

Presentation of Specification to TSG or WG

Presentation to: TSG SA Meeting #21

Document for presentation: TS 23.234, Version 2.0.0

Presented for: Approval

Abstract of document:

This paper presents the Stage 2 WLAN specification 3GPP TS 23.234. The 3GPP WLAN subsystem provides bearer services for connecting a 3GPP subscriber via WLAN to IP based services compatible with those offered via PS domain.

This document is sent to SA for Approval.

Changes since last presentation to TSG-SA Meeting #20:

- 1) End-to-End tunnelling has been selected as the architectural solution for scenario 3.
 - 2) Progress on Network Selection.
 - 3) General editorial cleanup.
-

Outstanding Issues:

The remaining issue for scenario 2 is:

- 1) WLAN access network selection and PLMN Selection algorithm in the UE.

The remaining issues for scenario 3 are:

- 1) W-APN Resolution
 - 2) Functional description of per user charging in a Visited Network.
 - 3) Routing policy enforcement.
 - 4) Interworking with 3GPP PS-based services. Most of the aspects associated with IP connectivity are complete. Some issues remain with services such as Service Based Local Policy interaction and SMS.
 - 5) Procedures such as end-to-end message flows.
-

Information for SA

With respect to scenario 3, one of the key discussion points has been if the tunnel which connects the UE in the WLAN network to the 3G network terminates in the Packet Data Gateway (PDG) or in the Wireless Access Gateway (WAG). This resulted in two of the following options being identified for the stage 2 WLAN TS.

Option 1

End-to-End (UE-to-PDG) Tunnelling: This approach is based on existing VPN-like tunnel set up procedures between the UE and the PDG.

Option 2

Tunnel Switching: This approach is based on VPN-like tunnel set up between the UE and the WAG. The WAG then sets up another tunnel using GPRS concepts towards the PDG for user data transfer.

Summary:

An extensive deliberation and enough consideration of both options were performed, but there was no unanimous support for either of the options, as both options are valid and have their merits. SA2 has thus decided to select the end-to-end tunnelling option that had majority support. This approach was taken, as it was felt that further deliberation of the issue would not bring a unanimous resolution within the required timeframe.

3GPP TS 23.234 V2.0.0 (2003-09)

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)**



The present document has been developed within the 3rd Generation Partnership Project (3GPP™) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification. Specifications and reports for implementation of the 3GPP™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

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>

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2002, 3GPP Organizational Partners (ARIB, CWTS, ETSI, T1, TTA, TTC).
All rights reserved.

Contents

Foreword.....	6
Introduction.....	6
1 Scope.....	7
2 References.....	7
3 Definitions, symbols and abbreviations.....	8
3.1 Definitions.....	8
3.2 Symbols.....	9
3.3 Abbreviations.....	9
4 WLAN Radio networks interworking with 3GPP.....	9
5 High-level Requirements and Principles.....	10
5.1 Access Control Requirements.....	10
5.2 Access Control Principles.....	11
5.3 User Identity.....	13
5.3.1 General.....	13
5.3.2 NAI Username.....	13
5.3.3 NAI Realm Name.....	13
5.3.4 Roaming NAI.....	14
5.4 Network Advertisement and Selection.....	14
5.4.1 Description of the issue.....	14
5.4.2 WLAN Access Network Selection.....	15
5.4.2.1 Case of IEEE 802.11 WLANs.....	15
5.4.2.2 Case of other WLANs.....	16
5.4.3 VPLMN Advertisement and Selection.....	16
5.4.3.1 Network Advertisement.....	16
5.4.3.2 Network Selection.....	16
5.5 Authentication methods.....	16
5.6 Service Authorization Principles for scenario 3.....	17
5.6.1 Accessing Home Network provided services.....	17
5.6.2 Accessing Visited Network provided services.....	17
5.6.3 External IP Network selection.....	18
5.7 IP Connectivity for scenario 3.....	18
5.7.1 Principles.....	18
5.7.2 Tunnelling Requirements.....	18
5.8 Roaming requirements for scenario 3.....	19
5.9 Scenario 3 Routing Enforcement.....	19
5.9.1 Purpose for routing enforcement.....	19
5.9.2 Routing Enforcement in the WLAN AN.....	19
5.9.3 Policy Enforcement in the HPLMN.....	20
5.9.4 Policy Enforcement in the VPLMN.....	20
5.10 IP address allocation for the WLAN UE.....	20
5.11 Charging.....	20
6 Interworking Architecture.....	21
6.1 Reference Model.....	21
6.1.1 Non Roaming WLAN Inter-working Reference Model.....	21
6.1.2 Roaming WLAN Inter-working Reference Model.....	21
6.2 Network elements.....	23
6.2.1 WLAN UE.....	23
6.2.2 3GPP AAA Proxy.....	23
6.2.3 3GPP AAA Server.....	24
6.2.4 HLR/HSS.....	24
6.2.5 WLAN Access Gateway.....	24
6.2.5.1 Routing Enforcement.....	25
6.2.5.2 Per-user Charging Generation.....	25

6.2.5.3	Summary.....	25
6.2.6	Packet Data Gateway.....	26
6.3	Reference Points.....	27
6.3.1	W _r reference point.....	27
6.3.1.1	General description.....	27
6.3.1.2	Functionality.....	27
6.3.1.3	Protocols.....	27
6.3.2	W _x reference point.....	28
6.3.3	D'/Gr' reference point.....	28
6.3.4	W _b reference point.....	28
6.3.5	W _o reference point.....	29
6.3.6	W _f reference point.....	29
6.3.7	W _g reference point.....	29
6.3.8	W _n reference point.....	29
6.3.9	W _p reference point.....	30
6.3.10	W _i reference point.....	30
6.3.11	W _m reference point.....	30
6.3.12	W _s reference point.....	30
6.3.12.1	General description.....	30
6.3.12.2	Functionality.....	30
6.3.12.3	Protocols.....	30
6.3.13	W _c reference point.....	31
6.3.14	W _u reference point.....	31
7	Procedures.....	32
7.1	WLAN Access Authentication and Authorisation.....	33
7.2	Subscriber Profile Update.....	34
7.3	Cancelling WLAN Registration.....	35
7.4	Disconnecting a Subscriber by WLAN.....	35
7.5	Disconnecting a Subscriber by Online Charging System.....	36
7.6	Charging offline charged subscribers.....	37
7.7	Charging online charged subscribers.....	38
7.8	Tunnel establishment.....	39
Annex A (informative): Reference Points Signalling Flows.....		41
A.1	Signalling Sequences examples for W _r Reference Point.....	41
A.1.1	Authentication, Authorisation and Session Key delivery.....	41
A.1.2	Immediate purging of a user from the WLAN access.....	43
A.2	Signalling Sequences examples for W _x Reference Point.....	44
A.2.1	Authentication Information Retrieval.....	44
A.2.2	Subscriber Profile Retrieval.....	45
A.2.3	Subscriber Profile Update.....	46
A.2.4	WLAN Registration.....	47
A.2.5	Cancel Registration.....	47
A.2.6	Purge Function for WLAN interworking.....	48
A.3	Signalling Sequences examples for D' Reference Point.....	49
A.3.1	Authentication Information Retrieval.....	49
A.3.2	Subscriber Profile Retrieval.....	50
A.4	Gr' Signalling Mechanisms to support WLAN service.....	50
A.4.1	Introduction.....	50
A.4.2	InfoRetrieval procedure:.....	51
A.4.2	GprsLocationUpdate procedure:.....	51
A.5	Example of Authentication procedures.....	52
A.5.1	EAP/AKA Procedure.....	52
A.5.2	EAP SIM procedure.....	55
A.5.3	Alternative EAP initialisation.....	58
A.5.4	Re-authentication message sequence chart.....	59

Annex B (informative): WLAN Radio Technologies	60
Annex C (informative): Site to Site Tunnelling	62
C.1 WLAN UE IP address allocation considerations.....	62
Annex D (informative): Information on the discussed tunnel switching alternative	63
D.1 Non Roaming WLAN Inter-working Reference Model.....	63
D.2 Roaming WLAN Inter-working Reference Model	63
D.3 WAG Description.....	64
D.4 Wu Reference Point.....	65
D.5 Wn Reference Point.....	65
D.6 Wp Reference Point.....	65
Annex E (informative): W-APN resolution comparison.....	65
E.1 Solutions considered.....	65
E.1.1 UE DNS Client	66
E.1.2 WAG DNS Client.....	66
E.2 Visited Network Services.....	67
E.2.1 Enhancements to UE DNS Client approach.....	68
E.2.2 Enhancements to WAG DNS client approach.....	68
Annex F (informative): Change history	68

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)."
- [11] 3GPP TS 33.234: "WLAN Interworking Security."
- [12] RFC2284: "PPP Extensible Authentication Protocol (EAP)"
- [13] RFC 2486: "The Network Access Identifier"
- [14] IETF Internet-Draft, "Diameter Base Protocol".
<http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-17.txt>
- [15] J. Caron, "DNS Based Roaming", <http://www.ietf.org/internet-drafts/draft-caron-dns-based-roaming-00.txt>, April 2002, (work in progress)
- [16] 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

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.

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

External IP Network/External Packet Data Network: An IP network to which access may be provided through the 3GPP system, rather than directly from the WLAN AN. For example, the Internet, an operator's IP network or a 3rd party IP network such as a corporate IP network.

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.

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.

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.

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

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

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

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

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

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

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.

WLAN UE's local IP address: An address that is necessary to deliver the packet to a WLAN UE in a WLAN AN. It identifies the WLAN UE in the WLAN AN. WLAN UE's local IP address may be translated by Network Address Translation prior to being received by the interworking function.

WLAN UE's remote IP address: An address used in the data packet encapsulated by the WLAN UE-initiated tunnel. It represents the identity of the WLAN UE in the network which the WLAN UE is accessing.

3.2 Symbols

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

D'	Reference point between a pre-R6 HSS/HLR and a 3GPP AAA Server
Gr'	Reference point between a pre-R6 HSS/HLR and a 3GPP AAA Server
Wb	Reference point between a WLAN Access Network and a 3GPP AAA Server/Proxy (charging signalling)
Wc	Interface between a 3GPP AAA Proxy and a 3GPP AAA Server (charging signalling)
Wf	Reference point between a CGw/CCF and a 3GPP AAA Server/Proxy
Wg	Interface between a 3GPP AAA Proxy and WAG
Wi	Reference point between a Packet Data Gateway and an external IP Network
Wm	Reference point between a Packet Data Gateway and a 3GPP AAA Server
Wn	Reference point between a WLAN Access Network and a WLAN Access Gateway
Wp	Reference point between a WLAN Access Gateway and a Packet Data Gateway
Wo	Reference point between a 3GPP AAA Server and an OCS
Wr	Reference point between a WLAN Access Network and a 3GPP AAA Server/Proxy (control signalling)
Ws	Interface between a 3GPP AAA Proxy and a 3GPP AAA Server (control signalling)
Wu	Reference point between a WLAN UE and a Packet Data Gateway
Wx	Reference point between an HSS and a 3GPP AAA Server

3.3 Abbreviations

AP	Access Point
APN	Access Point Name
CCF	Charging Collection Function
CGw	Charging Gateway
OCS	Online Charging System
PDA	Personal Digital Assistant
PDG	Packet Data Gateway
UE	User Equipment
WAG	WLAN Access Gateway
W-APN	WLAN APN
WLAN	Wireless Local Area Network
WLAN AN	WLAN Access Network
WLAN UE	WLAN User Equipment

4 WLAN Radio networks interworking with 3GPP

This specification defines two new procedures in the 3GPP System:

- WLAN Access, Authentication and Authorisation, which provides for access to the WLAN and the locally connected IP network (e.g. Internet) to be authenticated and authorised through the 3GPP System
- Access to External IP networks, which allows WLAN UEs to establish connectivity with an External IP network, such as 3G operator networks, corporate Intranets or the Internet from a suitable IP network.

For scenario 3, access to External IP Networks should, as far as possible, be technically independent of WLAN Access Authentication and Authorisation. However, Access to External IP Networks from 3GPP WLAN interworking systems shall be possible only if WLAN Access Authentication/Authorisation has been completed first.

Note: The independence requirement does not preclude the possibility that the procedure for access to external IP network may rely on information derived in the procedure for WLAN Access Authorization.

Scenario 2 requires the first of these capabilities only. Scenario 3 requires a combination of both.

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 supports access to External IP networks, including those supporting 3GPP PS Domain based services. Scenario 2 offers direct connection from the WLAN to the Internet/intranet. The WLAN includes WLAN access points and intermediate AAA elements. It may additionally include other devices such as routers. The WLAN User Equipment (WLAN UE) includes all equipment that is in possession of the end user, such as a computer, WLAN radio interface adapter etc.

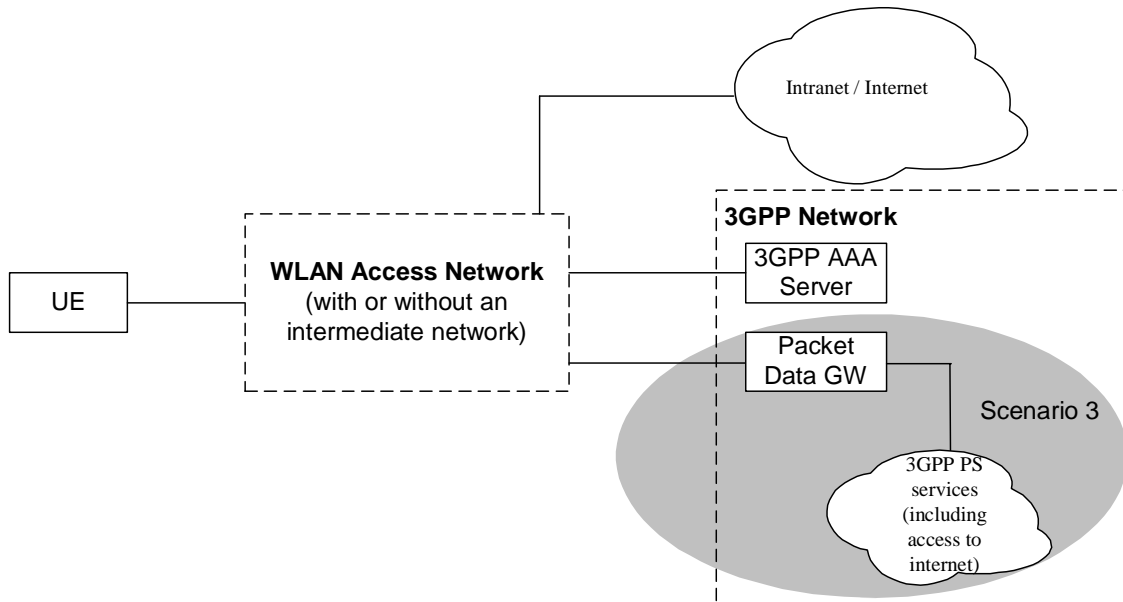


Figure 4.1: Simplified WLAN Network Model. The shaded area refers to scenario 3 functionality

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 assess 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

5.1 Access Control Requirements

The following functional requirements have been identified:

- 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.
- Results of WLAN Access Authorization requests shall be indicated to the WLAN, so that the WLAN can take appropriate action.
- The WLAN Access Authorization 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.
- Service based policy control shall be possible for the services authorized for the user.
- Access to 3GPP PS based services shall be provided via WLAN. The interworking architecture shall be able to support all 3GPP PS based services.
- Access to PS based services normally provided by the 3GPP PS Core Network shall be provided via WLAN. WLAN access to these services shall support the same features as those supported via the 3GPP PS Core Network according to operator choice, e.g. private addressing schemes, external address allocation, secure tunneling to private external network. Quality of Service shall be supported when accessing these services via WLAN, although 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.
- When the WLAN inter-working system does not support access to 3GPP PS based services, the WLAN UE shall be able to detect it.
- 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: This may mandate additional functionality existing in the WLAN AN

- The technical solution for access control to External IP networks from WLAN shall be decoupled from WLAN Access Control.

