
  - Ensures that packets from authorised UEs are only routed to the PDG in the HPLMN and that packets from other sources than the PDG in the HPLMN are not routed to the UE.

  If service is provided through a PDG in the VPLMN the WAG:

  - Ensures that all packets from the UE are routed to the VPLMN.
  - Ensures that packets from authorised UEs are only routed to the PDG in the VPLMN and that packets from other sources than the PDG in the VPLMN are not routed to the UE.

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

6.2.5.1. Routing Enforcement

Information regarding the selected PDG, including whether the PDG is in the HPLMN or the VPLMN is provided by the HPLMN to the VPLMN.

In the roaming case, the PDG information is delivered from the HPLMN to the VPLMN using AAA signalling.

Within the VPLMN, the routing policy enforcement information is delivered to the WAG.

Details of the policy enforcement information are FFS.

Note: Whether information regarding one or all PDGs is provided will likely impact the signalling which supports the activation of a further W-APN. Delivering information of all valid PDGs may limit impacts on signalling for further W-APN establishment.

The policy enforcement delivered during initial authentication will be bound to a user’s AAA signalling. The WAG requires functionality to be able to securely bind this information to a user’s traffic.

It is FFS how this binding is achieved.

The binding of the policy to a user's traffic allows the WAG to drop un-authorized packets sent to/from a user.

6.2.5.2. Per-user Charging Generation is FFS

If required, according to the above requirements for routing enforcement, the WAG has sufficient information to bind a user’s traffic to AAA signalling (and implicitly to a user’s 3GPP identity). The binding can allow an accounting client in the WAG to generate charging records and correlate these with AAA signalling. Hence, per-user charging information can be generated.

6.2.5.3. Summary

Scenario 3 option requires new functionality to exist in the VPLMN, in the WAG.

Two issues which are FFS are:

1. The detailed definition of routing enforcement information delivered to the WAG (including between HPLMN and VPLMN)

2. How the WAG binds the routing enforcement to a user’s traffic.

Note1: Since bullet item 1 is largely decoupled from discussion on tunnelling options, from a WAG perspective, the key differentiator is how the WAG binds the routing enforcement to a user’s traffic.

Note 2: Binding of the per-user charging records generated by the WAG (if required) can be built on the scenario 2 functionality which binds a user’s 3GPP identity to AAA based accounting.

6.2.6 Packet Data Gateway

3GPP PS based services (Scenario 3) are accessed via a Packet Data Gateway. 3GPP PS based services may be accessed via a Packet Data Gateway in the user's Home Network or a PDG in the selected VPLMN. The process of authorisation and service selection (e.g. W-APN selection) and subscription checking determines whether a service shall be provided by the home network (Figure 6.2.a) or by the visited network (Figure 6.2.b). The resolution of the IP address of the Packet Data Gateway providing access to the selected service will be performed in the PLMN functioning as the home network (in the VPLMN or HPLMN). Successful activation of a selected service results in

- Determination of the Packet Data Gateway IP address used by the UE
- Allocation of an IP address (the UE's home address) to the UE by the HPLMN (if one is not already allocated)
- Registration of the IP address allocated by the WLAN/VPLMN with the Packet Data Gateway and binding of this address with the home IP address

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 de-capsulation and encapsulation;
- Allows allocation of the IP address by which the UE is identified by the Home Network;
- Performs registration of the address allocated by the WLAN/VPLMN (e.g. transport address) and binding of this address with the home IP address;
- Provides procedures for unbinding a transport address with the home IP address;
- Provides procedures for authentication and prevention of hijacking (i.e. ensuring the validity of the UE initiating any binding of transport address with the home address, unbinding etc.)
- May filter out unauthorised or unsolicited traffic with packet filtering functions. All types of message screening are left to the operators' control, e.g. by use of Internet firewalls.
- 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 Network (i.e. the 3GPP AAA Proxy in the roaming case and the 3GPP AAA server in the non-roaming case). The prime purpose of the protocols crossing this reference point is to transport 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 Network.
- Carrying data for authorization signalling between WLAN AN and 3GPP Network.
- Enabling the identification of the operator networks amongst which the roaming occurs.

- Carrying keying data for the purpose of radio interface integrity protection and encryption.
- When such functionality is supported by the WLAN AN, purging a user from the WLAN access for immediate service termination

6.3.1.3 Protocols

Wr reference point 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.

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 (for WLAN Access) 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.
- Retrieval of service related information (e.g. W-APNs that may be selected by the UE) including an indication of whether the VPLMN is allowed to provide this service.

6.3.3 D'/Gr'

This optional reference point is located between 3GPP AAA Server and pre-R6 HLR/HSS. 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.

When the HLR makes it possible ~~T~~the functionality of the reference point is to enable:

- Retrieval of authentication vectors, e.g. for USIM authentication, from HLR.

- Registration of the 3GPP AAA Server of an authorised WLAN user in the HLR.
- Indication of change of subscriber profile within HLR(e.g indication for the purpose of service termination).
- Purge procedure between the 3GPP AAA server and the HLR.
- Fault recovery procedure between the HLR and the 3GPP AAA server.
- Retrieval of service related information (e.g. APNs that may be selected by the UE) including indications of whether the service is to be supported by the HPLMN or by an identified VPLMN.
- Retrieval of online/offline charging function address from HLR.

Please refer to Annex A for further details of how this may work for different network scenarios.

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 WLAN user

To minimize the requirements put on the WLAN Access Network and to protect the confidentiality of the subscriber's 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 WLAN user.

Additional reference points in scenario 3:

6.3.7 Wg

This is an AAA interface between the 3GPP AAA proxy and the WAG. It is used to provide information needed by the WAG to perform routing enforcement functions for authorised users.

6.3.8 Wn

This is the reference point between the WLAN Access Network and the WAG. This interface is to force traffic on a UE initiated tunnel to travel via the WAG. A site-to-site tunnel (see Annexes D and E) may be provided for the routing enforcement.~~The definition of this reference point is for further study~~

6.3.9 Wp

This is the reference point between the WAG and PDG.

6.3.10~~9~~ Wi

This is the reference point between the Packet Data Gateway 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 IMS, RADIUS Accounting or Authentication, DHCP.

Wi reference point is similar to the *Gi* reference point provided by the PS domain. Interworking with packet data 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 the use of a private addressing scheme. When 3GPP network is provided for IMS, Wi reference point is used for policy control interface. It is ffs whether Wi or other reference point is used or not.

6.3.11~~0~~ 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 tunnelling attributes and UE's IP configuration parameters from/via Packet Data Gateway.

The protocol crossing this reference point is Diameter.

6.3.12~~1~~ Ws

6.3.12~~1~~.1 General description

The reference point Ws connects the 3GPP AAA Proxy, possibly via intermediate networks, to the 3GPP AAA Server. The prime purpose of the protocols crossing this reference point is to transport authentication, authorization and related information in a secure manner.

6.3.12~~1~~.2 Functionality

The functionality of the reference point is to transport AAA messages including:

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

6.3.12~~1~~.3 Protocols

Ws reference point shall be based on a single AAA protocol. EAP authentication shall be transported over *Ws* reference point.

[Editor’s note: the choice of RADIUS or Diameter is out of the scope of this TS]

6.3.13~~2~~ Wc

The reference point Wc is located between the 3GPP AAA Server and the 3GPP AAA Proxy. The prime purpose of the protocols crossing this reference point is to transport charging related information in a secure manner. The reference point shall be based on a single AAA protocol.

[Editor’s note: the choice of RADIUS or Diameter is out of the scope of this TS]

The functionality of the reference point is to transport:

- Charging signalling per WLAN user

7 Procedures

Editor's note: the following procedures are FFS:

- Subscriber Selects WLAN network/HPLMN;
- Subscriber Registers;
- Subscriber Reselects WLAN/HPLMN/VPLMN;
- Subscriber Activates First Data Tunnel;
- Subscriber Activates Next Data Tunnel;
- Subscriber Deactivates Data Tunnel;
- Subscriber Deactivates Last Data Tunnel;
- WAG requests deregistration;
- PDG requests deregistration;
- 3GPP AAA Server/HLR/HSS requests deregistration;
- 3GPP AAA Server/HLR/HSS updates service information (needed?);

7.1 Authentication and Authorisation

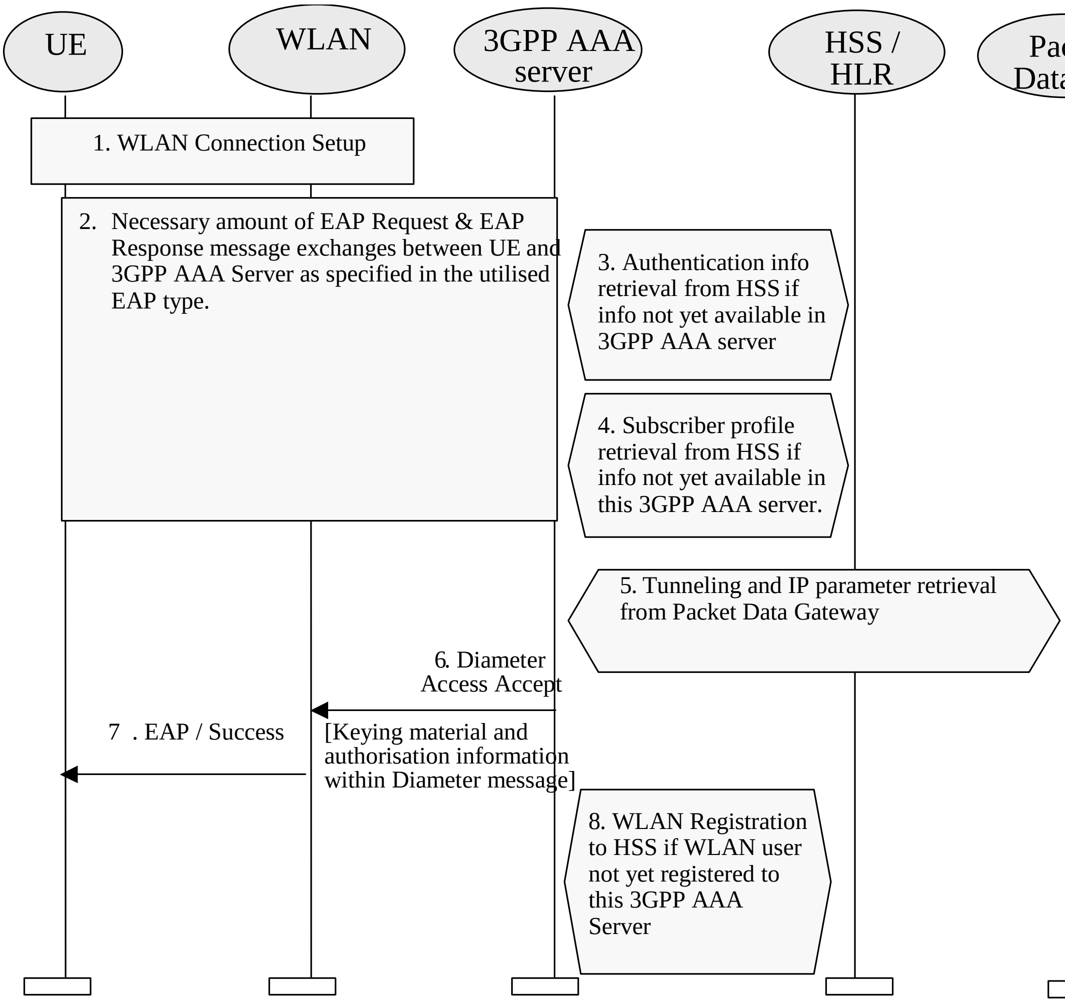

UE
WLAN
3GPP AAA server
HSS / HLR
Packet Data GW
1. WLAN Connection Setup
2. Necessary amount of EAP Request & EAP Response message exchanges between UE and 3GPP AAA Server as specified in the utilised EAP type.
3. Authentication info retrieval from HSS if info not yet available in 3GPP AAA server
4. Subscriber profile retrieval from HSS if info not yet available in this 3GPP AAA server.
5. Tunneling and IP parameter retrieval from Packet Data Gateway
6. Diameter Access Accept
[Keying material and authorisation information within Diameter message]
7 . EAP / Success
8. WLAN Registration to HSS if WLAN user not yet registered to this 3GPP AAA Server

Figure 7.1Authentication and authorisation procedure

1. WLAN connection is established with a WLAN 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 WLAN interface encapsulated within a WLAN 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 Tunnelling 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 message, keying material derived from the EAP authentication as well as connection authorisation information (e.g. NAS Filter Rule or Tunnelling 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