5.2 Access Control Principles

End to End Authentication: WLAN Authentication signaling is executed between WLAN UE and 3GPP AAA Server for the purpose of authenticating the end-user and 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 AN and 3GPP network: WLAN Authentication signalling shall be transported **between any WLAN AN and 3GPP network** by a standard protocol, which is independent of 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 Authorization: This defines the process(es) in 3GPP AAA Server verifying whether WLAN Access should be allowed to a subscriber and deciding what access rules/policy should be applied to a subscriber. It is the access stage after the access authentication, but before service authorisation and WLAN UE's local IP address allocation.

After the authentication process succeeds, there could be additional conditions for the 3GPP AAA Server to decide whether the access is allowed and what access rules/policy should be applied. These conditions may be based on the subscriber's profile, the account status, O&M rules or local agreements.

The procedure for WLAN Access Authorization between the WLAN UE and the 3GPP AAA Server is combined with the WLAN Access Authentication.

Access rules/policy decided by the 3GPP AAA Server may be deployed in the 3GPP AAA Server, or/and 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 WLAN UE is "WLAN-attached" after successful authentication and WLAN Access Authorization.

A WLAN UE is "WLAN-detached" in 3GPP network after its disconnection, or its authentication or WLAN Access Authorization being cancelled.

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

The WLAN 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 WLAN UE's WLAN-attach status directly from the AAA Server or through the HSS. These entities and the corresponding reference points are not in the scope of this TS.

The description of the corresponding status in the WLAN 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 WLAN 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 subscriber profile retrieved from HSS. The 3GPP AAA Server selects a W-APN based on the requested W-APN and on the user's subscription/local policy.

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

Editor's Note: Whether the request is sent to the WAG or to the PDG is ffs.

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 User Identity

5.3.1 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.

5.3.2 NAI Username

The NAI username part format is specified in IETF EAP-SIM and EAP-AKA specifications. Details of these are covered in Stage 3 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, WLAN UE shall use the previously allocated Reauthentication ID as specified in the IETF EAP-SIM and EAP-AKA specifications as its NAI user identity.

5.3.3 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 WLAN UE shall by default derive the NAI realm from a PLMN_ID as described in the following steps:

1. To retrieve the PLMN ID from the IMSI 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.

5.3.4 Roaming NAI

A roaming NAI is constructed when the WLAN UE authenticates through a VPLMN. The WLAN UE shall indicate in the NAI both the user's HPLMN and the chosen VPLMN, based on their MCC and MNC.

The realm portion of the roaming NAI shall be constructed according to Section 5.3.2 based on the chosen Visited Network MCC and MNC.

The details of the construction of the username part of the roaming NAI are for stage 3.

5.4 Network Advertisement and Selection

5.4.1 Description of the issue

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

In addition to WLAN Access 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.

WLAN Access Network advertisement and selection depends on the particular WLAN technology.

VPLMN advertisement and selection should be independent of WLAN technology.

The generic Network Advertising and Selection scenario is illustrated in Figures 5.1 and 5.2.

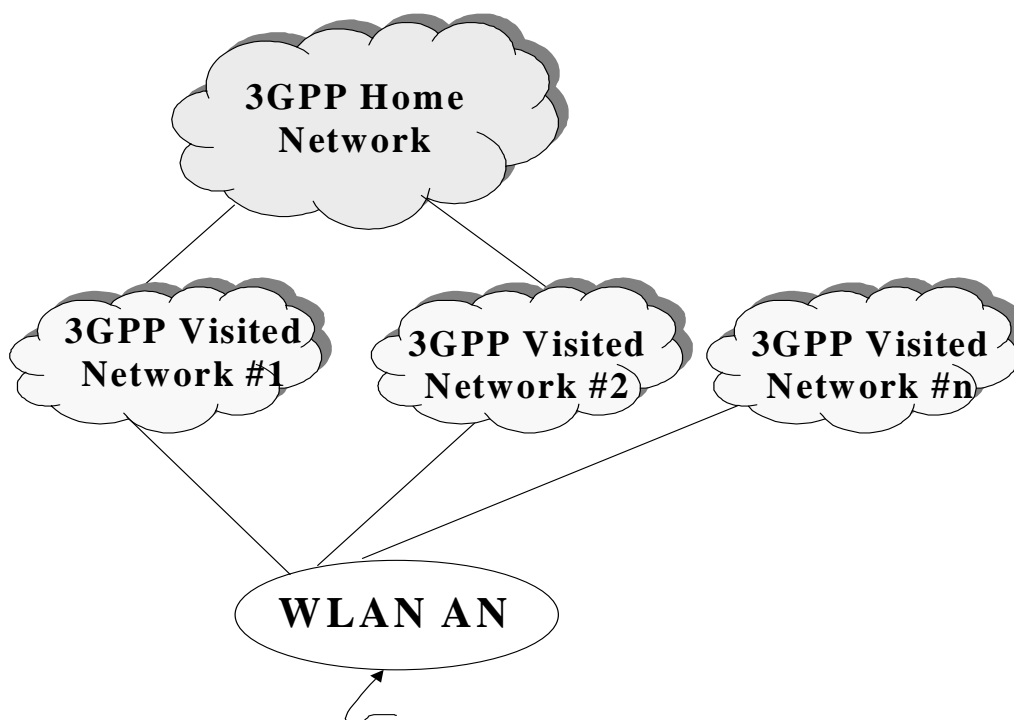


Figure 5.1 Network Advertising and Selection Scenario

An area is shown covered by a WLAN Access Networks having a set of roaming agreements with different 3G networks (3GPP Visited Network #1,#2,...,#n). A WLAN UE entering the WLAN AN wants to connect to his own 3GPP Home Network to which he is a subscriber (as shown in Figure 5.1).

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.

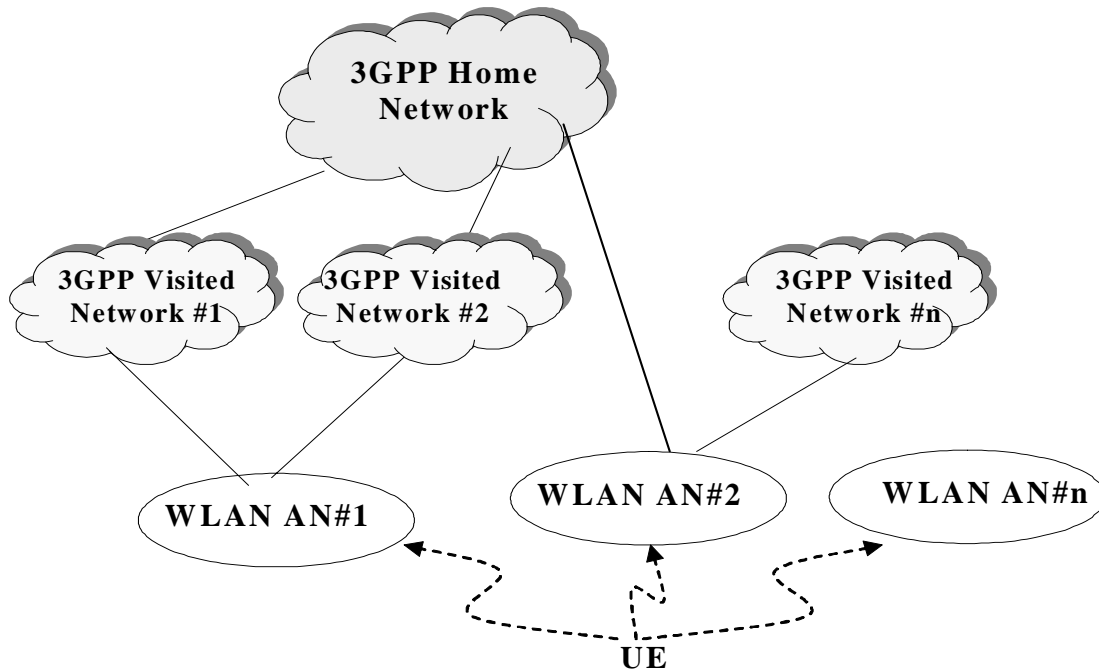


Figure 5.2 – Network Advertising and Selection Scenario

Another scenario is represented by an area covered by some WLAN Access Networks (WLAN AN#1, #2, ..., #n) having a set of roaming agreements with different 3G networks (3GPP Visited Network #1,#2,...,#n) and where one of the WLAN Access Network has a directly roaming agreement with the 3GPP Home network, or the WLAN Access Network is directly deployed by the 3GPP Home network. A UE entering the area wants to connect to his own 3GPP Home Network to which he is a subscriber (as shown in Figure 5.2).

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

5.4.2 WLAN Access Network Selection

5.4.2.1 Case of IEEE 802.11 WLANs

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 WLAN 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 WLAN 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 be able to 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.

5.4.2.2 Case of other WLANs

Other WLANs, such as HiperLAN or Bluetooth, are not described in this TS but not excluded.

5.4.3 VPLMN Advertisement and Selection

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

- The user shall be able to select the Visited Network
- Use the NAI for routing of AAA messages.
- Have low latency and overhead.
- Use existing EAP mechanisms, if possible.
- Be extensible to permit advertisement of WLAN characteristics other than the PLMNIDs of roaming partners.

5.4.3.1 Network Advertisement

Network advertisement information shall be provided which enumerates the roaming partners and associated NAI realms. A single mechanism shall be used to provide that information. This information shall be provided to the WLAN UE when the WLAN has no direct roaming relationship with the subscribers HPLMN.

5.4.3.2 Network Selection

The WLAN UE shall provide an initial NAI, constructed according to Section 5.4.2 indicating the WLAN 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 WLAN UE's Home 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 WLAN UE. The WLAN 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.

After the network advertisement information is delivered, the WLAN UE attempts to authenticate with the roaming NAI determined in the prior step.

The WLAN AN shall use the NAI to route the EAP traffic to the appropriate VPLMN AAA Proxy.

5.5 Authentication methods

Authentication methods are discussed in TS 33.234 [6].

5.6 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.

5.6.1 Accessing Home Network provided services

The following functionality and requirements have been identified:

- It shall be possible to support multiple service authorizations after a successful WLAN authentication/authorisation (i.e. EAP success).
- The Service authorisation procedure should, as far as possible, be independent from WLAN Access authentication and authorisation.
- The routing policy applied at WLAN Access Authentication and Authorisation may include policy determining whether the user has IP connectivity the WAGs or PDGs used for Access to External IP networks.
- It shall be possible to permit access to different services simultaneously.
- 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 WLAN 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.

- The 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 external network, i.e. Wi interface.

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

5.6.2 Accessing Visited Network provided services

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

- In order for the UE to be able to use W-APNs in the VPLMN, 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 external network, i.e. Wi interface.

5.6.3 External IP Network selection

The WLAN 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 indicate a point of interconnection to the external IP network (i.e. PDG).

A W-APN is indicated by the WLAN UE in the tunnel establishment procedure between the WLAN 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).

5.7 IP Connectivity for scenario 3

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

5.7.1 Principles

The WLAN UE initiates the establishment of tunnels and is involved in packet encapsulation/decapsulation. The tunnel shall be between the WLAN UE and the PDG. In the non roaming case, the PDG shall be in the Home PLMN; in the roaming case, the PDG may be either in the Home or in the Visited PLMN (both cases shall be supported).

The following steps are performed after WLAN access authentication/authorisation:

1. W-APN resolution and discovery of the tunnel endpoint (PDG) IP-address is performed using the following procedures:
 - Details of the APN resolution mechanism are FFS.
2. Tunnel establishment, including mutual authentication, shall occur between the WLAN UE and the PDG.

Note 1: Filtering attributes may be needed in order to enable the WLAN to enforce that the WLAN UE tunnels all traffic as required. Filtering attributes may be transmitted from 3GPP AAA Server to WLAN over the Wt reference point. The WLAN sets up appropriate packet filters.

Note 2: The PDG is described in section 6.

The tunnel establishment is not coupled to WLAN access authentication/authorisation. The WLAN UE may establish several tunnels in order to access several external IP networks simultaneously. The external IP network selection is performed as part of the establishment of each tunnel.

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

5.7.2 Tunnelling Requirements

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

- Minimal requirements to the underlying IP connectivity network, i.e. WLAN 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 WLAN UE may be obtained from/through the remote tunnel endpoint
- Set up secure tunnels between WLAN UE and remote tunnel endpoint. Especially support encryption and integrity protection during tunnel establishment and while transporting user data packets, if enabled.
- Remote IP address (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)
- Local IP address (outer IP):
 - Tunnel shall be able to support IPv4 and IPv6 transport addresses
 - Non-routable in the public internet (e.g. private) WLAN UE's local IP addresses shall be supported
- The protocol should be fully specified and 3GPP should define its usage to enable multi-vendor inter-operability.

5.8 Roaming requirements for scenario 3

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 to 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 allow the home network to limit the set of 3GPP services available for a given roaming user.
- Scenario 3 requires that all packets sent to/from a WLAN UE are routed via a VPLMN in a 3GPP network.

5.9 Scenario 3 Routing Enforcement

5.9.1 Purpose for routing enforcement

In order to ensure operator policies, e.g. QoS, Charging can be applied to user traffic, scenario 3 requires routing policy enforcement to be implemented in the 3GPP-WLAN interworking system.

5.9.2 Routing Enforcement in the WLAN AN

Routing enforcement shall be used to ensure that all packets sent to/from the WLAN UE for 3G PS service are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case). However, this routing enforcement shall not prevent the WLAN AN from routing non 3G PS service traffic to another network (e.g. the Internet) other than PLMN.

When subscription limits a WLAN UE to exclusively access 3GPP PS service, the PLMN can indicate to the WLAN AN routing enforcement policy to ensure that all packets sent to/from the WLAN UE are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case).