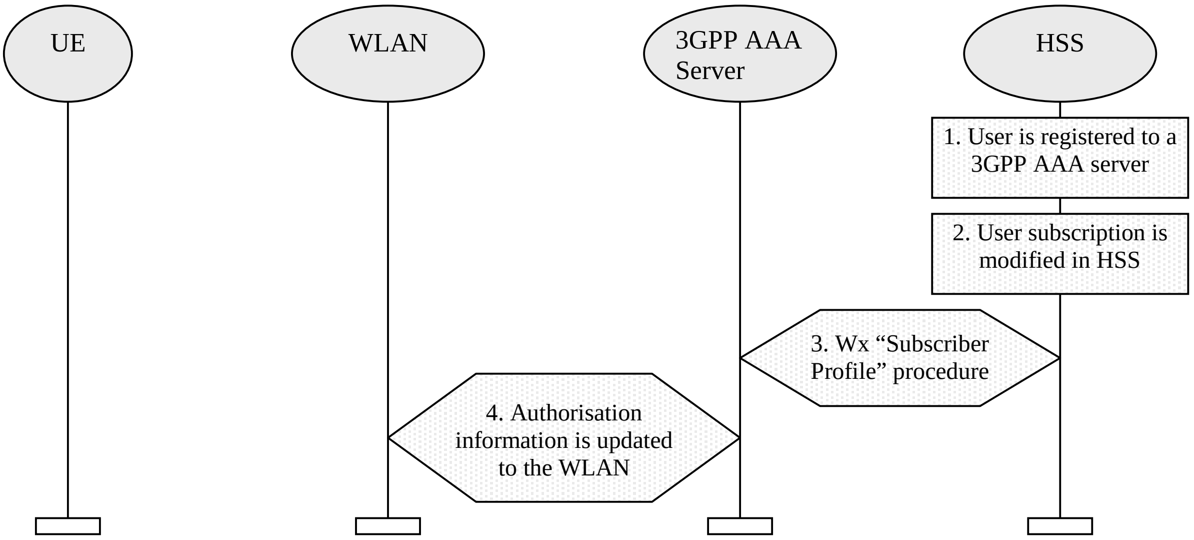

UE
WLAN
3GPP AAA Server
HSS
1. User is registered to a 3GPP AAA server
2. User subscription is modified in HSS
3. Wx “Subscriber Profile” procedure
4. Authorisation information is updated to the WLAN

Figure 7.2 Subscriber Profile Update Procedure

1. User is registered to a 3GPP AAA server

2. Subscribers subscription is modified in the 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 Cancelling WLAN Registration

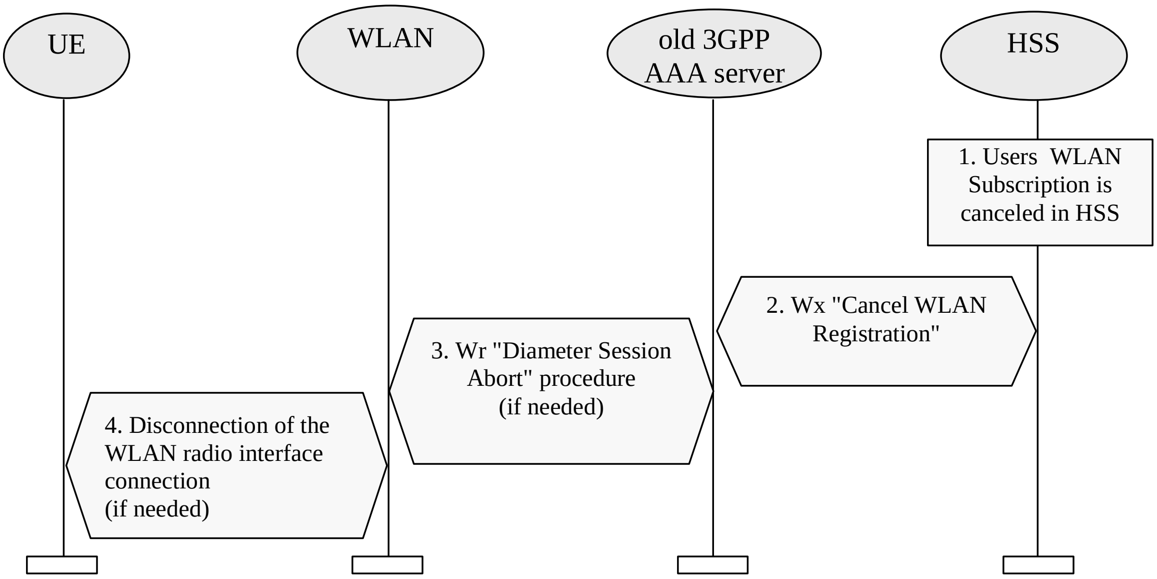

UE
WLAN
old 3GPP AAA server
HSS
1. Users WLAN Subscription is canceled in HSS
2. Wx "Cancel WLAN Registration"
3. Wr "Diameter Session Abort" procedure (if needed)
4. Disconnection of the WLAN radio interface connection (if needed)

Figure 7.3 Cancellation of WLAN Registration Procedure

1. The 3GPP subscribers WLAN subscription is cancelled 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

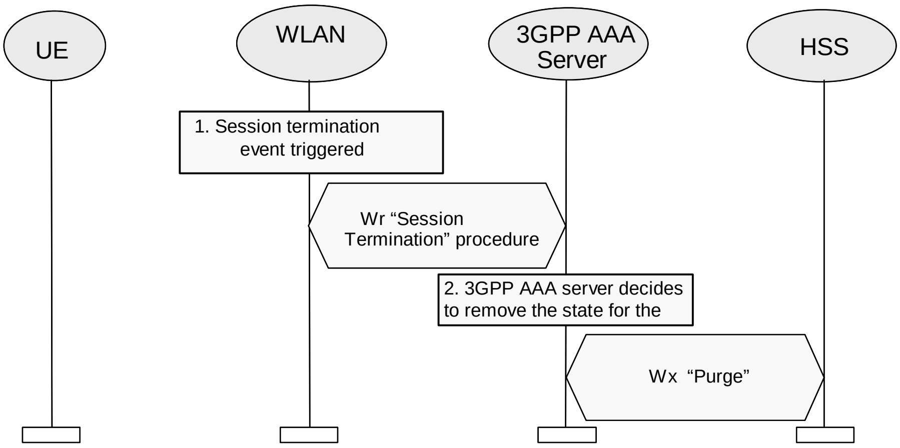

UE
WLAN
3GPP AAA Server
HSS
1. Session termination event triggered
Wr "Session Termination" procedure
2. 3GPP AAA server decides to remove the state for the
Wx "Purge"

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

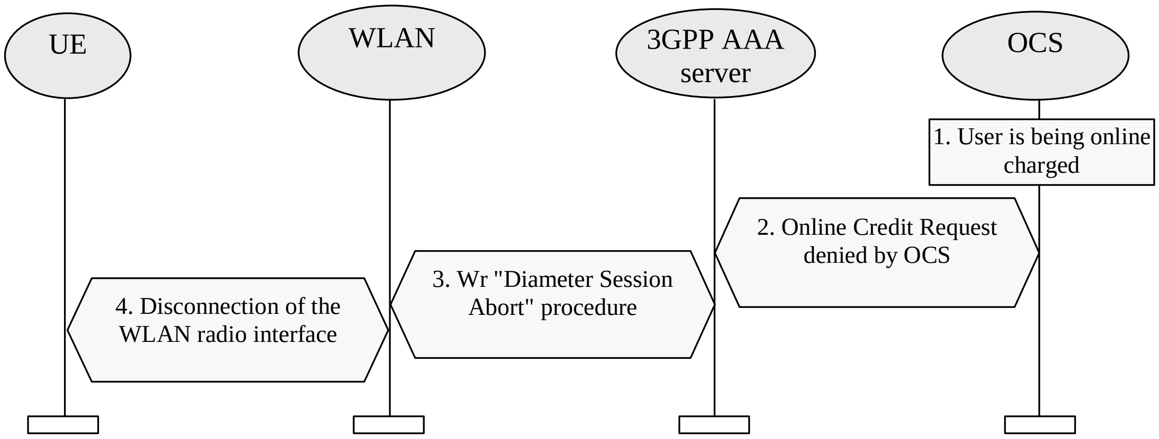

UE
WLAN
3GPP AAA server
OCS
1. User is being online charged
2. Online Credit Request denied by OCS
3. Wr "Diameter Session Abort" procedure
4. Disconnection of the WLAN radio interface

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

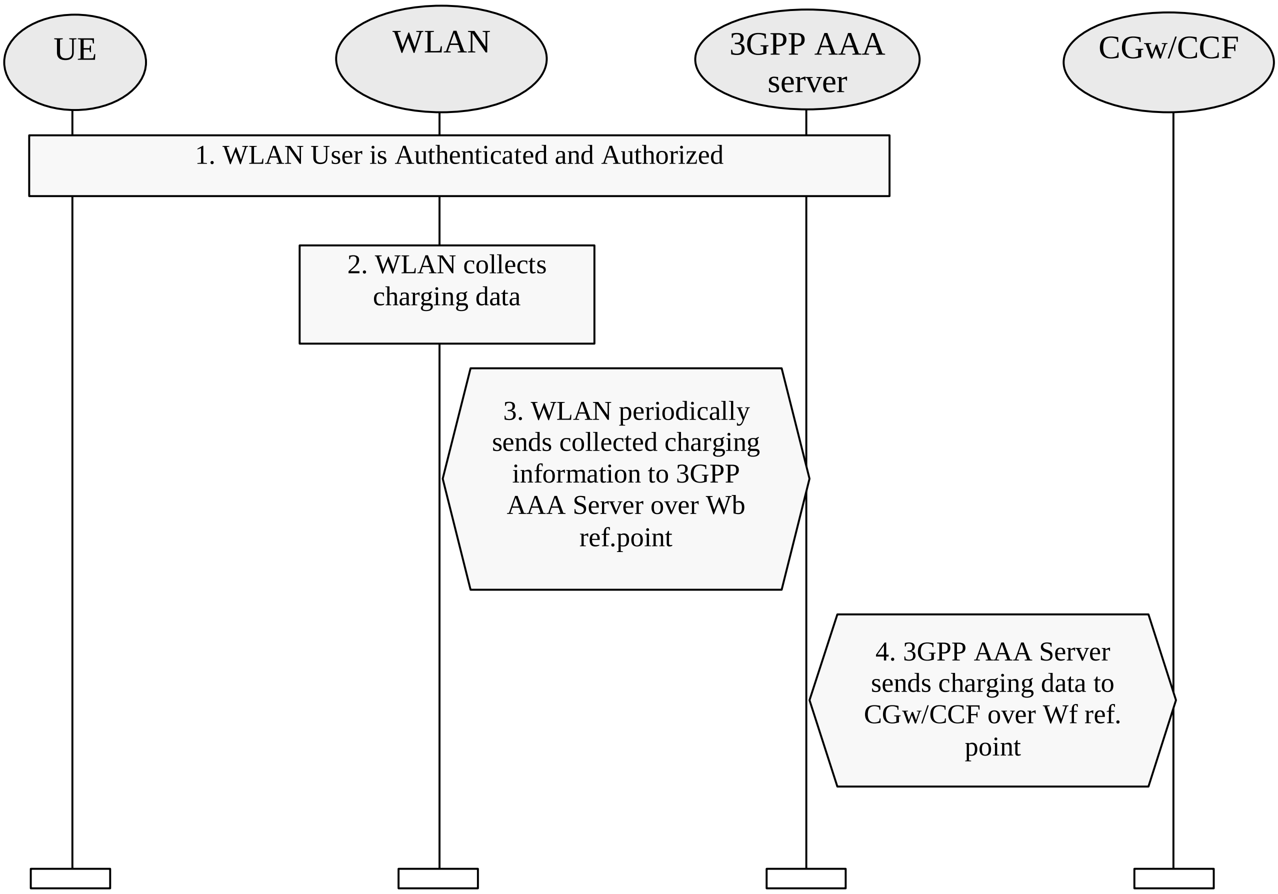

UE
WLAN
3GPP AAA server
CGw/CCF
1. WLAN User is Authenticated and Authorized
2. WLAN collects charging data
3. WLAN periodically sends collected charging information to 3GPP AAA Server over Wb ref.point
4. 3GPP AAA Server sends charging data to CGw/CCF over Wf ref. point

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

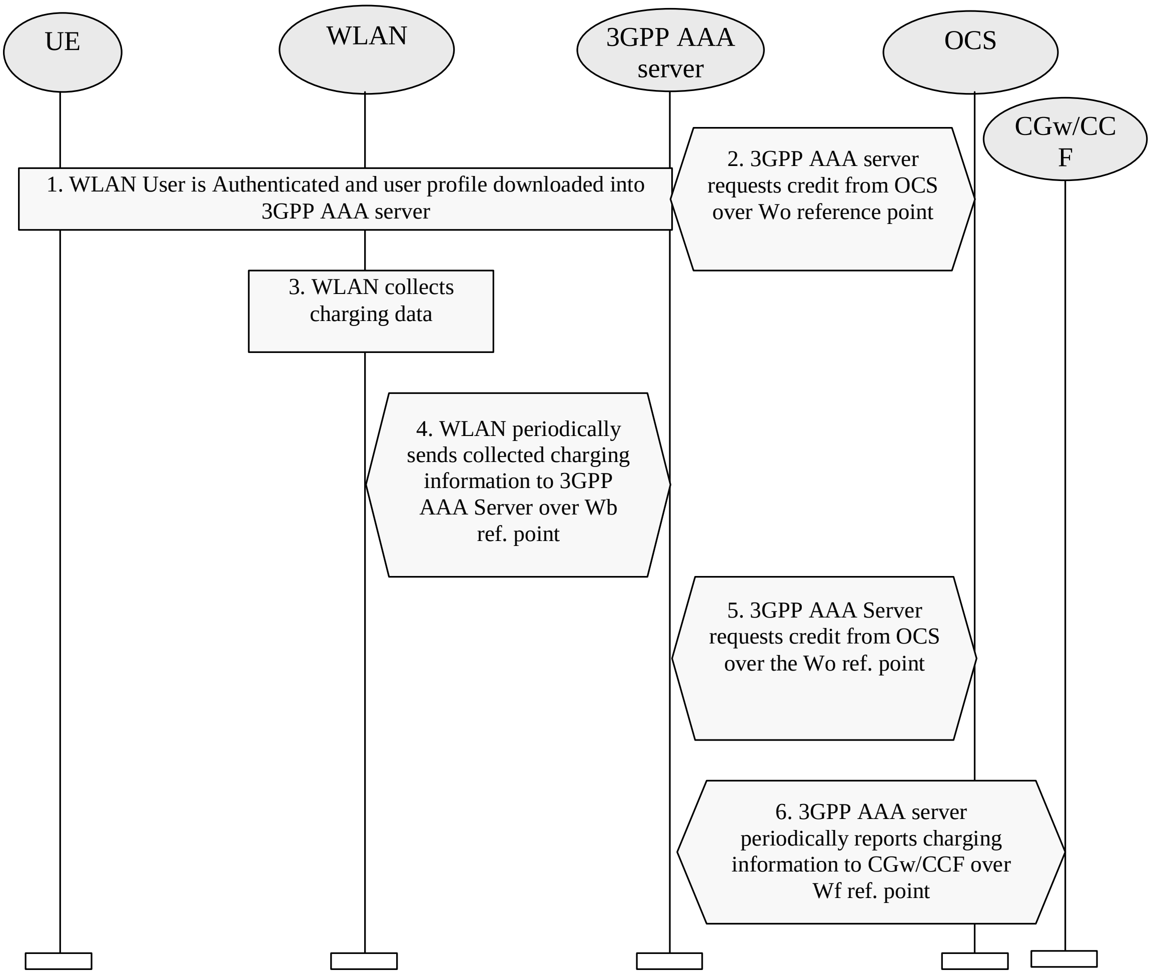

UE
WLAN
3GPP AAA server
OCS
CGw/CC F
1. WLAN User is Authenticated and user profile downloaded into 3GPP AAA server
2. 3GPP AAA server requests credit from OCS over Wo reference point
3. WLAN collects charging data
4. WLAN periodically sends collected charging information to 3GPP AAA Server over Wb ref. point
5. 3GPP AAA Server requests credit from OCS over the Wo ref. point
6. 3GPP AAA server periodically reports charging information to CGw/CCF over Wf ref. point

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.

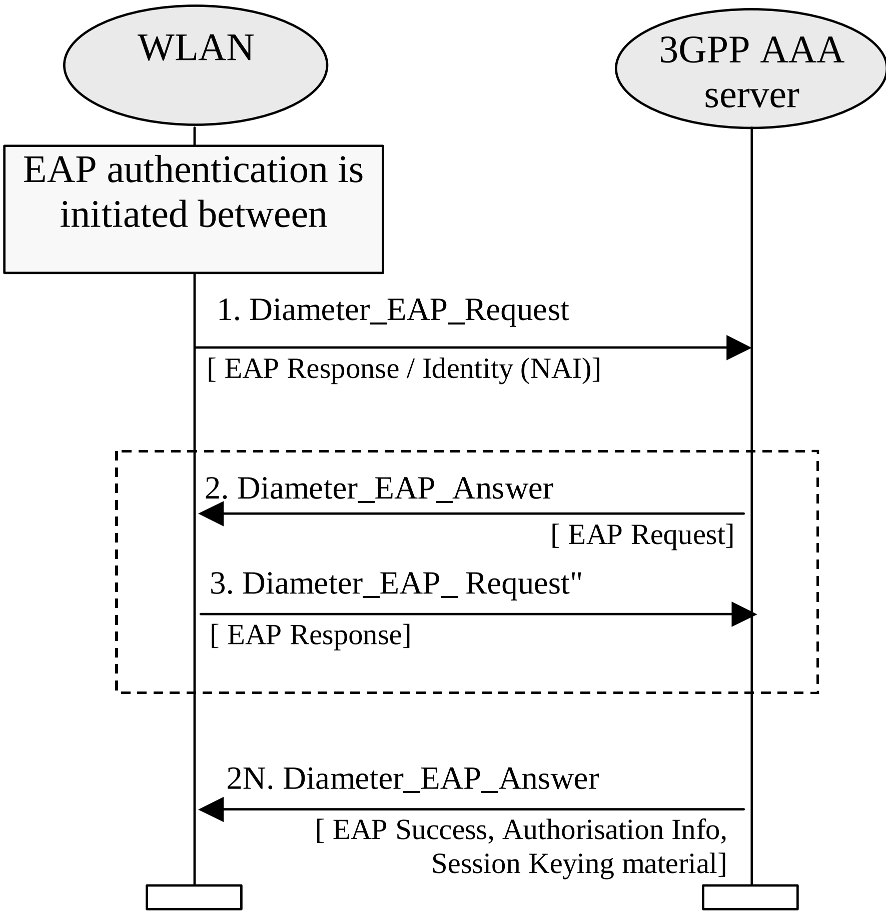


Figure A.1.1 Signalling example on Wr Reference Point for Authentication and Authorisation

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 Tunnelling attributes) for the authenticated session. Message also carries the keying material from 3GPP AAA Server to WLAN to be used for the authenticated session by WLAN.

A.1.2 Immediate purging of a user from 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 cancelled or when the 3GPP subscribers online charging account expires.

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

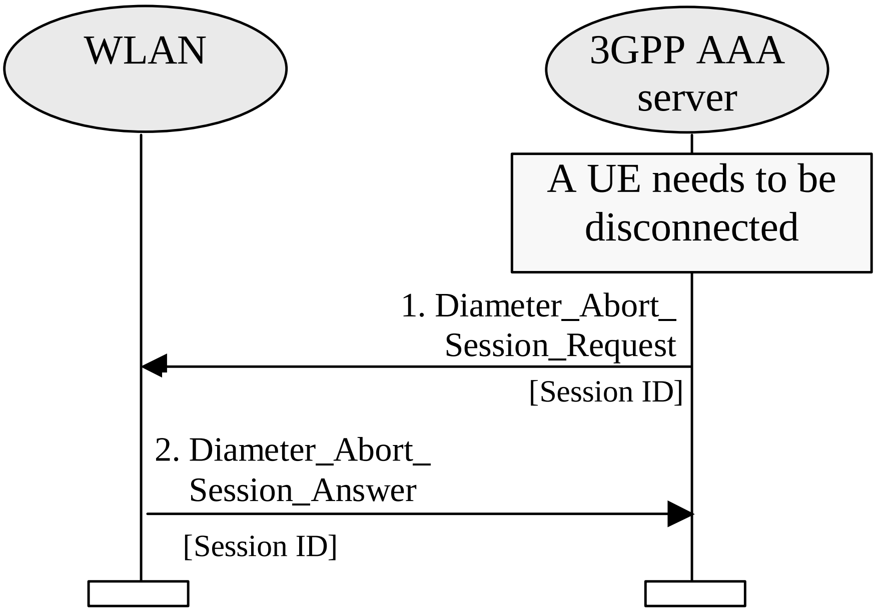

WLAN
3GPP AAA server
A UE needs to be disconnected
1. Diameter_Abort_ Session_Request
[Session ID]
2. Diameter_Abort_ Session_Answer
[Session ID]

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.

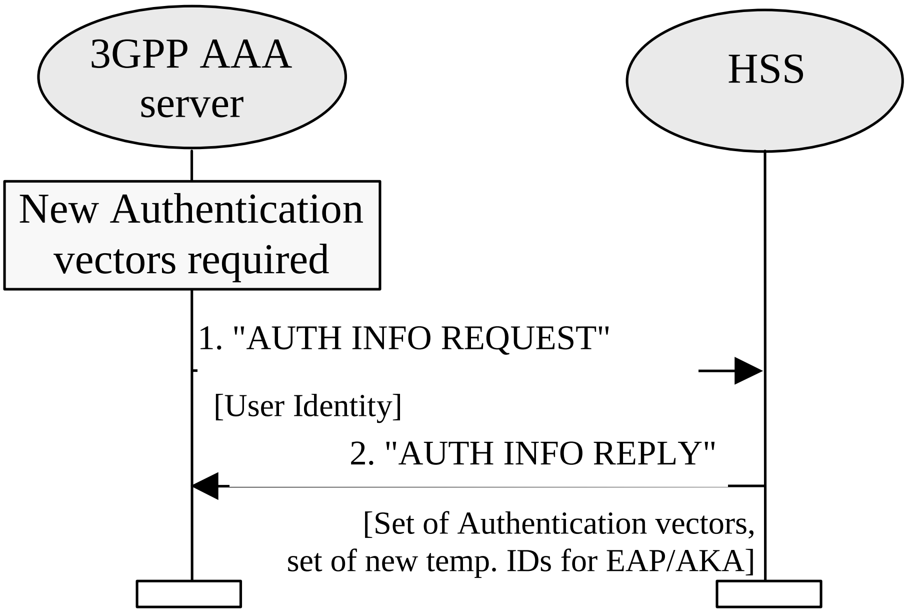

3GPP AAA server
HSS
New Authentication vectors required
1. "AUTH INFO REQUEST"
[User Identity]
2. "AUTH INFO REPLY"
[Set of Authentication vectors,
set of new temp. IDs for EAP/AKA]

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.

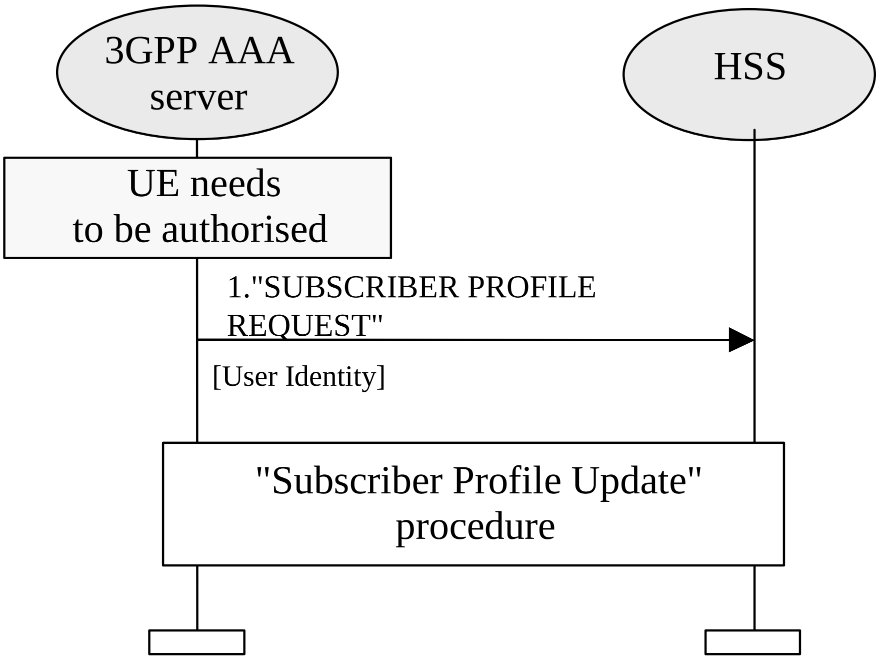

3GPP AAA server
HSS
UE needs to be authorised
1."SUBSCRIBER PROFILE REQUEST"
[User Identity]
"Subscriber Profile Update" procedure

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 clause.