For WLAN UEs with non-exclusive access to 3GPP PS service, routing enforcement in the WLAN AN shall ensure that packets sent to/from the PDG are routed to the right entity in the interworking VPLMN (roaming case) or HPLMN (no roaming case).

Routing enforcement should not prevent the WLAN AN from supporting scenario 2 WLAN UE and non 3G interworking WLAN terminals.

Routing enforcement should have minimal impact on the WLAN AN.

5.9.3 Policy Enforcement in the HPLMN

When operating in scenario 3 and access is via a tunnel endpoint 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.

5.9.4 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.

5.10 IP address allocation for the WLAN UE

In Scenario 2, a WLAN UE needs to use its local IP address only. In Scenario 3, a WLAN UE shall use two IP address; its local IP address and remote IP address.

A WLAN UE's local IP address identifies the WLAN UE in the WLAN AN. In scenario 2, the WLAN UE's local IP address is assigned by the WLAN AN; in scenario 3, it can be assigned by a WLAN or by a PLMN (a VPLMN in roaming case and a HPLMN in non-roaming case). For the WLAN-assigned local IP address, which belongs to the address space of WLAN AN, there is no additional requirement on the WLAN. WLAN UE's local IP address allocation by the PLMN is for further study.

In scenario3, A WLAN UE's remote IP address identifies the WLAN UE in the network that the UE is accessing for the 3G PS service. It shall be used for the inner packet of the UE-initiated tunnel. It can be assigned by HPLMN, VPLMN or an external IP network. The only case where VPLMN assigns the remote IP address for the WLAN UE is when the UE-initiated tunnel terminates at the VPLMN's PDG. When the WLAN UE's remote IP address is allocated by the external IP network, the PDG is required to have an interface with an address allocation server, such as AAA or DHCP, belonging to the external IP network.

5.11 Charging

The following functionality and requirements have been identified:

- The WLAN Access Network shall be able to report the WLAN access usage to the appropriate 3GPP system (i.e. VPLMN in the roaming case and HPLMN in the non-roaming case).
- 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.
- It shall be possible to apply offline charging and online charging mechanisms for the WLAN interworking with 3GPP network.

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

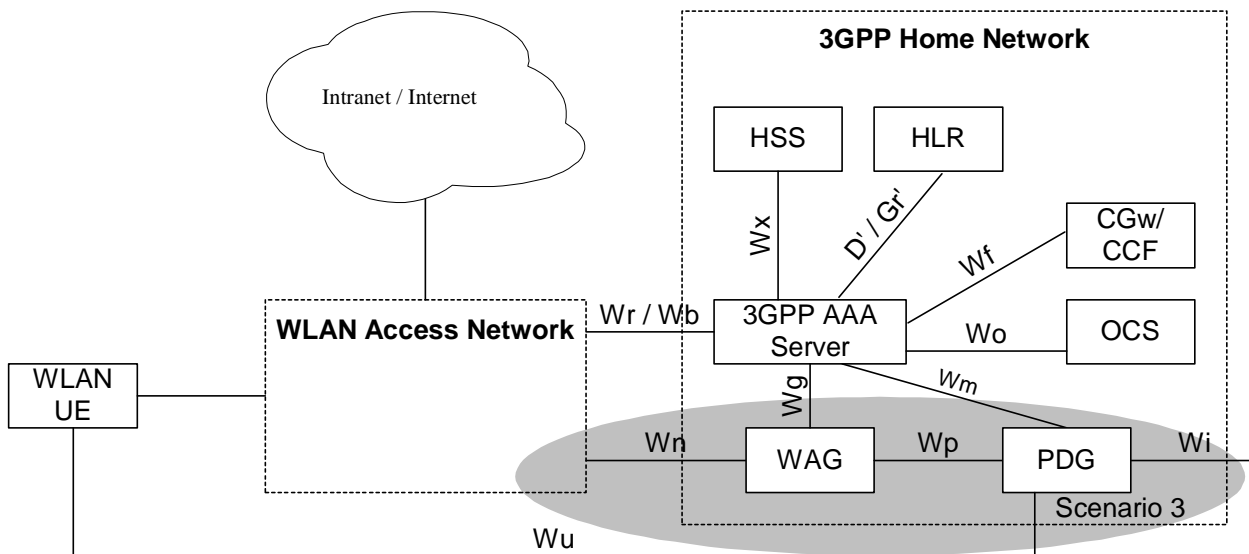


Figure 6.1 Non Roaming Reference Model. The shaded area refers to scenario 3 functionality

6.1.2 Roaming WLAN Inter-working Reference Model

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.

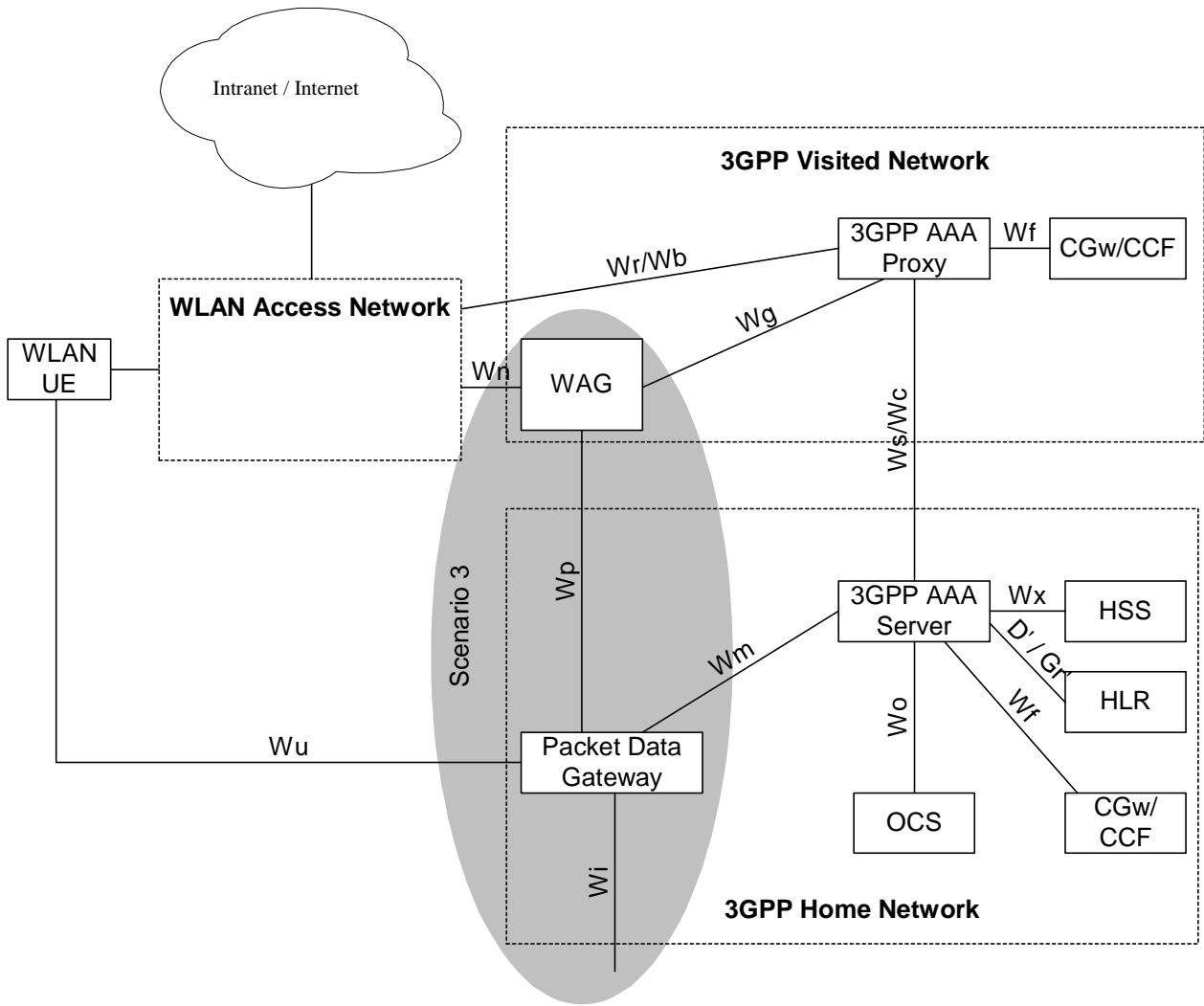


Figure 6.2a. Roaming Reference Model- 3GPP PS based services provided via the 3GPP Home Network (the shaded area refers to scenario 3 functionality)

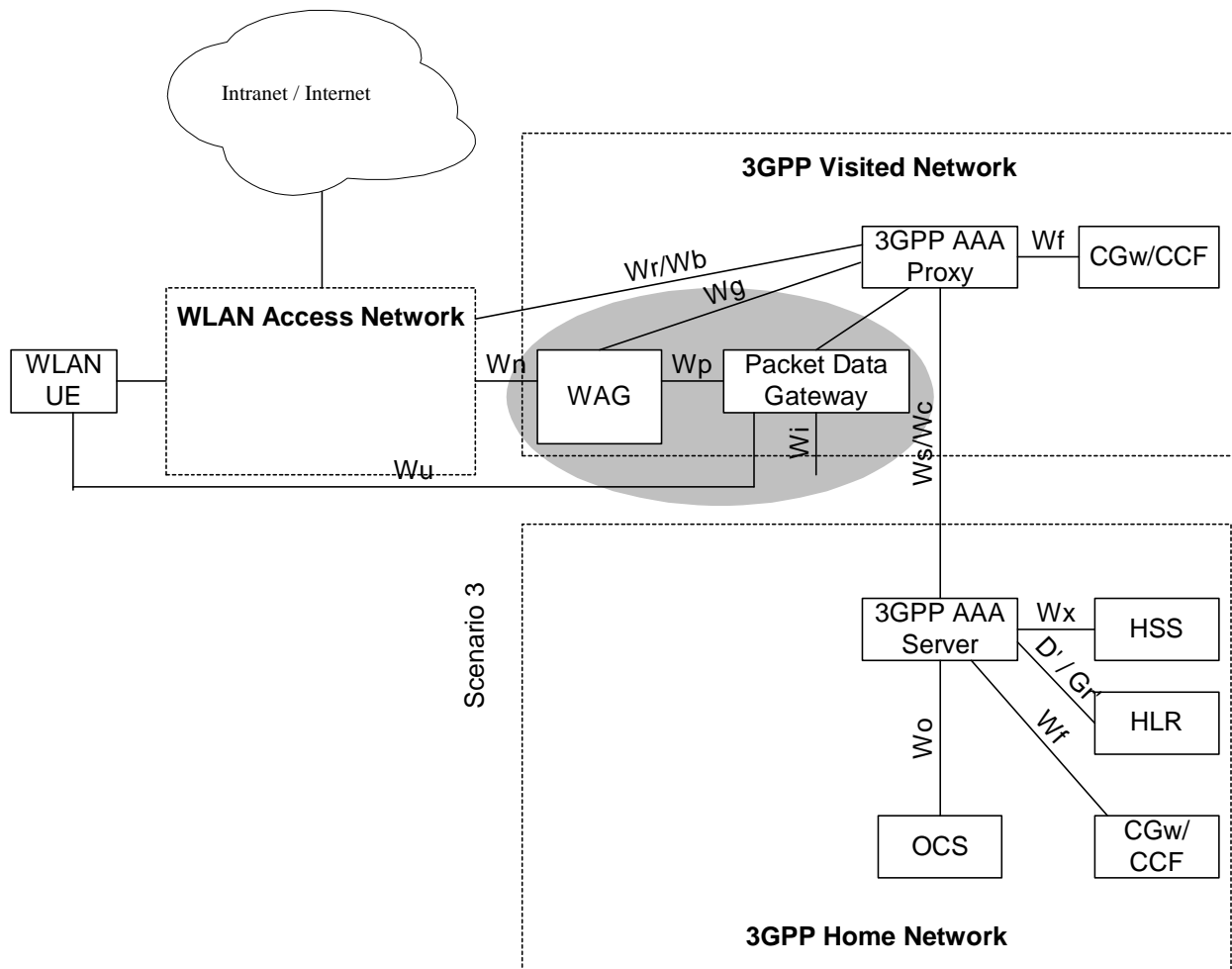


Figure 6.2b. Roaming Reference Model- 3GPP PS based services provided via the 3GPP Visited Network (the shaded area refers to scenario 3 functionality)

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 WLAN UE may be capable of WLAN access only, or it may be capable of both WLAN and 3GPP System accesses. Some WLAN UE may be capable of simultaneous access to both WLAN and 3GPP systems. The WLAN 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 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 per-user charging/accounting information to the VPLMN CCF/CGw for roaming users
- Service termination (O&M initiated termination from visited network operator)
- Protocol conversion when the Wr and Ws or Wb and Wc interfaces do not use the same protocol

For Scenario 3 only:

- Receiving authorization information related to subscriber requests for W-APNs in the Home or Visited network
- Authorization of access to Visited network W-APNs according to local policy

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:

- Retrieves authentication information and subscriber profile (including subscriber's authorization information) from the HLR/HSS of the 3GPP subscriber's home 3GPP network.
- Authenticates the 3GPP subscriber based on the authentication information retrieved from HLR/HSS. The authentication signaling may pass through AAA proxies.
- Communicates authorization information to the WLAN potentially via AAA proxies.
- Registers its (the 3GPP AAA server) address or name with the HLR/HSS for each authenticated and authorized 3GPP subscriber.
- Initiates the Purge procedure when the 3GPP AAA server deletes the information of a subscriber.
- May act also as a AAA proxy (see above).
- Maintains the WLAN UE's WLAN-attach status.
- Provides the WLAN UE's WLAN-attach status to other entities (which are out of the scope of this TS).
- Generates and reports per-user charging/accounting information to the HPLMN CCF/CGw.

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 WLAN UE's WLAN-attach status for other entities, e.g. answers or relays the WLAN-attach status query from other entities (which are out of the scope of this TS).

6.2.5 WLAN Access Gateway

The WLAN Access Gateway applies to scenario-3.

The WLAN Access Gateway is a gateway via which the data to/from the WLAN Access Network shall be routed via a PLMN to provide a WLAN UE with 3G PS based services in scenario 3.

The WLAN Access Gateway shall be in the VPLMN in the roaming case, and in the HPLMN in the non-roaming case.

The WLAN Access Gateway:

- Allows VPLMN to generate charging information for users accessing via the WLAN AN in the roaming case.
- Enforces routing of packets through the PDG.

Editor's note: Per-user charging generation in the WAG is FFS.

Note: per-user charging generation in the WAG is not required when the WAG and PDG are in the same network, i.e. the non-roaming case.

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

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

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

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 3GPP AAA Server to the 3GPP AAA Proxy.

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

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.

Editor's note: 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

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.