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.

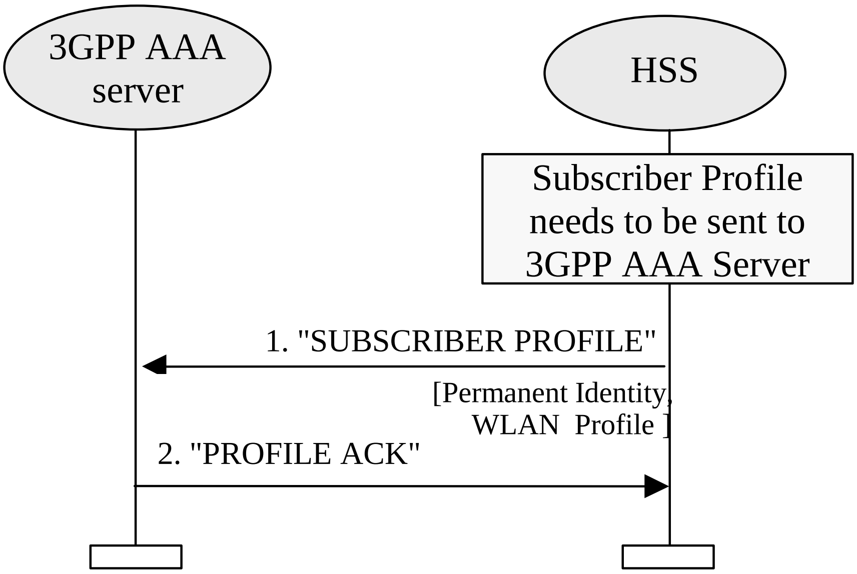

3GPP AAA server
HSS
Subscriber Profile needs to be sent to 3GPP AAA Server
1. "SUBSCRIBER PROFILE"
[Permanent Identity, WLAN Profile]
2. "PROFILE ACK"

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.

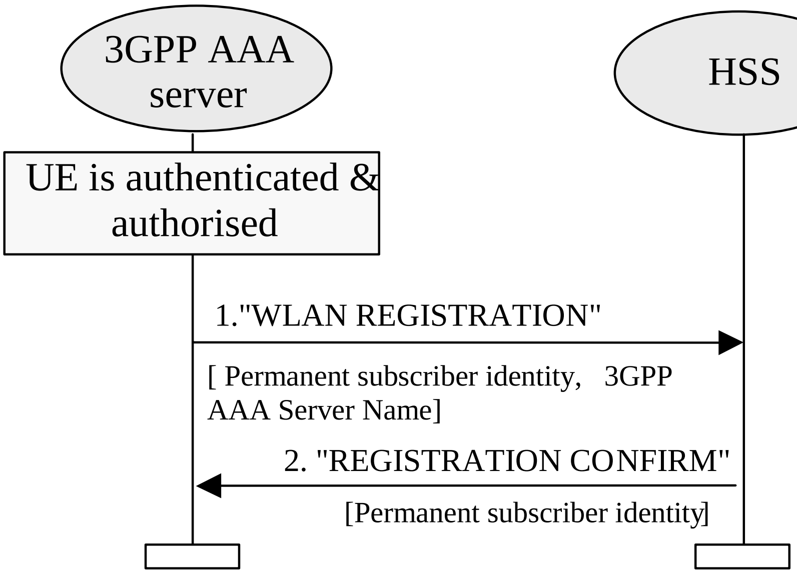

3GPP AAA server
HSS
UE is authenticated & authorised
1."WLAN REGISTRATION"
[Permanent subscriber identity, 3GPP AAA Server Name]
2. "REGISTRATION CONFIRM"
[Permanent subscriber identity]

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 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.

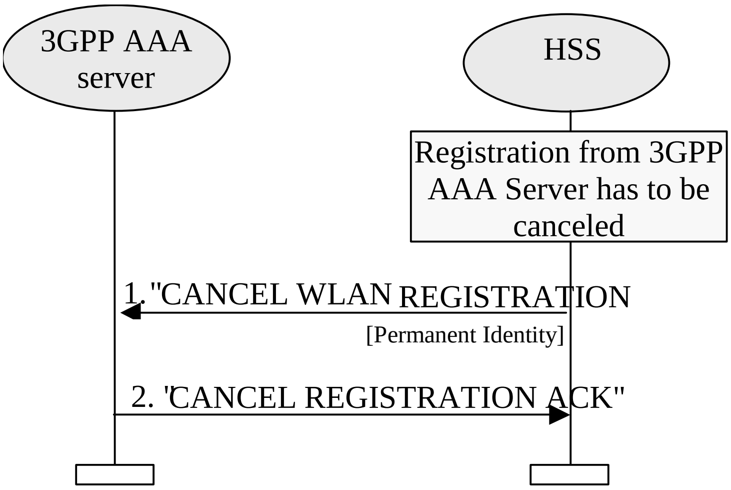

3GPP AAA server
HSS
Registration from 3GPP AAA Server has to be canceled
1. "CANCEL WLAN REGISTRATION
[Permanent Identity]
2. "CANCEL REGISTRATION ACK"

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 cancelled 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 interworking

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 interworking 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.

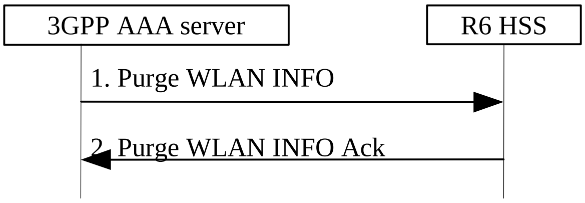


Figure A.2.6 Signalling example on Wx Reference Point for Purge Procedure

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

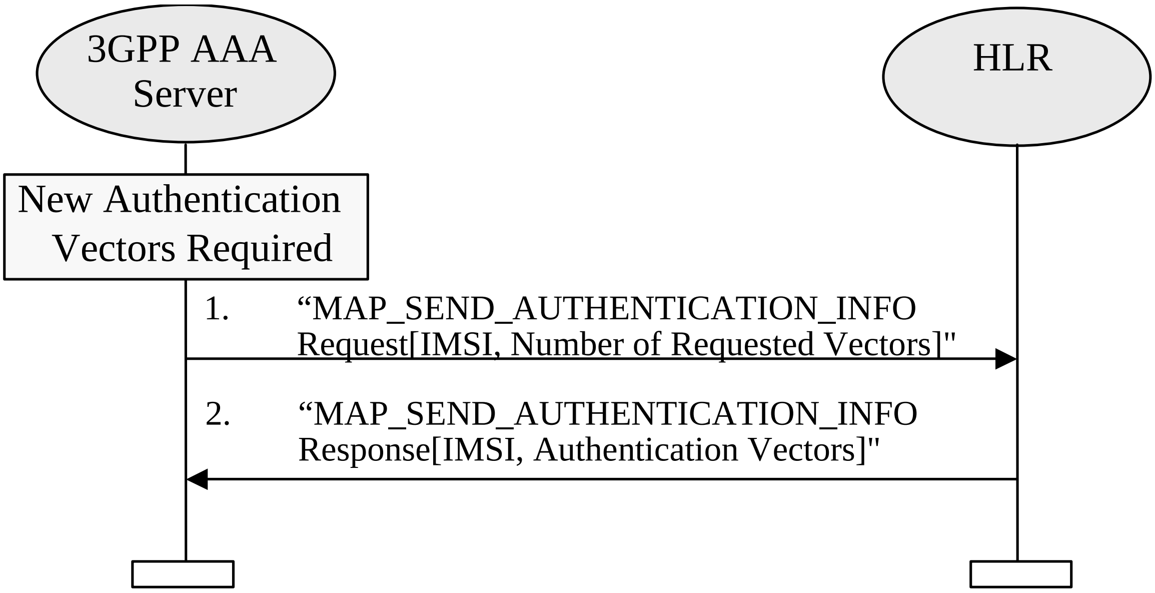

3GPP AAA Server
HLR
New Authentication Vectors Required
1. “MAP_SEND_AUTHENTICATION_INFO Request[IMSI, Number of Requested Vectors]"
2. “MAP_SEND_AUTHENTICATION_INFO Response[IMSI, Authentication Vectors]"

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

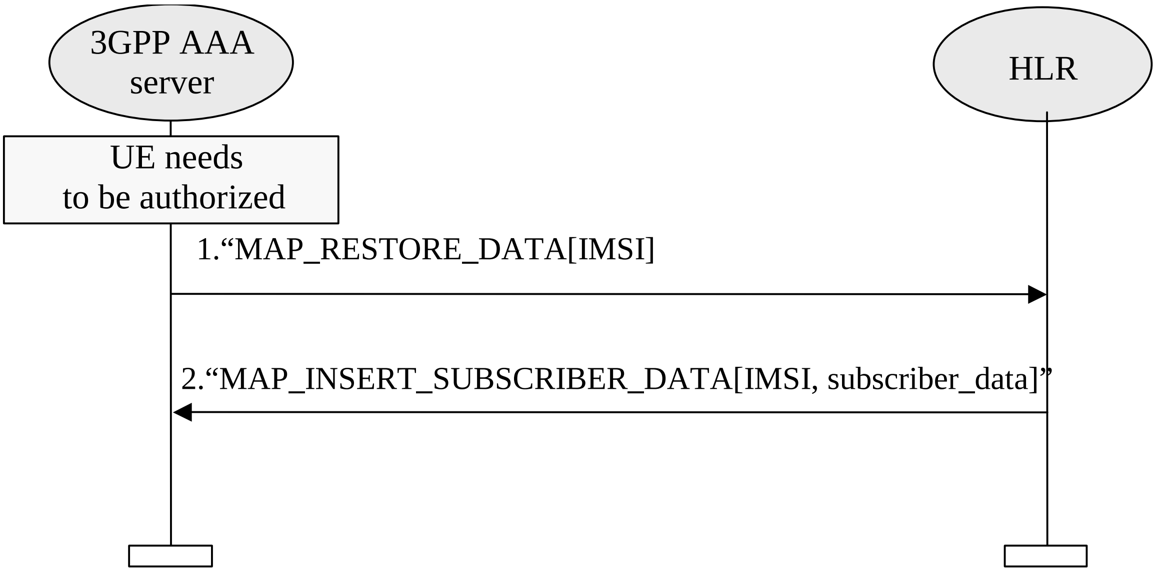

3GPP AAA server
HLR
UE needs to be authorized
1.“MAP_RESTORE_DATA[IMSI]
2.“MAP_INSERT_SUBSCRIBER_DATA[IMSI, subscriber_data]”

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 signalling 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’ signalling 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.

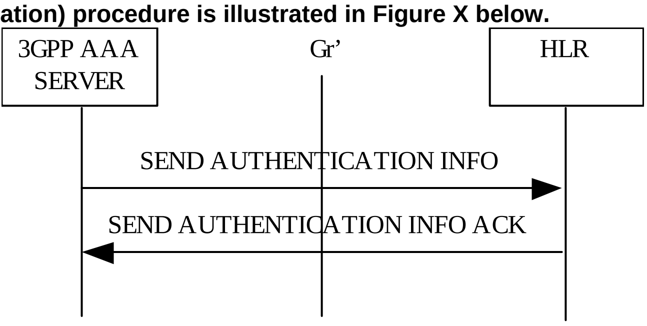


Figure X. infoRetrieval procedure

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.

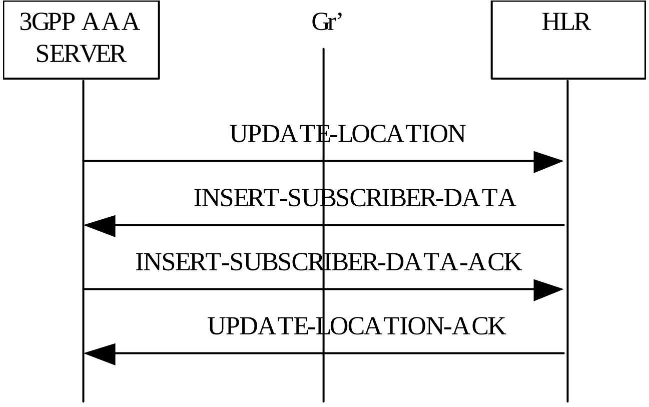


Figure X.1. gprsLocationUpdate procedure

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:

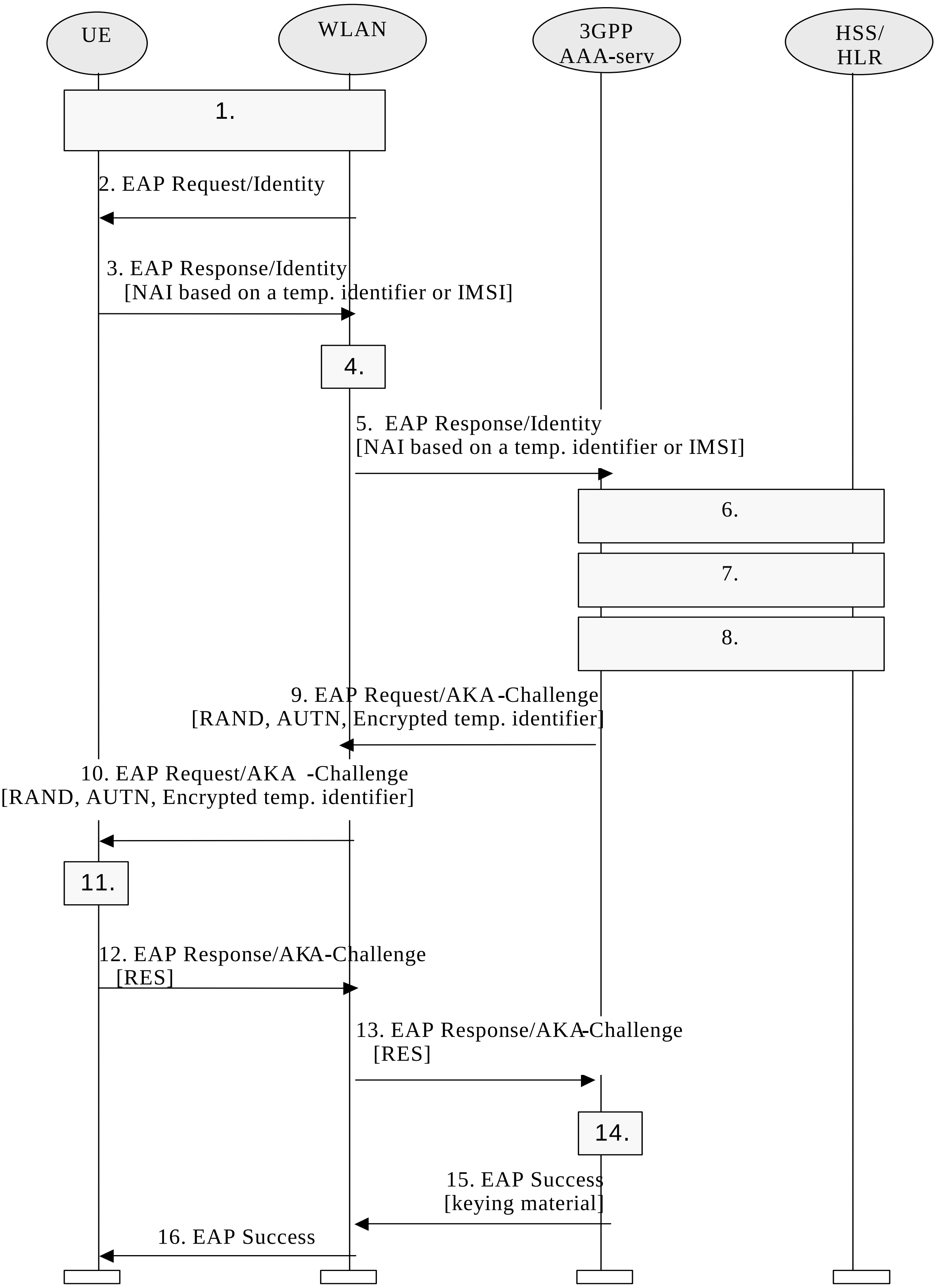

UE
WLAN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity [NAI based on a temp. identifier or IMSI]
4.
5. EAP Response/Identity [NAI based on a temp. identifier or IMSI]
6.
7.
8.
9. EAP Request/AKA-Challenge [RAND, AUTN, Encrypted temp. identifier]
10. EAP Request/AKA -Challenge [RAND, AUTN, Encrypted temp. identifier]
11.
12. EAP Response/AKA-Challenge [RES]
13. EAP Response/AKA-Challenge [RES]
14.
15. EAP Success [keying material]
16. EAP Success

Figure A.4.1 Authentication based on EAP AKA scheme

1. After WLAN connection establishment, Extensible Authentication Protocol is started with a WLAN 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 WLAN interface encapsulated within a WLAN 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 1 : 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 2 : 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 3: 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 4: 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:

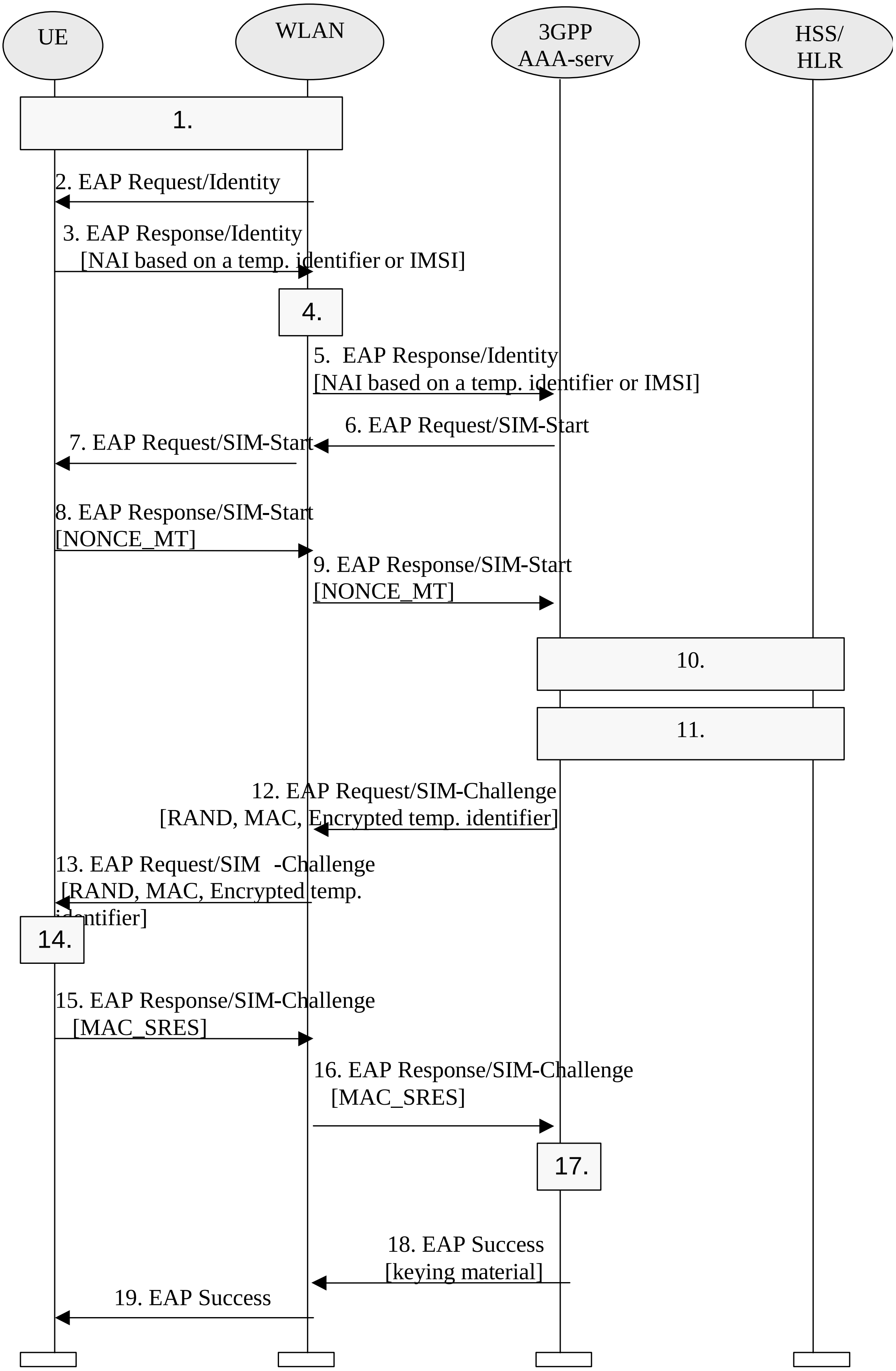

UE
WLAN
3GPP AAA-serv
HSS/ HLR
1.
2. EAP Request/Identity
3. EAP Response/Identity [NAI based on a temp. identifier or IMSI]
4.
5. EAP Response/Identity [NAI based on a temp. identifier or IMSI]
6. EAP Request/SIM-Start
7. EAP Request/SIM-Start
8. EAP Response/SIM-Start [NONCE_MT]
9. EAP Response/SIM-Start [NONCE_MT]
10.
11.
12. EAP Request/SIM-Challenge [RAND, MAC, Encrypted temp. identifier]
13. EAP Request/SIM -Challenge [RAND, MAC, Encrypted temp. identifier]
14.
15. EAP Response/SIM-Challenge [MAC_SRES]
16. EAP Response/SIM-Challenge [MAC_SRES]
17.
18. EAP Success [keying material]
19. EAP Success

Figure A.4.2 Authentication based on EAP SIM scheme

1. After WLAN connection establishment, Extensible Authentication Protocol is started with a WLAN 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 WLAN interface encapsulated within a WLAN 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 1 : 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 2 : 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 3: 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 4: 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 5: 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.

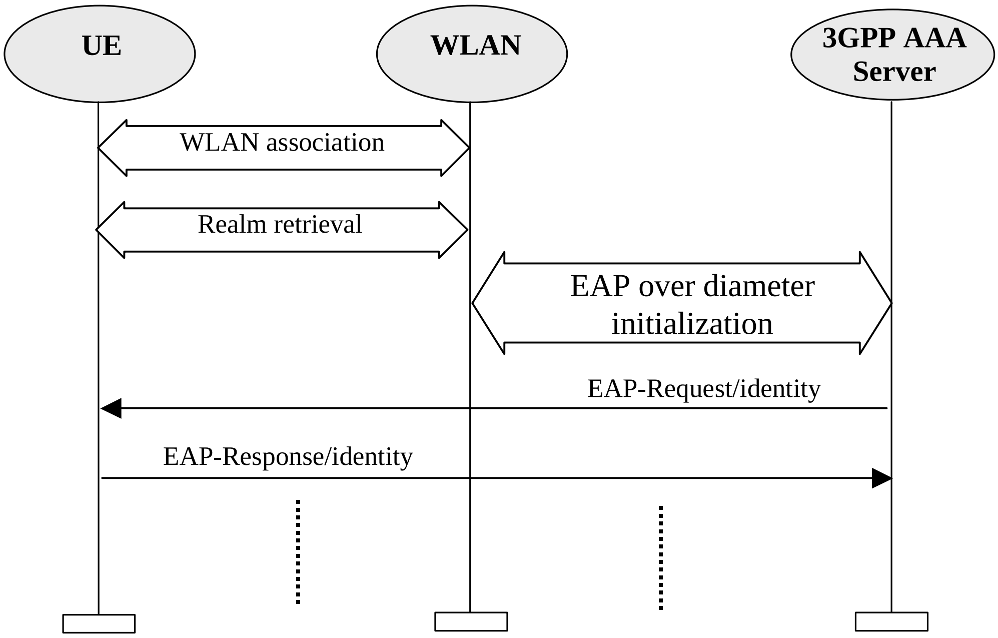


Figure A.4.3 End-to-end EAP initialisation session

A.5.4 Re-authentication message sequence chart

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

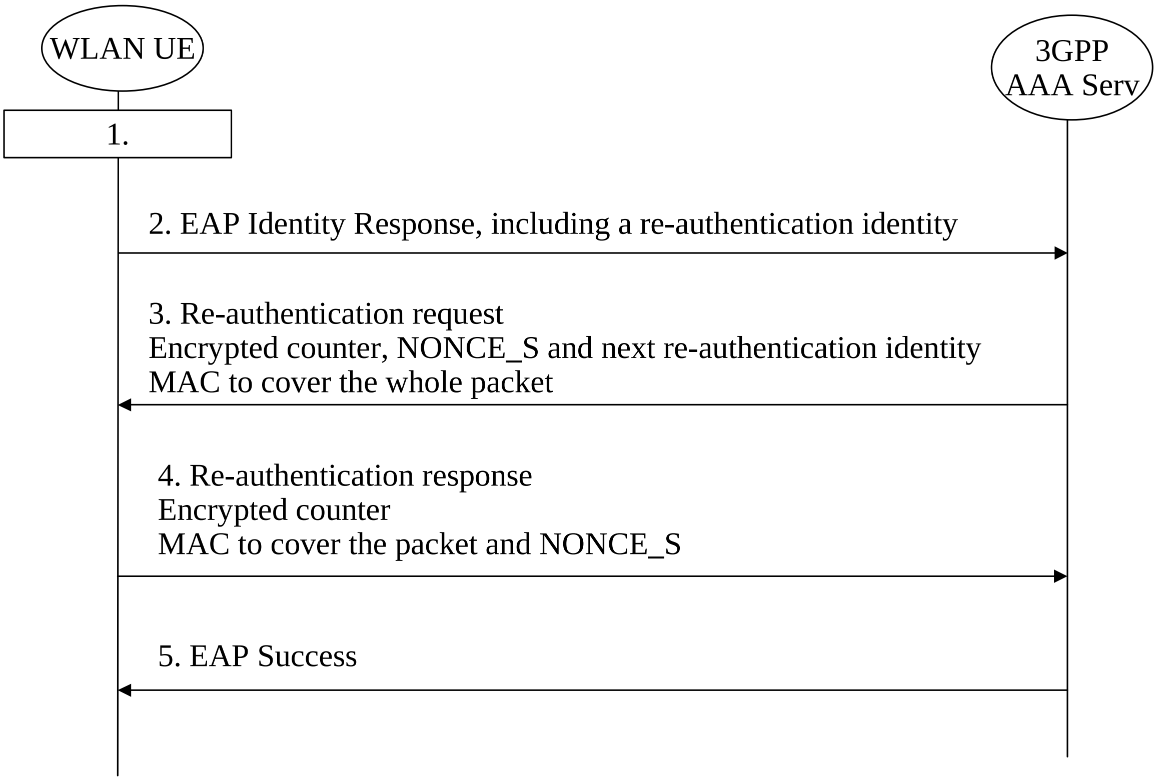

WLAN UE
3GPP AAA Serv
1.
2. EAP Identity Response, including a re-authentication identity
3. Re-authentication request
Encrypted counter, NONCE_S and next re-authentication identity
MAC to cover the whole packet
4. Re-authentication response
Encrypted counter
MAC to cover the packet and NONCE_S
5. EAP Success