Note: From a WAG perspective, the key differentiator is how the WAG binds the routing enforcement to a user's traffic.

6.2.6 Packet Data Gateway

The Packet Data Gateway applies to scenario-3.

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 WLAN UE;
- Allocation of a WLAN UE's remote IP address (the WLAN UE's home address) to the WLAN UE by the HPLMN (if one is not already allocated);
- Registration of the WLAN UE's local IP address with the Packet Data Gateway and binding of this address with the WLAN UE's remote IP address.

The Packet Data Gateway:

- Contains routing 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 WLAN UE's remote IP address;
- Relays the WLAN UE's remote IP address allocated by an external IP network to the WLAN UE, when external IP network address allocation is used.
- Performs registration of the WLAN UE's local IP address and binding of this address with the WLAN UE's remote IP address;
- Provides procedures for unbinding a WLAN UE's local IP address with the WLAN UE's remote IP address;
- Provides procedures for authentication and prevention of hijacking (i.e. ensuring the validity of the WLAN UE initiating any binding of the WLAN UE's local IP address with the WLAN UE's remote IP 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.
- Performs the functions of Service-based Local Policy Enforcement Point (controls the quality of service that is provided to a set of IP flow as defined by a packet classifier, control admission based on policy that is applied to the IP bearers associated with the flow, and configuration of the packet handling and "gating" functionality in the user plane.)

- Communicates with Policy Control Function (PCF) to allow service-based local policy and QoS inter-working information to be “pushed” by the PCF or to be requested by the PDG. This communication also provides information to support the following functions in the PDG:
 - Control of Diffserv inter-working;
 - Control of RSVP admission control and inter-working;
 - Control of “gating” function in PDG;
 - WLAN bearer authorization;
 - QoS charging related function.

6.3 Reference Points

6.3.1 Wr reference point

6.3.1.1 General description

The Wr reference point 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].

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 reference point

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 WLAN UE) including an indication of whether the VPLMN is allowed to provide this service.

6.3.3 D'/Gr' reference point

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 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 WLAN 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 reference point

The Wb reference point 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

The Wo reference point 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 reference point

The Wf reference point 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.

6.3.7 Wg reference point

The Wg reference point applies to scenario-3.

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 reference point

The Wn reference point applies to scenario-3.

This is the reference point between the WLAN Access Network and the WAG. This interface is to force traffic on a WLAN UE initiated tunnel to travel via the WAG. A site-to-site tunnel (see Annex C) may be provided for the routing enforcement.

6.3.9 Wp reference point

The Wp reference point applies to scenario-3.

This is the reference point between the WAG and PDG.

6.3.10 Wi reference point

The Wi reference point applies to scenario-3.

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 Wm reference point

The Wm reference point applies to scenario-3.

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

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

The protocol crossing this reference point is Diameter.

6.3.12 Ws reference point

The Ws reference point applies to scenario-3.

6.3.12.1 General description

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

6.3.12.2 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

6.3.12.3 Protocols

The 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 Wc reference point

The Wc reference point applies to scenario-3.

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.

6.3.14 Wu reference point

The Wu reference point applies to scenario-3.

The Wu reference point is located between the WLAN UE and the Packet Data Gateway. It represents the WLAN UE-initiated tunnel between the WLAN UE and the Packet Data Gateway. Transport for the Wu reference point protocol is provided by the Wn and Wp reference points, which ensure 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:

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

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 (if needed).*

7.1 WLAN Access Authentication and Authorisation

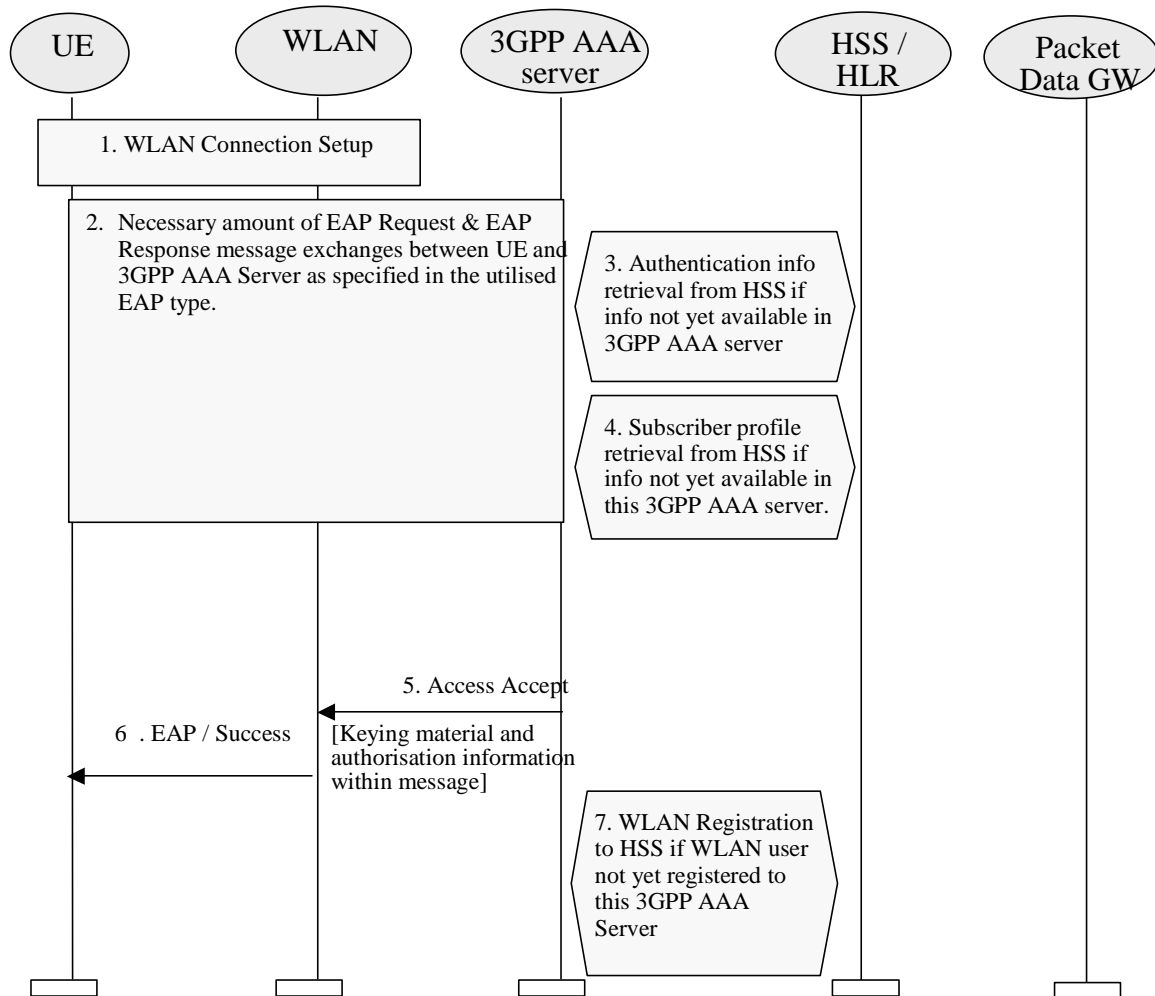


Figure 7.1 Authentication and authorisation procedure

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 W_r reference point.

A number of EAP Request and EAP Response message exchanges is executed between 3GPP AAA Server and WLAN 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 If the EAP authentication was successful, then 3GPP AAA Server sends 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 WLAN UE.

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

7 3GPP AAA server registers the WLAN users 3GPP AAA Server to the HSS. In registration messages the subscriber is identified by his permanent identity. This registration is needed only if the subscriber is not already registered to this 3GPP AAA Server.

7.2 Subscriber Profile Update

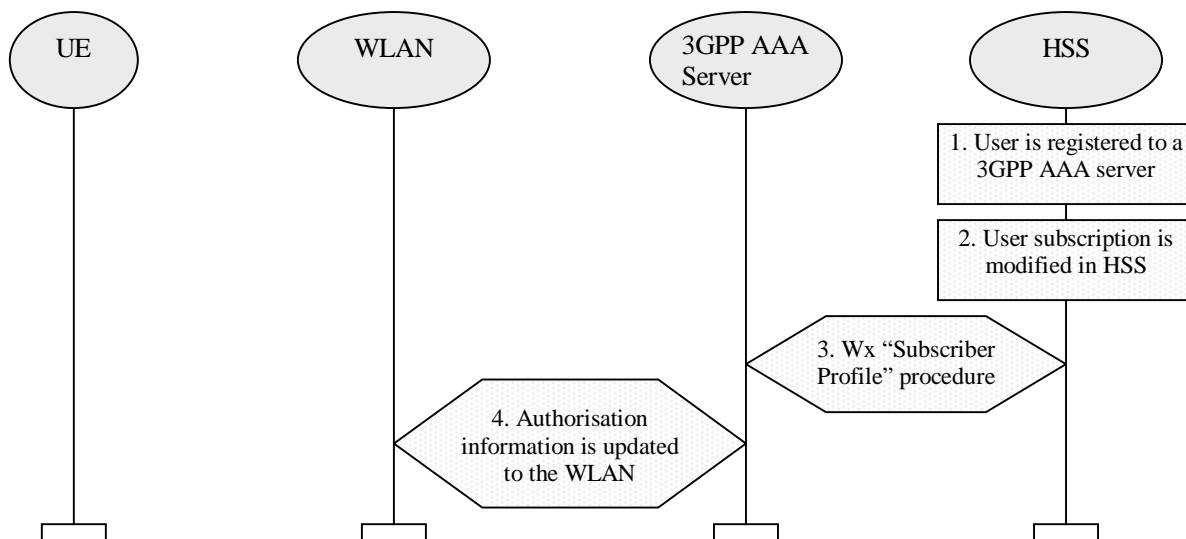


Figure 7.2 Subscriber Profile Update Procedure

1. User is registered to a 3GPP AAA server

2. Subscribers subscription is modified 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

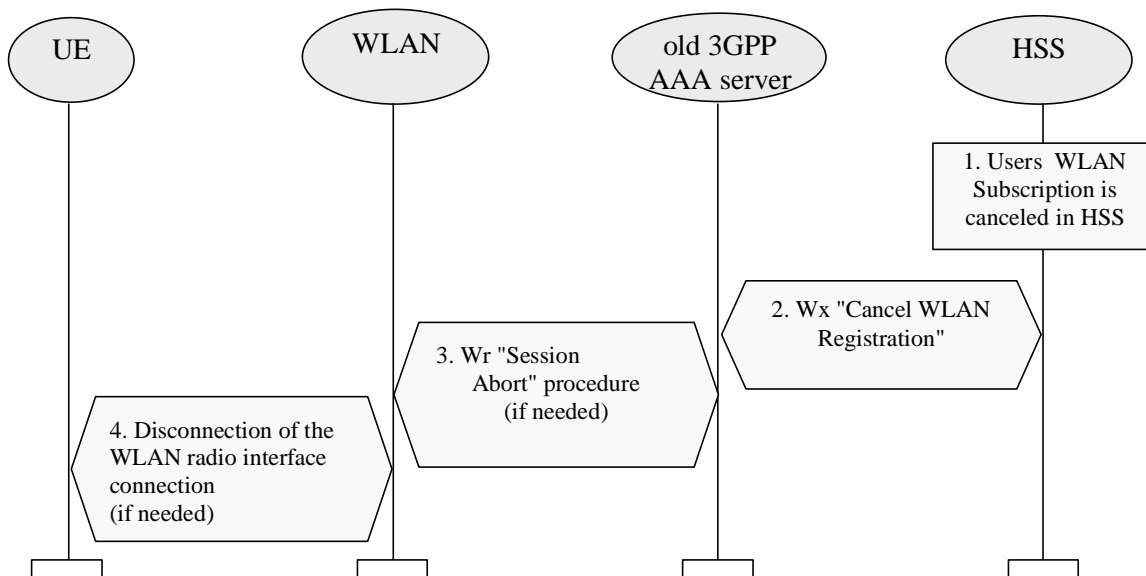


Figure 7.3 Cancellation of WLAN Registration Procedure

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 subscriber's connection still exists, Wr reference point procedure "Session Abort" procedure is executed towards WLAN.
4. If the radio connection still exists, WLAN disconnects the radio interface connection by WLAN technology specific mechanisms.

7.4 Disconnecting a Subscriber by WLAN

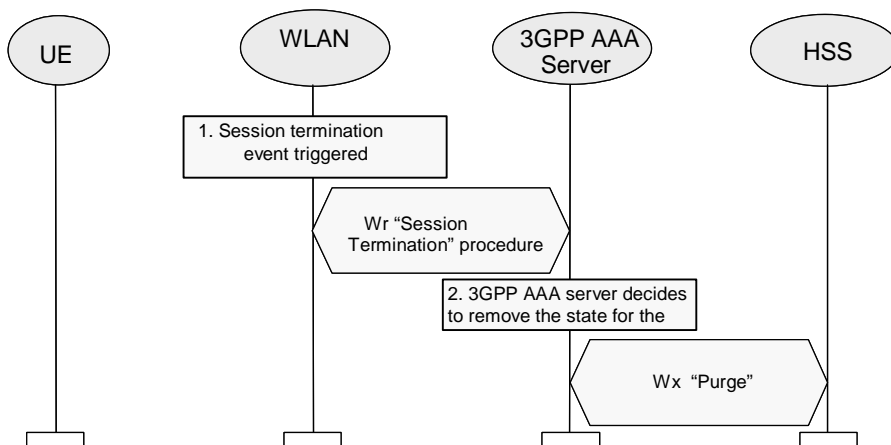


Figure 7.4 WLAN initiated disconnection procedure

1. WLAN detects that a Session related to a WLAN UE should be terminated towards the 3GPP AAA Server, e.g. when the WLAN UE has disappeared from WLAN coverage.
WLAN initiates Wr Session Termination procedure towards 3GPP AAA server.
2. In case when the 3GPP AAA server decides to remove the WLAN UEs state from the 3GPP AAA server, the 3GPP AAA server notifies HSS using Wx procedure “Purge” that the WLAN registration in the 3GPP AAA Server has been cancelled. HSS removes the state related to that 3GPP AAA server, e.g., the address of the serving 3GPP AAA server for the identified subscriber.