Figure A.4.4 Re-authentication signalling sequence

1. Either the UE or the WLAN initiates the authentication procedure with WLAN 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 tariffing. 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.

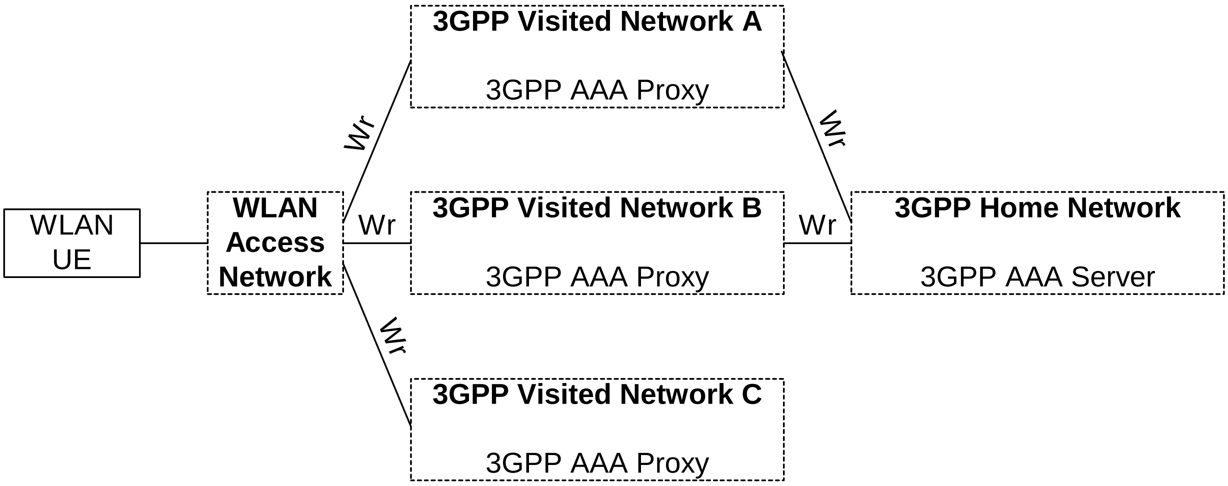


Figure C.1: AAA Routing with Hierarchical Roaming

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].

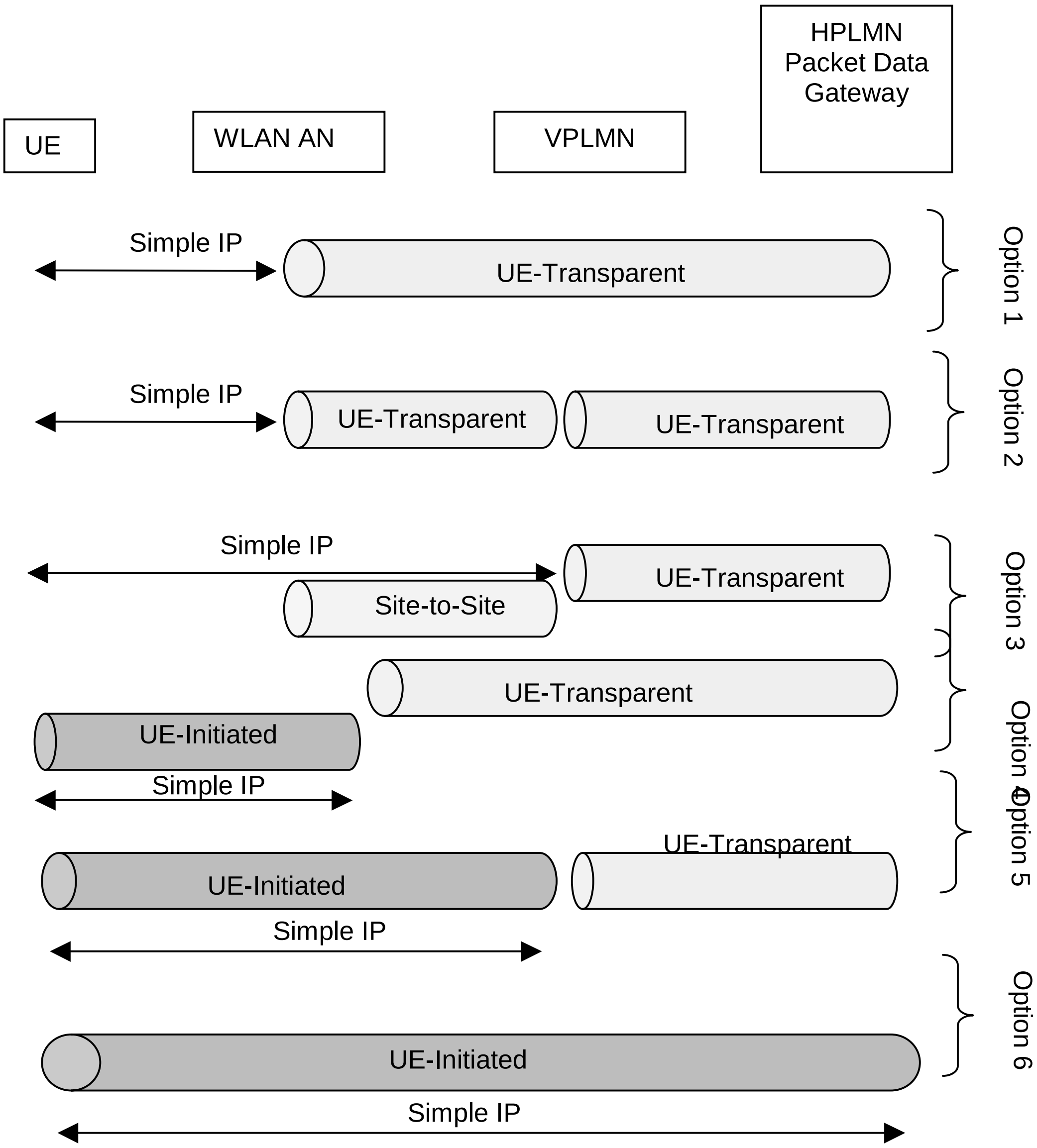
The ability of a WLAN UE to influence the routing of AAA requests, e.g., by using a specific realm part of the NAI, is FFS.

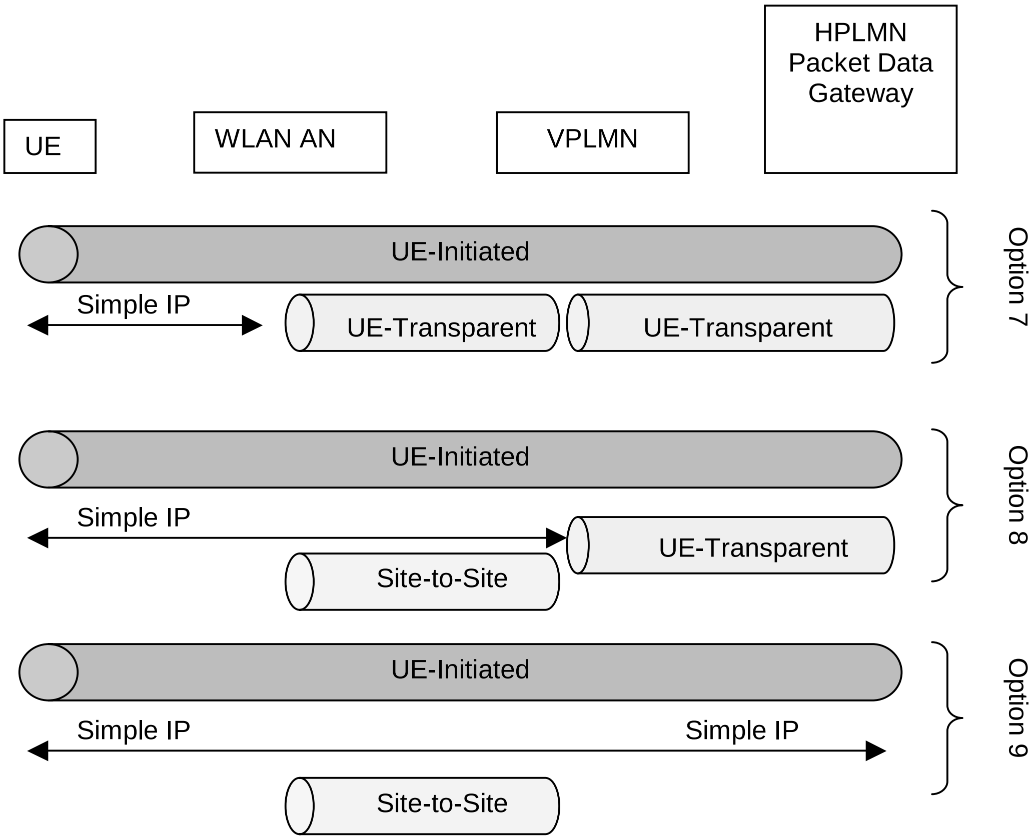
Annex D (informative): WLAN Tunnelling Options

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


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



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

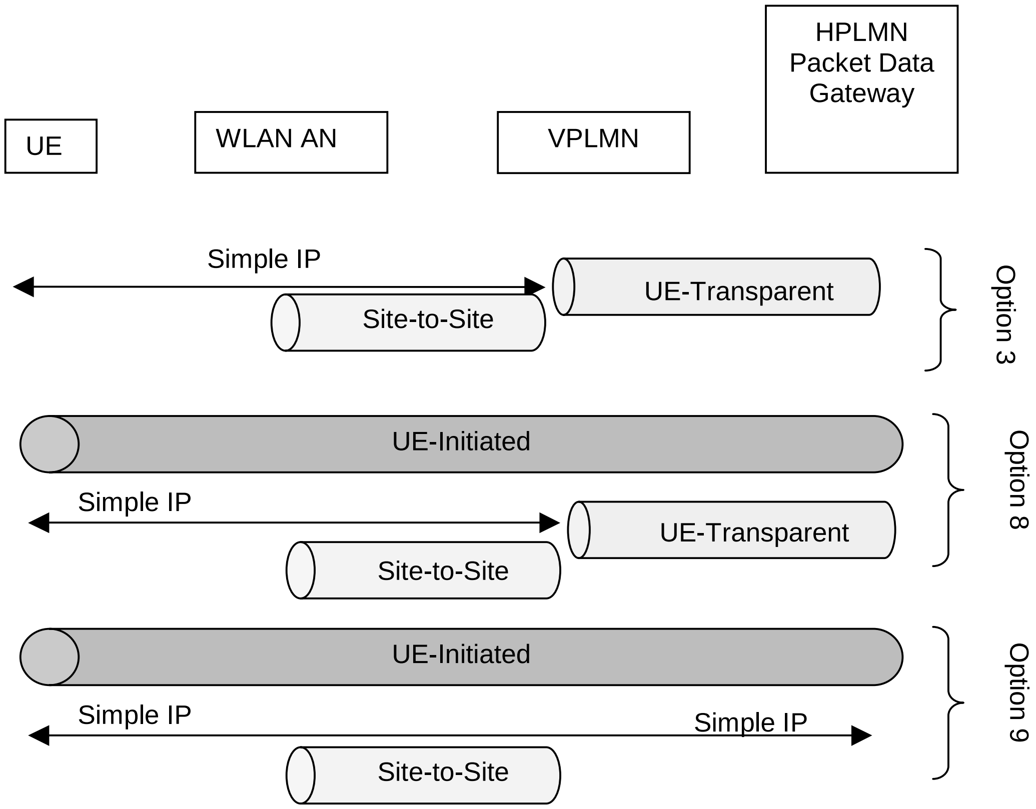
Option 9: UE tunnelling client required

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.