7.5 Disconnecting a Subscriber by Online Charging System

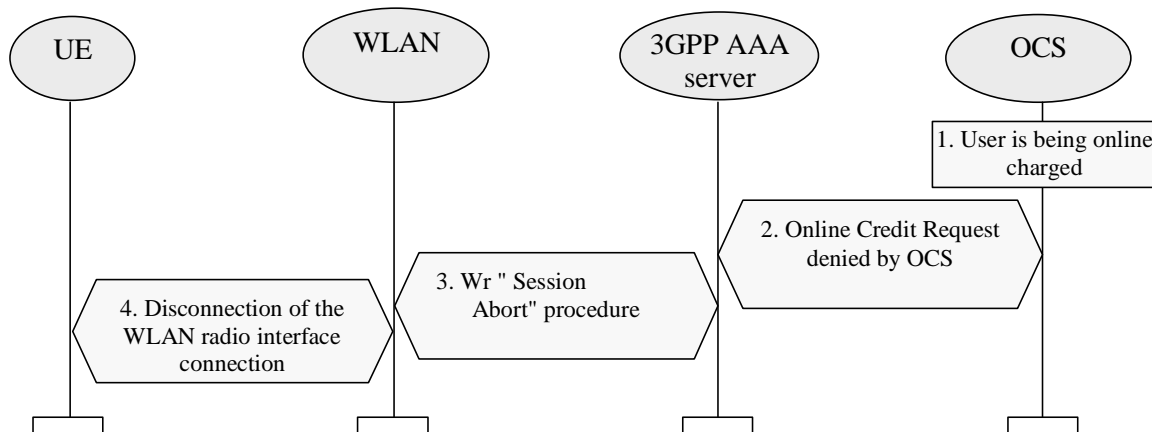


Figure 7.5 OCS Initiated Disconnection Procedure

1. A subscriber is being online charged by 3GPP AAA server.
2. OCS (online Charging System) denies credit request from the 3GPP AAA server for WLAN access. The possibly already retrieved online credit runs out.

3. To disconnect the subscriber's connection, W_r reference point procedure "Session Abort" procedure is executed towards WLAN.
4. WLAN disconnects the radio interface connection by WLAN technology specific mechanisms

7.6 Charging offline charged subscribers

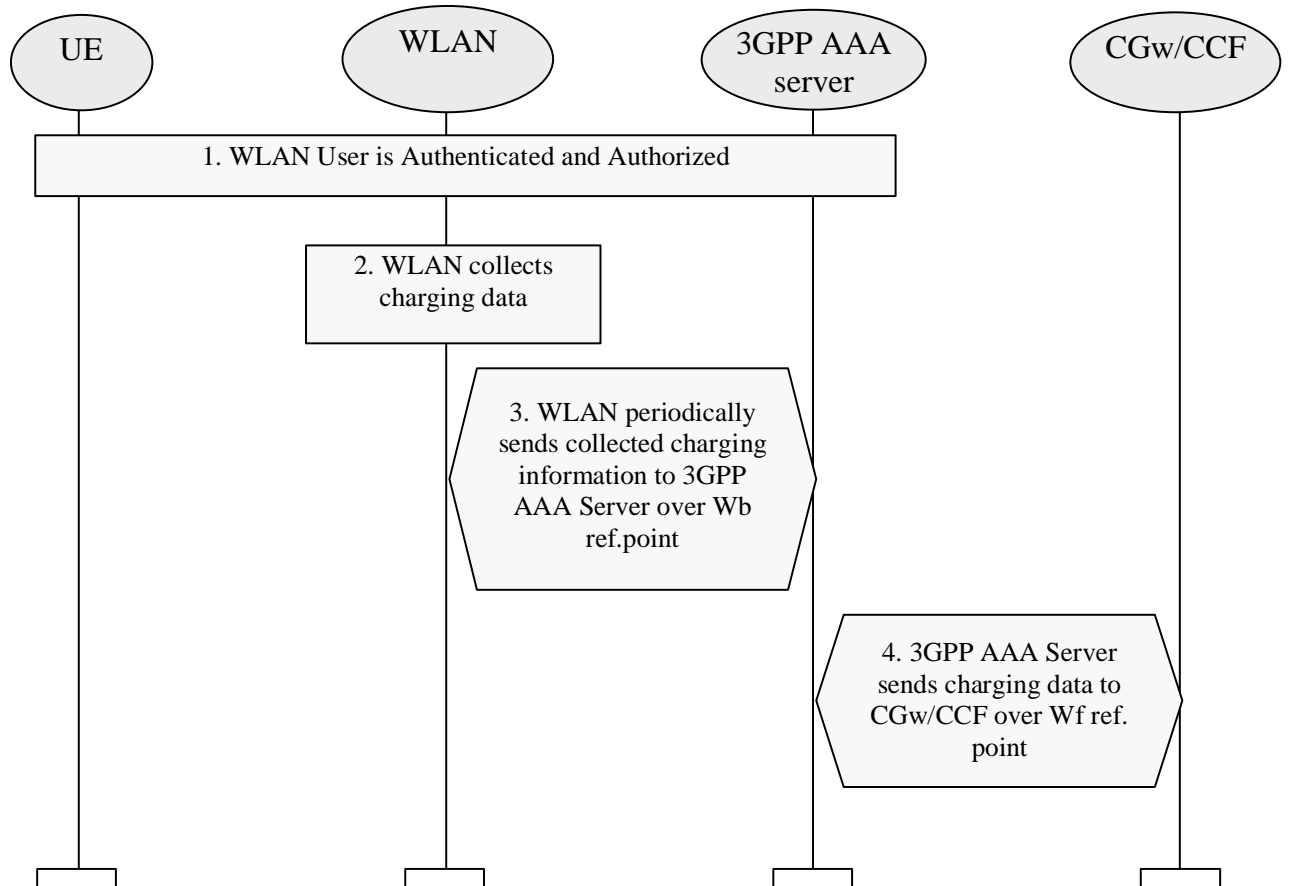


Figure 7.6 Charging Procedure for Offline Charged Subscribers

1. WLAN user is authenticated and authorized for WLAN access. User profile is downloaded into 3GPP AAA server. Part of the profile is information that the user is to be offline charged.
2. WLAN access network collects charging data related to access or services locally consumed.
3. WLAN access network periodically forwards collected charging information to the 3GPP AAA server over W_b reference point.
4. 3GPP AAA server forwards charging information to the CGw/CCF over the W_f reference point.

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

7.7 Charging online charged subscribers

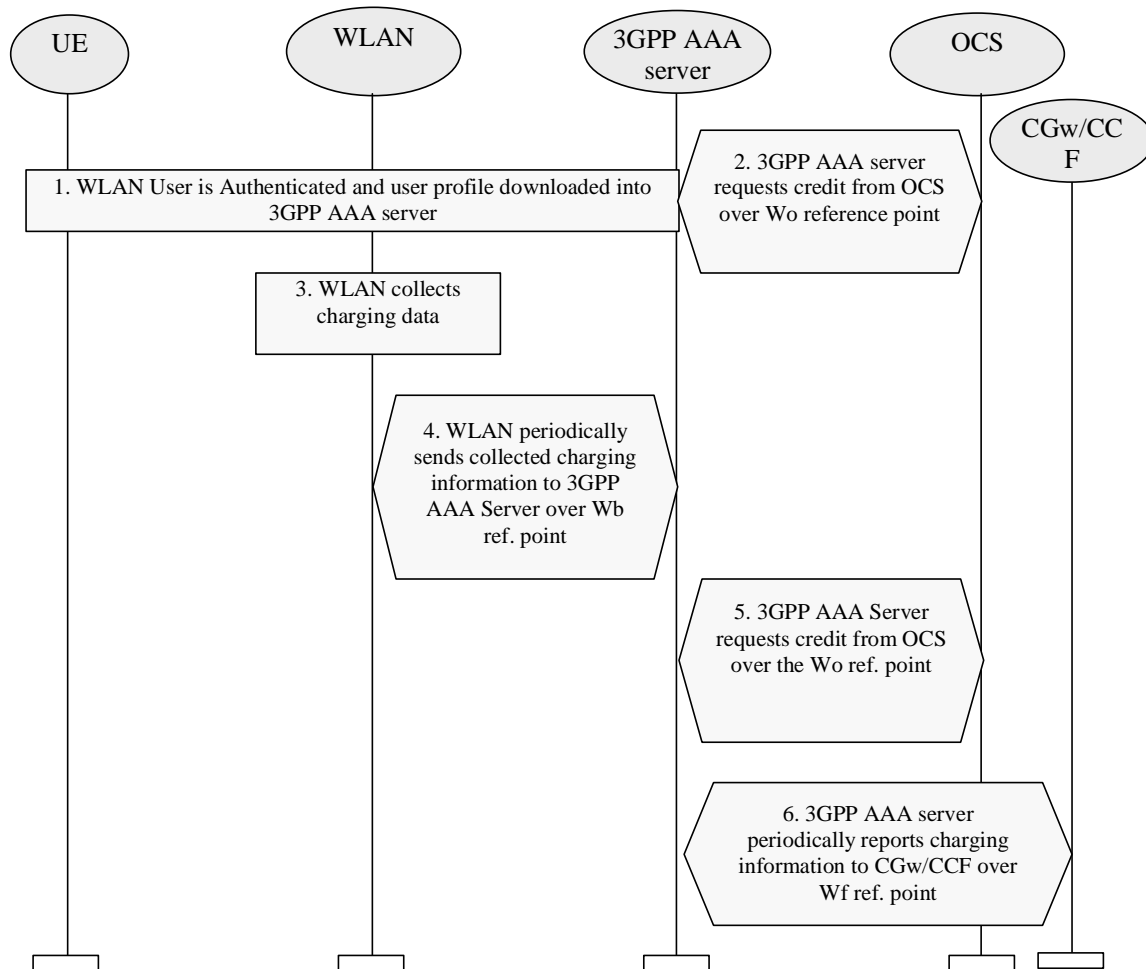


Figure 7.7 Charging Procedure for Online Charged Subscribers

1. WLAN user is authenticated and authorized for WLAN access. User profile is downloaded into 3GPP AAA server. Part of the profile is information that the user is to be online charged.
2. 3GPP AAA server obtains online charging credit from the OCS.
3. WLAN access network collects charging information.
4. WLAN access network periodically forwards collected charging information to the 3GPP AAA server over Wb reference point. WLAN access network does not request charging credit as the fact whether a user is online or 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.

7.8 Tunnel establishment

This information flow presents the generic messages exchange necessary in order to establish a WLAN UE-Initiated tunnel for Scenario 3 purposes.

Prior to the WLAN UE-Initiated tunnel establishment, it is necessary to follow two processes. Those two processes are highlighted and shown in the diagram:

1. WLAN Access Authentication and Authorisation

During this step Routing Policy enforcement rules associated to this user can be applied to WAG. E.g. depending it is a scenario 2-only user or scenario 3-only user there might be policy enforcement rules in the user subscription profile defining what it is allowed to access or not.

2. Provisioning of the WLAN UE's local IP address

After those processes are performed, the WLAN UE has the required IP connectivity to try to establish a WLAN UE-Initiated tunnel whenever the user requires it.

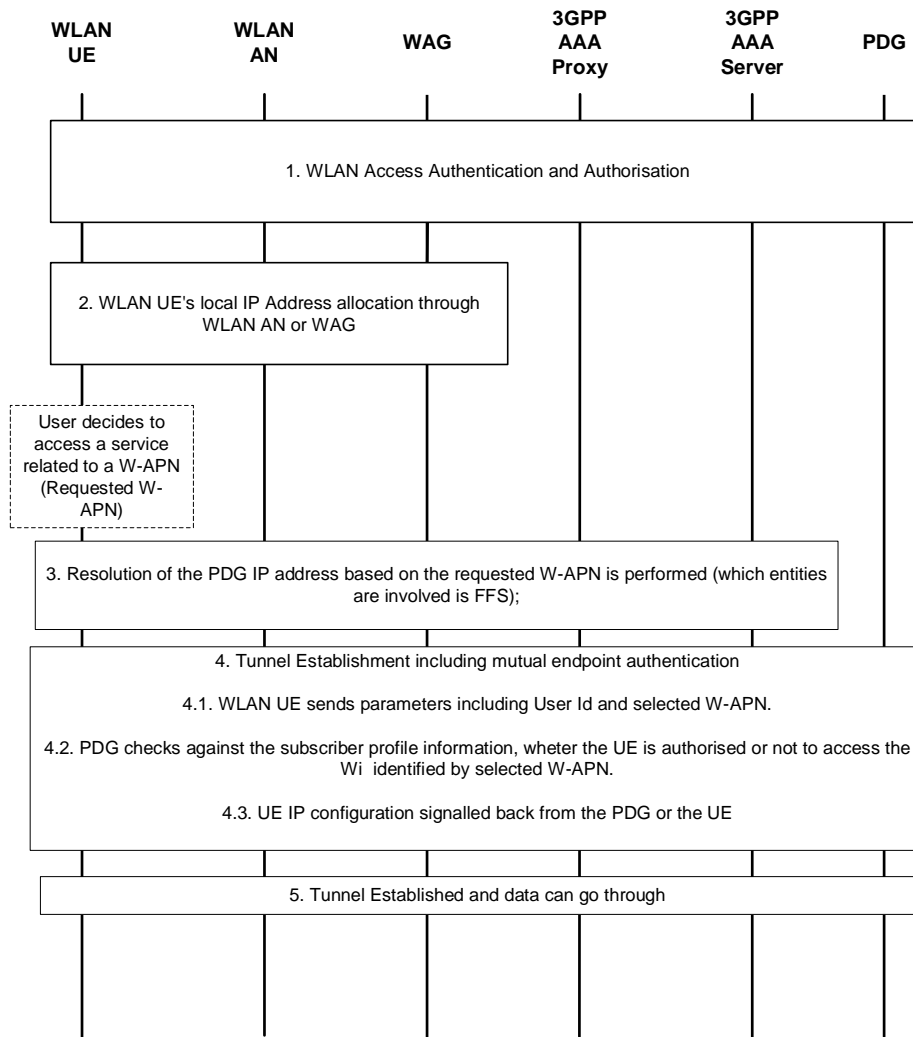


Figure 7.8. Example message flow to WLAN UE-Initiated tunnel establishment

When the User decides that it want to access a service, the WLAN UE builds the W-APN associated to the service requested by the user. The W-APN will be compound of the service identifier part and the gateway identifier part. The gateway Identifier part is having an FQDN format. The W-APN requested by the WLAN UE is the “Requested_W-APN”.

A detailed description of the WLAN UE-Initiated Tunnel Establishment in steps 3-5 is given below.

3. Resolution of the PDG IP address is performed based on the “Requested_W-APN” FQDN part. How this resolution is performed is for FFS (in the WLAN UE or in the VPLMN).
4. WLAN UE sends a “Tunnel_Establishment_Request” to the selected PDG indicating the user identity and the Selected W-APN. There is tunnel establishment signalling to authenticate the user and authorise to establish the tunnel between the WLAN UE and PDG. The PDG verifies the user and subscriber profile against the user subscriber profile for the authorisation. WLAN UE IP configuration is obtained in PDG and it is communicated to the WLAN UE
5. After the tunnelling establishment signalling has been completed, the WLAN UE is able to access the Wi reference point via the PDG and the user data can start to flow between the WLAN UE and the PDG to access Wi.

Annex A (informative): Reference Points Signalling Flows

Editor's Note: In this annex, references to Diameter should be considered as informative examples.

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 WLAN 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 authenticated session is delivered from the 3GPP AAA Server to the WLAN.

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

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

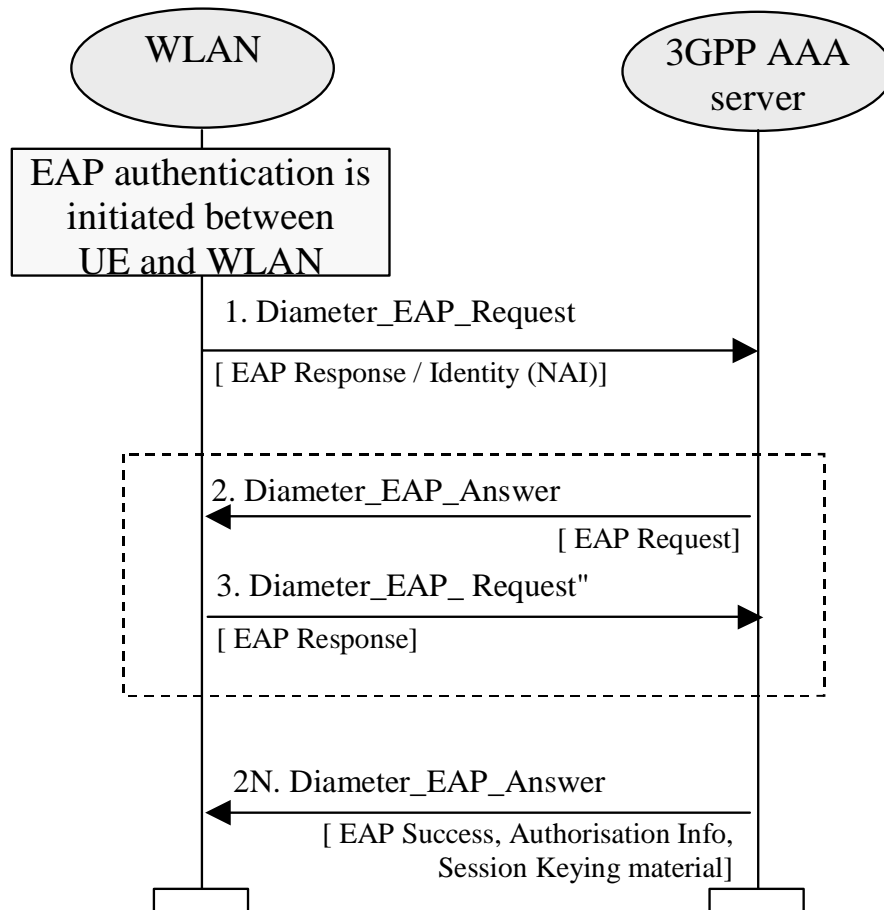


Figure A.1.1 Signalling example on W_r Reference Point for Authentication and Authorisation

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 WLAN UE.
3. WLAN 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 WLAN 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 WLAN UE shall be disconnected from accessing the WLAN interworking service.

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

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

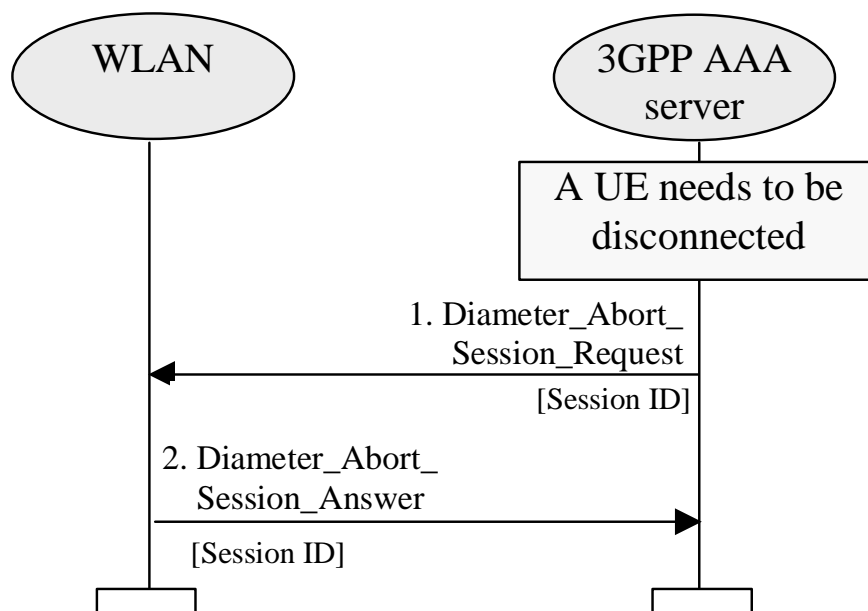


Figure A.1.2 Signalling example on W_r Reference Point for User Purging

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

A.2 Signalling Sequences examples for Wx Reference Point

A.2.1 Authentication Information Retrieval

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

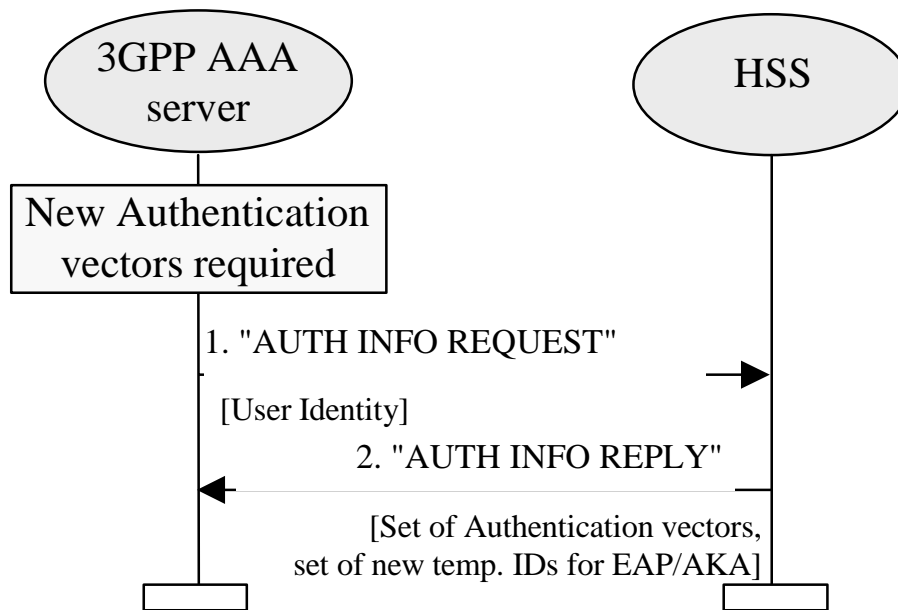


Figure A.2.1 Signalling example on Wx Reference Point for Authentication Information Retrieval

1. 3GPP AAA server detects that it requires new authentication vectors for a given 3GPP subscriber. This can happen for example, when a new 3GPP subscriber has accessed 3GPP AAA Server for authentication or when a new set of authentication information is required for one of the 3GPP subscribers already registered in the 3GPP AAA server.

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

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

Editor's 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.

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

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

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

A.2.2 Subscriber Profile Retrieval

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

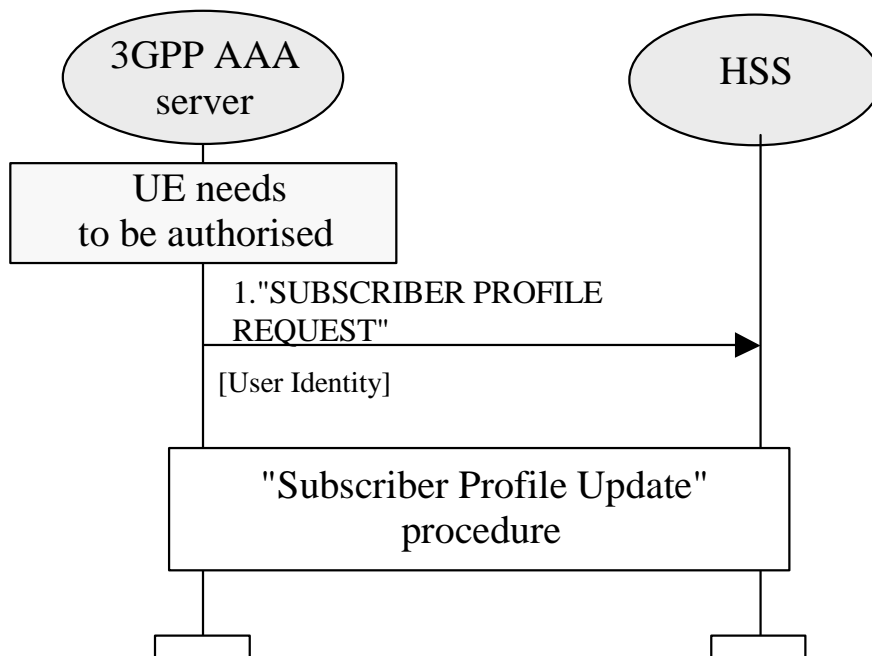


Figure A.2.2 Signalling example on Wx Reference Point for Subscriber Profile Retrieval

1. 3GPP AAA server detects that it requires the subscription profile for a given 3GPP subscriber. 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.

Editor's 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.

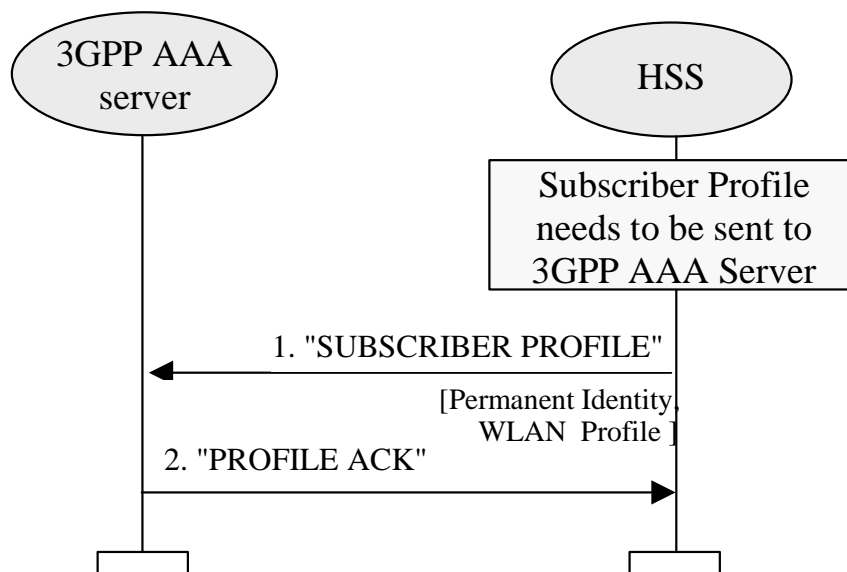


Figure A.2.3 Signalling example on Wx Reference Point for Subscriber Profile Update

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

HSS/HLR sends "SUBSCRIBER PROFILE" message to 3GPP AAA Server. For example, this message includes

- Users permanent unique identifier. In case of USIM authentication (EAP/AKA) the utilised unique identifier shall be the IMSI
- service authorisation information,
- charging mechanism (offline / online),
- in case of online charging the DNS name of the subscribers online charging system

3GPP AAA Server stores the subscriber profile information.

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

A.2.4 WLAN Registration

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

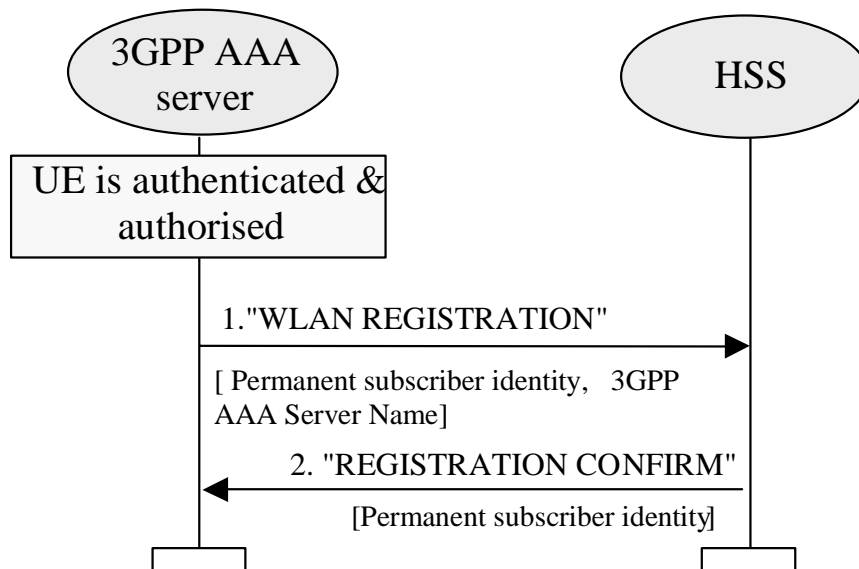


Figure A.2.4 Signalling example on Wx Reference Point for Subscriber Registration

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

A.2.5 Cancel Registration

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

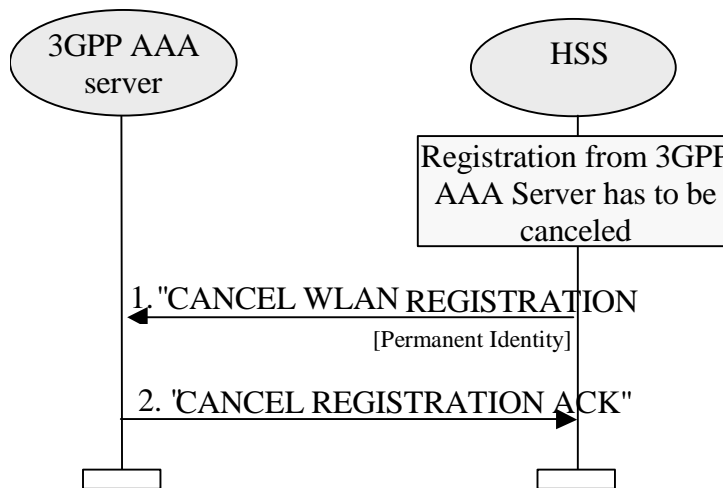


Figure A.2.5 Signalling example on Wx Reference Point for Registration Cancellation

1. HSS/HLR initiates the signalling when the registration of a 3GPP subscriber has to be 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.