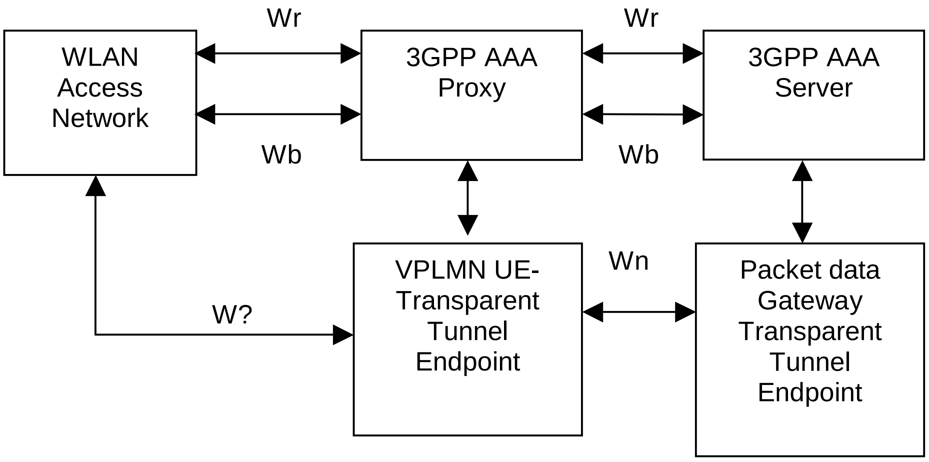
Tunnel Types to be discussed further:



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.


Wr
Wr
WLAN Access Network
3GPP AAA Proxy
3GPP AAA Server
Wb
Wb
Wn
VPLMN UE-Transparent Tunnel Endpoint
Packet data Gateway Transparent Tunnel Endpoint
W?

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.

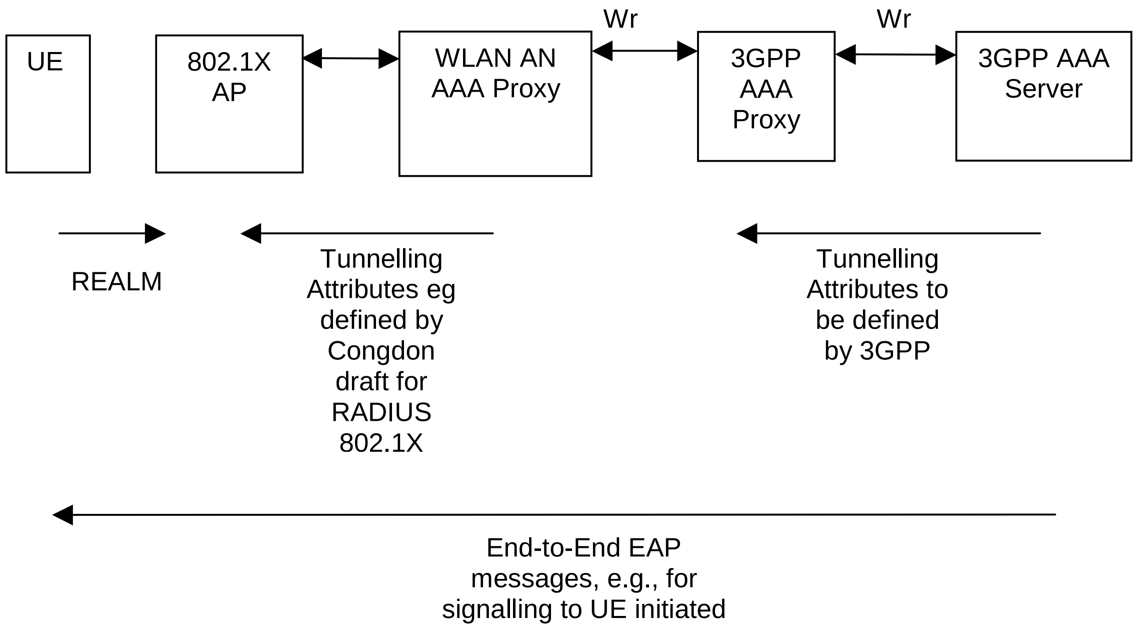
In Option 9, no compulsory tunnel is built but the VPLMN is still able to build per user state.

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.


Wr
Wr
UE
802.1X AP
WLAN AN AAA Proxy
3GPP AAA Proxy
3GPP AAA Server
REALM
Tunnelling Attributes eg defined by Congdon draft for RADIUS 802.1X
Tunnelling Attributes to be defined by 3GPP
End-to-End EAP messages, e.g., for signalling to UE initiated

Summary

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

Option 1, 4, 6.

Annex E (informative): Site to Site Tunnelling

Site-to-Site tunnelling is the tool used by local PLMN (VPLMN in roaming case and HPLMN in non-roaming case) to enforce user traffic to go through its network. Furthermore, Site-to-Site tunnelling moves the user's IP connectivity provisioning from WLAN Access Network to the local PLMN, enforcing data to go via WAG in local PLMN.

The existence of Site-to-Site tunnel between WLAN Access Network and the interworking PLMN is optional, but it has to enable multi-vendor interoperability between WLAN AN and PLMN. It is an aggregate tunnel pre-configured between WLAN Access Network and local PLMN, and not a per-user tunnel.

Site-to-Site tunnelling is an option for scenario 2. It is FFS its usage in Scenario 3.

E.1 UE IP address allocation considerations

When a Site-to-Site tunnel is used between WLAN Access Network and the interworking PLMN, the PLMN is responsible for IP address assignment to UEs accessing services via WLAN. The PLMN keeps track of which addresses have been assigned, and on which particular WLAN Access Network those addresses are being used.

Details of the Site-to-Site tunnel and IP address allocation are subject to operator agreement between the local PLMN and WLAN AN.

Annex F(informative):Additional changes to the reference model, reference points for the different tunnelling solutions

F.1 End-to-End tunnelling solution

This section is a placeholder to develop different sections that covers details of the End-to-End tunnelling solution.

F.1.1 Non Roaming WLAN Inter-working Reference Model

Editor's Note: This section would replace the current section 6.1.1 in case of end to end tunnel solution.

The 3GPP-WLAN Interworking reference model in the non-roaming case is shown in Figure F.1

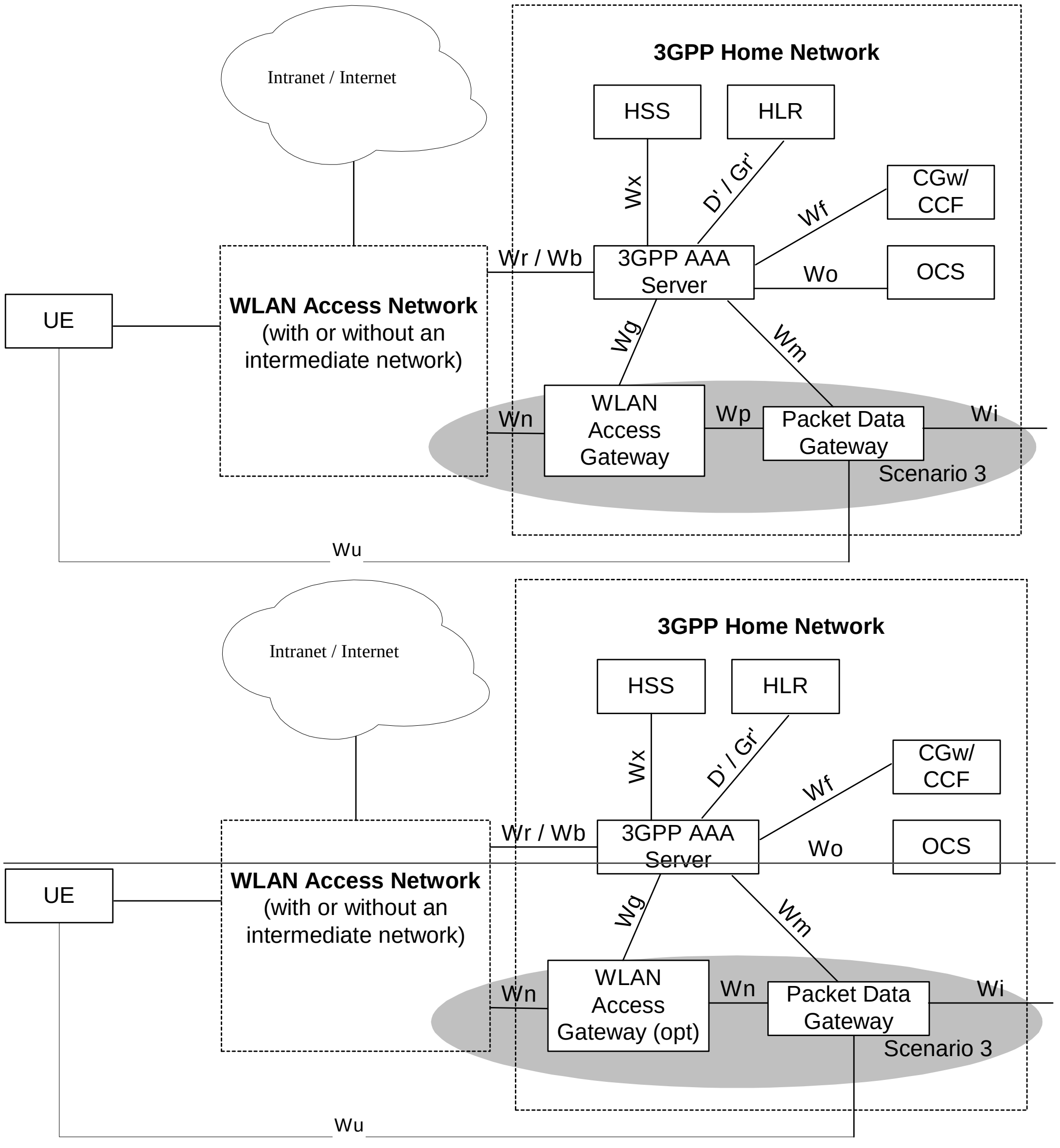


figure F.1 Non Roaming Reference Model.

F.1.2 Roaming WLAN Inter-working Reference Model

Editor's Note: The content of this section would be added to the current section 6.1.2 in case of end to end tunnel solution.

Figure F.2 shows the 3GPP-WLAN interworking reference model in the roaming case.

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 AAA Proxy relays access control signalling and accounting information to the Home 3GPP AAA Server.

It can also issue charging records to the Visited Network's CGw/CCF when required.