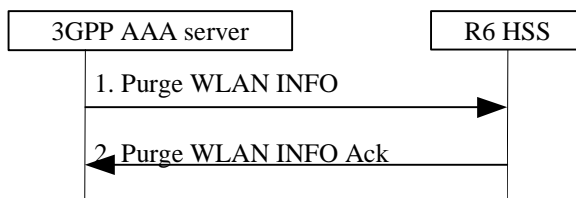


Figure A.2.6 Signalling example on Wx Reference Point for Purge Procedure

- 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

A.3.1 Authentication Information Retrieval

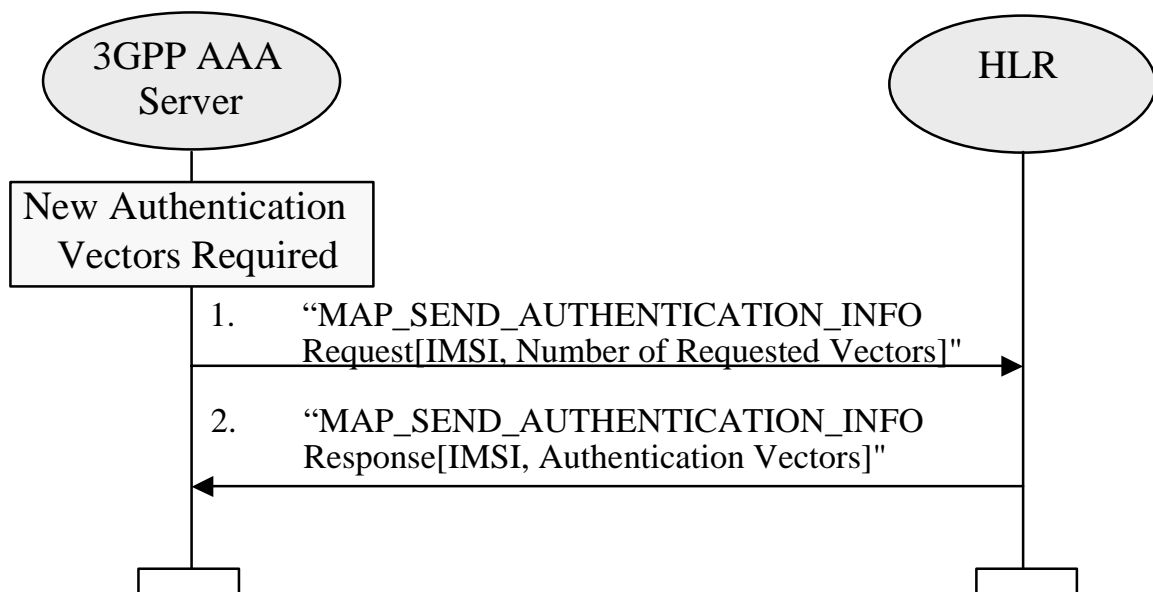


Figure A.3.1 Authentication Information Retrieval using D' interface

1. 3GPP AAA server detects that it requires new authentication vectors for a given 3GPP subscriber. This can happen for example, when a new 3GPP subscriber has accessed 3GPP AAA Server for authentication or when a new set of authentication information is required for one of the 3GPP subscribers already registered in the 3GPP AAA server.

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

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

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

A.3.2 Subscriber Profile Retrieval

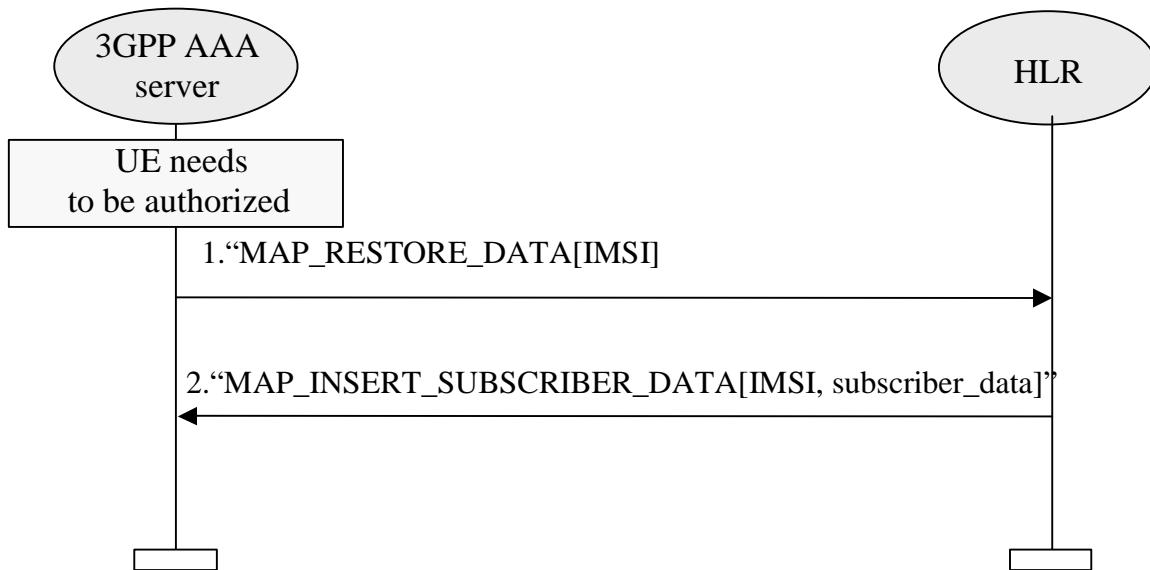


Figure A.3.2 Subscriber Profile Retrieval using D' interface

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

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

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

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

A.4 Gr' Signalling Mechanisms to support WLAN service

A.4.1 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 procedure.

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.

A.4.2 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.

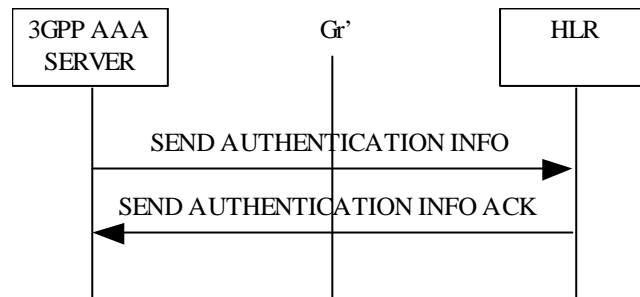


Figure A.4.1. infoRetrieval procedure

A.4.2 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.

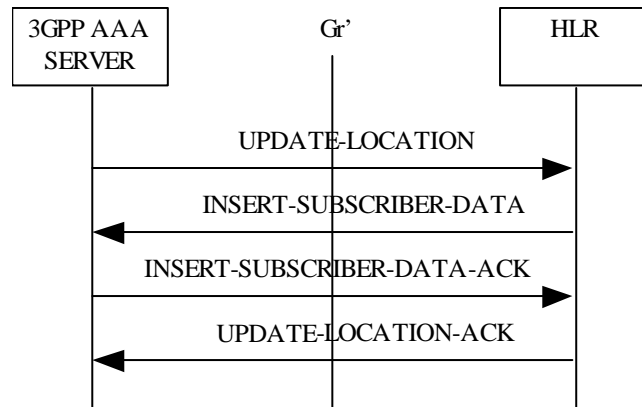


Figure A.4.2 gprsLocationUpdate procedure

A.5 Example of Authentication procedures

A.5.1 EAP/AKA Procedure

USIM based authentication may be based on existing AKA method. In the case of WLAN-3GPP system interworking, this method should be supported by a generic authentication mechanism (independently of the underlying WLAN standard), e.g. EAP. EAP/AKA authentication mechanism is described in Internet Draft draft-arkko-pppext-eap-aka. The current version is 05 (draft-arkko-pppext-eap-aka-05.txt). The following procedure is based on EAP/AKA authentication mechanism:

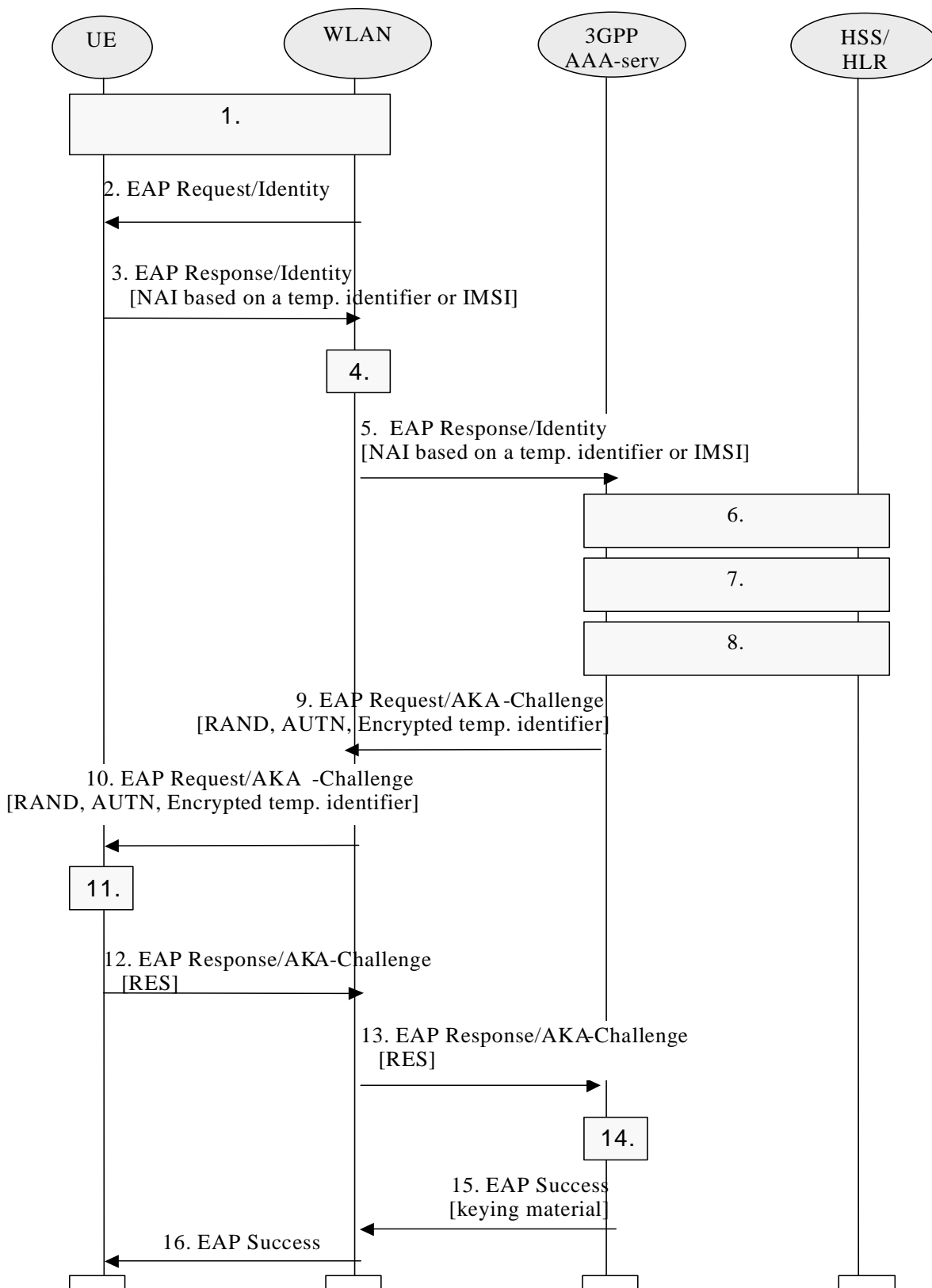


Figure A.5.1 Authentication based on EAP AKA scheme

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 WLAN UE.

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

3. The WLAN UE starts EAP AKA authentication procedure by sending an EAP Response/Identity message. The WLAN UE sends its identity complying with Network Access Identifier (NAI) format specified in RFC 2486. NAI contains the temporary identifier allocated to WLAN 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 WLAN 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 WLAN UE
11. WLAN 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.

WLAN UE derives required additional keying material from IK and CK. WLAN UE decrypts temporary identifier and saves it to be used on next authentication.
12. WLAN 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 WLAN UE.
16. WLAN informs the WLAN UE about the successful authentication with the EAP Success message. Now the EAP AKA exchange has been successfully completed, and the WLAN 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:

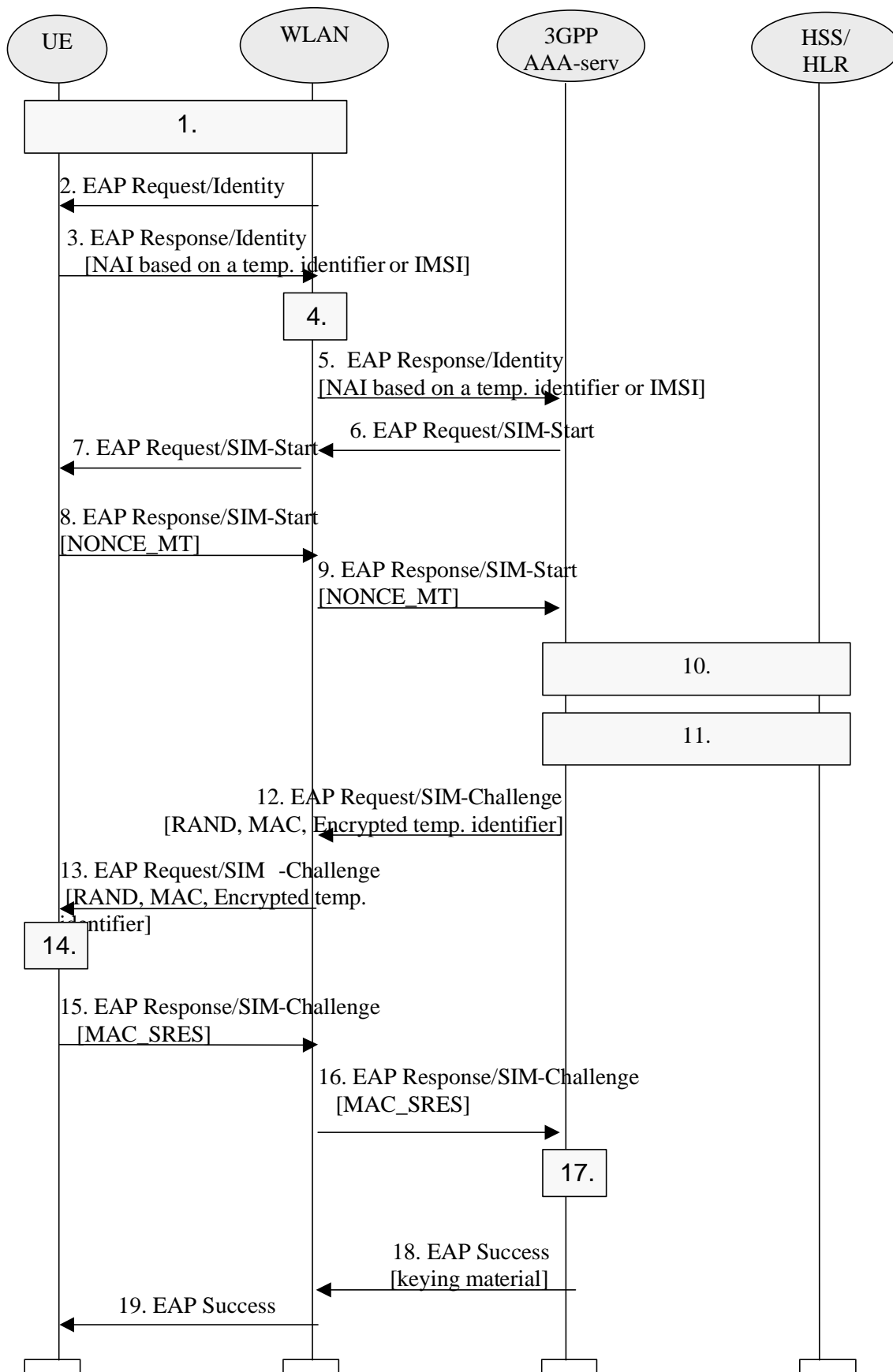


Figure A.5.2 Authentication based on EAP SIM scheme

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 WLAN UE.