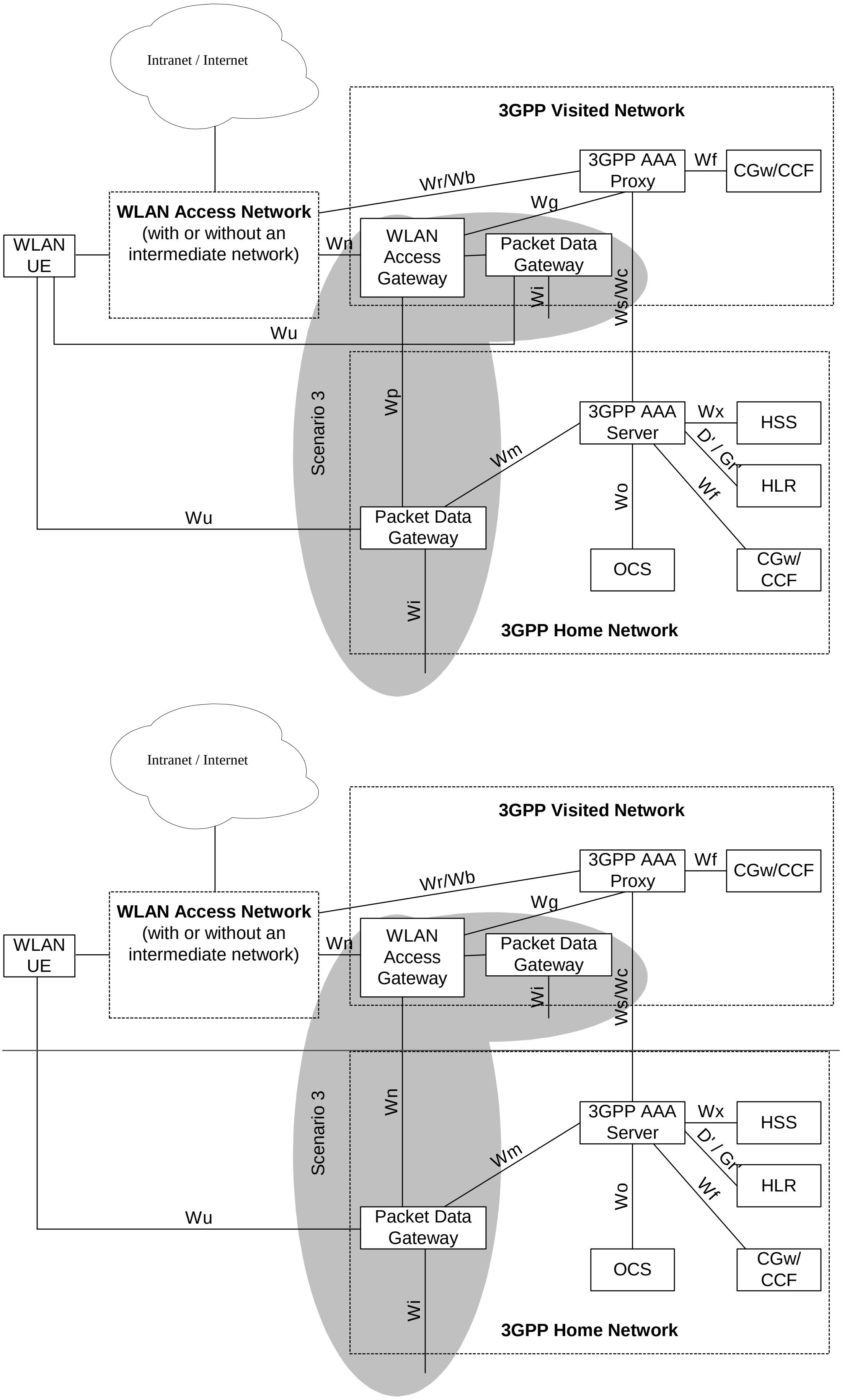


Figure F.2 Roaming Reference Model.

F.1.3 Wu Reference Point

Editor's Note: This section would become section 6.3.x in case of end to end tunnelling.

The Wu reference point is located between the UE and the Packet Data Gateway. It represents the UE-initiated tunnel between the UE and the Packet Data Gateway. Transport for the Wu reference point protocol is provided by the Wn and Wp reference points, which ensures that the data are routed via the WLAN Access Gateway where routing policy enforcement is applied.

The functionality of the Wu reference point is to enable:

- **UE-initiated tunnel establishment**
- **User data packet transmission within the UE-initiated tunnel**
- **Tear down of the UE initiated tunnel**

F.2: Tunnel switching solution

This section is a placeholder to develop different sections that covers details of the tunnel switching solution.

F.2.1 Non Roaming WLAN Inter-working Reference Model

Editor's Note: This section would replace the current section 6.1.1 in case of WAG-Terminated tunnel solution.

The 3GPP-WLAN Interworking reference model in the non-roaming case is shown in Figure F.3

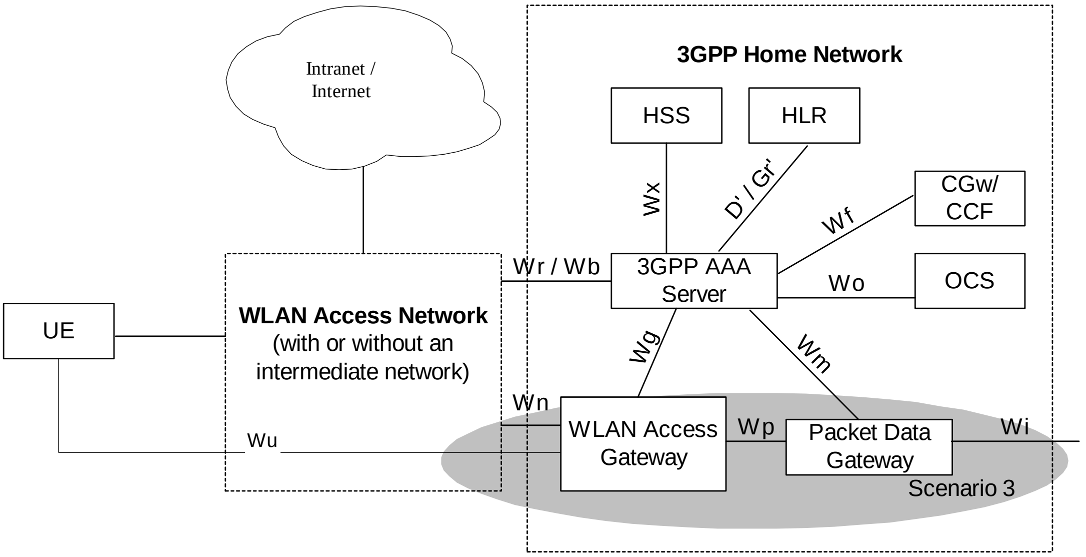


Figure F.3 Non Roaming Reference Model.

F.2.2 Roaming WLAN Inter-working Reference Model

Editor's Note: The content of this section would be added to the current section 6.1.2 in case of WAG Terminated tunnel solution.

Figure F.4 shows the 3GPP-WLAN interworking reference model in the roaming case.

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 AAA Proxy relays access control signalling and accounting information to the Home 3GPP AAA Server.

It can also issue charging records to the Visited Network's CGw/CCF when required.

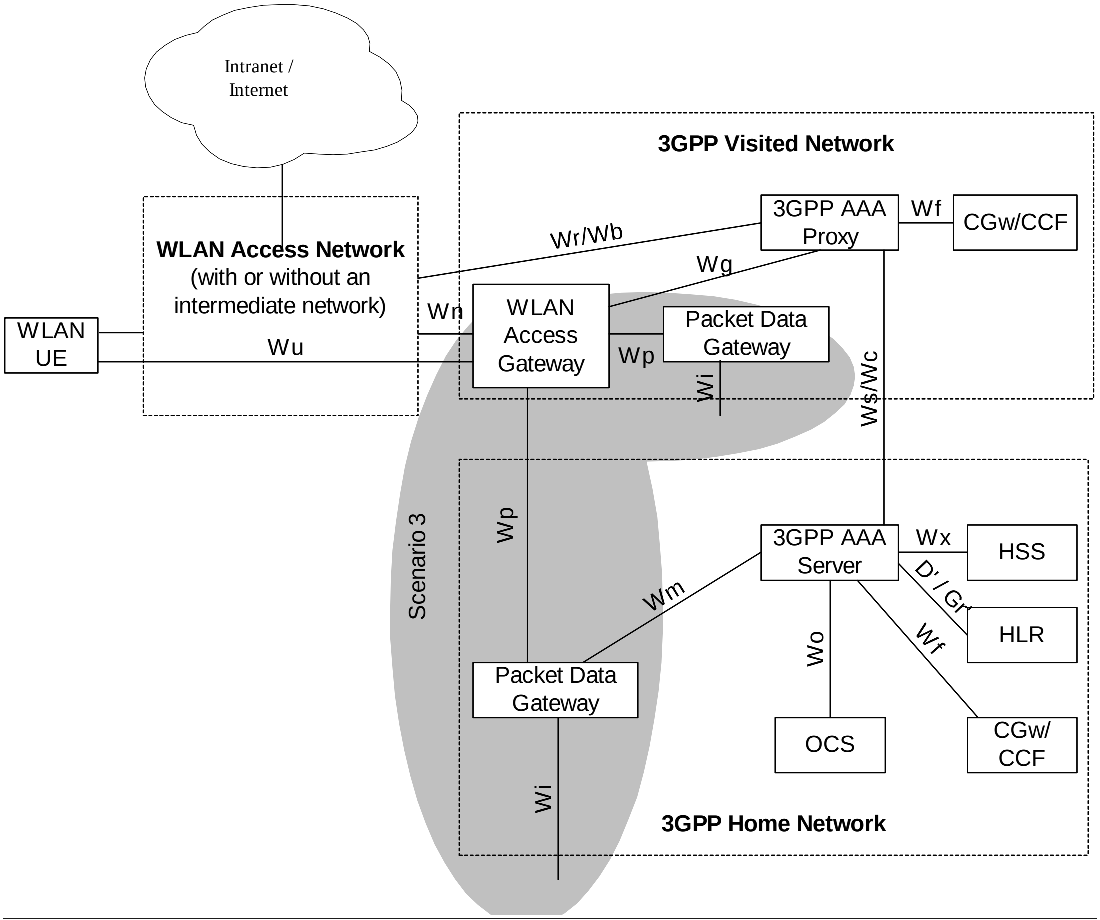


Figure F.4 Roaming Reference Model.

F.2.3 WAG Description

Editor's Note: This section would replace the Scenario 3 parts of section 6.2.5 in the case of WAG Terminated tunnelling.

6.2.5 WLAN Access Gateway

Support of WAG in scenario 3 is mandatory for both roaming and non-roaming cases.

The WAG shall:

- o Support the setup of a secure tunnel initiated by the UE, and cooperate with the PDG to supply required parameters (e.g. DNS address, DHCP address, etc) from the destination network to the UE.
- o Resolve the address of the PDG from the W-APN information supplied by the UE and verified with the 3G AAA Server.
- o Set up a tunnel to the appropriate PDG(s).
- o Route packets between the UE initiated tunnel and the tunnel to the PDG.
- o Serve as a firewall for the network connecting the WAG and PDG, allowing only trusted packets into the 3G network.
- o Update user status information in the 3G AAA Server.
- o Generate accounting information, especially when located in the VPLMN.

F.2.4 Wu Reference Point

Editor's Note: This section would become section 6.3.x in case of WAG Terminated tunnelling.

The reference point Wu is located between the UE and the WAG. The purpose of this reference point is to transport tunnelled user data traffic securely between the UE and the 3GPP network to provide PS-based services to the UE. In roaming cases, the Wu reference point is terminated between the UE and the WAG in the VPLMN. The WLAN may apply a routing enforcement policy, if necessary, to ensure packets are routed only to the WAG.

This reference point is not required to be used when no 3G PS-based Services are provided and a direct connection to external IP network (Internet/Intranet) exists in which case the user data can be directly routed from the WLAN access network without passing 3GPP network, as it is the case with scenario 2.

No specific tunnelling protocol is specified for the Wu reference point, but the current working assumption is that the UE will be able to use an existing VPN client.

F.2.5 Wn Reference Point

Editor's Note: This section would become section 6.3.8 in case of WAG Terminated tunnelling.

6.3.8 Wn

Reference point Wn is located between the WAG and the PDG in the HPLMN. This reference point serves the purpose of transporting tunnelled WLAN user data between WAG and the PDG. The tunnel may not need to be encrypted if the transport network (e.g. GRX) is trusted. Since the network entities connected by Wn serves a similar purpose as the connecting network entities of the Gn interface in GPRS; the GTP protocol would be considered as a candidate for the Wn reference point.

F.2.6 Wp Reference Point

Editor's Note: This section would become section 6.3.y in case of WAG Terminated tunnelling.

6.3.y Wp

Reference point Wp is located between the WAG in the VPLMN and the PDG in the HPLMN. This reference point caters for the roaming WLAN traffic by transporting tunnelled WLAN user data between WAG in the VPLMN and the PDG in the HPLMN. Since the network entities connected by Wp serves a similar purpose as the connecting network entities of the Gp interface in GPRS; the GTP protocol would be considered as a candidate for the Wp reference point.

Annex G (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
2002-10	SA2#27	S2-022989			Modifications/enhancements for scenarios 2 and 3	1.0.0	1.1.0
2002-11	SA2#28	S2-023517			Modifications/enhancements for scenarios 2 and 3	1.1.0	1.2.1
2003-01	SA2#29	S2-030295			Modifications/enhancements for scenarios 2 and 3	1.2.1	1.4.0
2003-02	SA2#30	S2-030727			Split between scenarios 2 and 3	1.4.0	1.6.0
2003-04	SA2#31	S2-031514			Modifications for scenarios 2 and 3	1.6.0	1.7.0
2003-04					Modifications/enhancements for scenarios 2 and 3	1.7.0	1.8.0
2003-05	SA2#32				Modifications/enhancements for scenarios 2 and 3; sent for information to SA#20; scenario 2 now considered as stable; authentication definitely moved to SA3.	1.8.0	1.10.0