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

3. The WLAN UE starts EAP SIM authentication procedure by sending an EAP Response/Identity message. The WLAN UE sends its identity complying to Network Access Identifier (NAI) format specified in RFC 2486. NAI contains the temporary identifier allocated to WLAN 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-ppext-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 WLAN UE
8. The WLAN UE chooses a fresh random number NONCE_MT. The random number is used in network authentication.

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

This computing gives N SRES and Kc values.

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

The WLAN 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 WLAN UE cancels the authentication (not shown in this example). The WLAN UE continues the authentication exchange only if the MAC is correct.

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

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

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

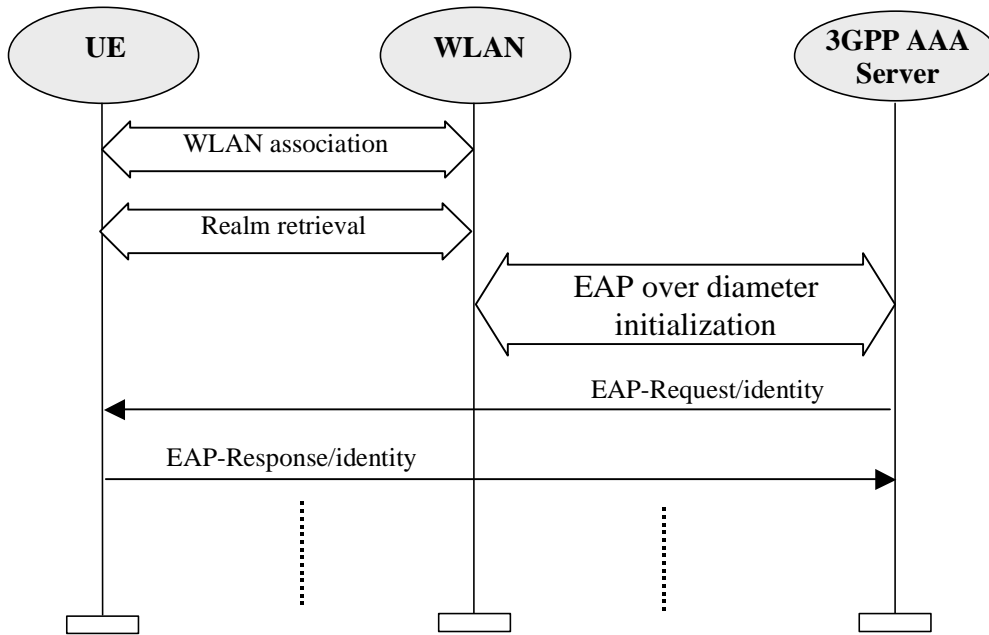


Figure A.5.3 End-to-end EAP initialisation session

A.5.4 Re-authentication message sequence chart

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

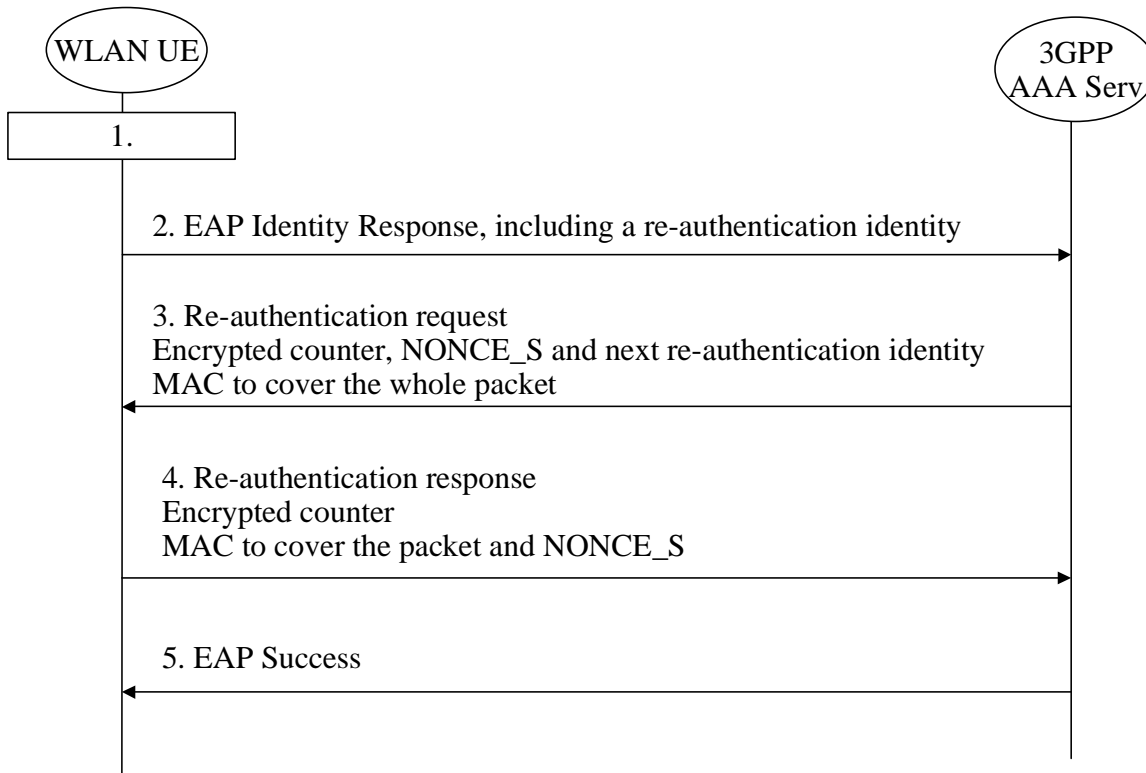


Figure A.4.4 Re-authentication signalling sequence

1. Either the WLAN 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 WLAN 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): Site to Site Tunnelling

Site-to-Site tunnelling is a 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.

C.1 WLAN 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 WLAN 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 D (informative): Information on the discussed tunnel switching alternative

D.1 Non Roaming WLAN Inter-working Reference Model

The 3GPP-WLAN Interworking reference model in the non-roaming case is shown in Figure D.1.1.

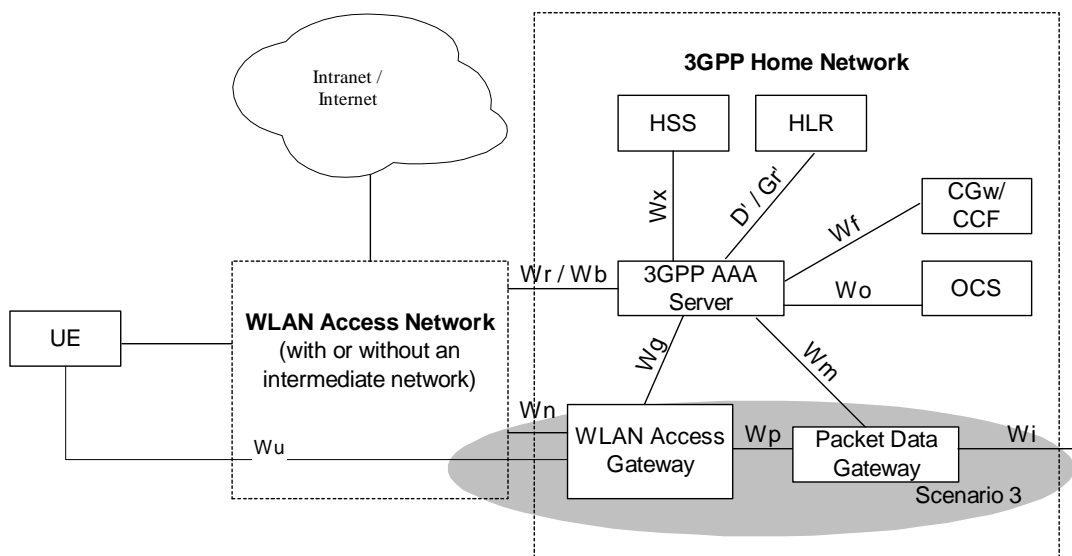


Figure D.1.1 Non Roaming Reference Model

D.2 Roaming WLAN Inter-working Reference Model

Figure D.2.1 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 W_x and W_o interfaces are intra-operator. The 3GPP network interfaces to other 3GPP networks, WLANs, and intermediate networks via the W_r and W_b 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.

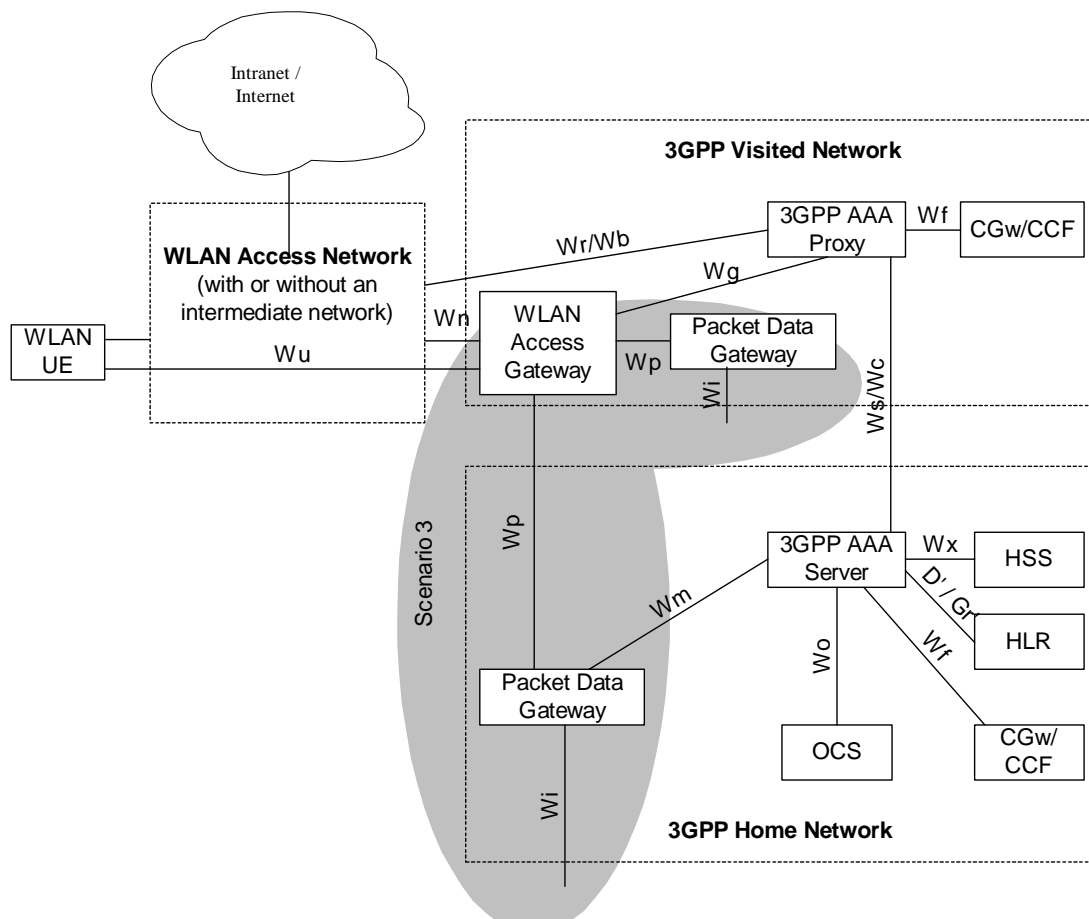


Figure D.2.1 Roaming Reference Model

D.3 WAG Description

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

The WAG shall:

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

D.4 Wu Reference Point

The reference point Wu is located between the WLAN UE and the WAG. The purpose of this reference point is to transport tunnelled user data traffic securely between the WLAN UE and the 3GPP network to provide PS-based services to the WLAN UE. In roaming cases, the Wu reference point is terminated between the WLAN 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 WLAN UE will be able to use an existing VPN client.

D.5 Wn Reference Point

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.

D.6 Wp Reference Point

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 E (informative): W-APN resolution comparison

E.1 Solutions considered

Two solutions are currently considered for APN resolution: “UE DNS client” and “WAG DNS client”. These two solutions are described in this section. For simplicity we first consider only Home network PDGs. The solutions can both be extended to support Visited network PDGs as described in Section 3 below.

The two solutions have the following properties:

1. Packets are not routed onto GRX from a UE which has not been authenticated by the 3GPP system
2. Packets are not routed onto GRX towards a PDG, unless a UE that is subscribed to a W-APN served by that PDG is present on the WLAN. Packets from users with Scenario 2 only subscription, or which are not authenticated are not routed onto GRX.
3. The Home Network has the final decision about which PDG is used to provide access to a particular W-APN.

In the flows below we do not always show the whole authentication exchange associated with a tunnel setup or APN access request message.

E.1.1 UE DNS Client

In this solution, the addresses of the PDGs are stored in the DNS of the HPLMN. The UE is configured with a DNS server, e.g. using DHCP. This DNS server may be in the WLAN AN or the VPLMN. During activation of an APN, the UE performs a public DNS lookup using a standard format domain name to obtain the address of a PDG. Note that the DNS servers in the WLAN AN and VPLMN can be configured in a way that a DNS query to the HPLMN DNS system is not routed through the Internet. The UE then attempts a tunnel establishment to this PDG.

In order to meet Requirements 1 and 2, policies must be downloaded to the WAG at initial WLAN Access Authentication. These policies will open a route through the WLAN AN on to GRX for the particular PDGs that the UE is authorised to access. Since the UE IP address is not allocated at this time, the source address in these filters must be wildcarded, meaning that other authenticated UEs can send packets towards the PDGs.

At any one time, an authenticated UE can send packets to the set of PDGs supporting APNs that are subscribed by any of the authenticated UEs on the WLAN. This set is updated as UEs arrive and leave the WLAN.

In order to meet Requirement 3, the Home Network must have the possibility to redirect the tunnel establishment request to a different PDG.

The message flow for this case is shown below (starting with the final EAP response of the initial EAP exchange):

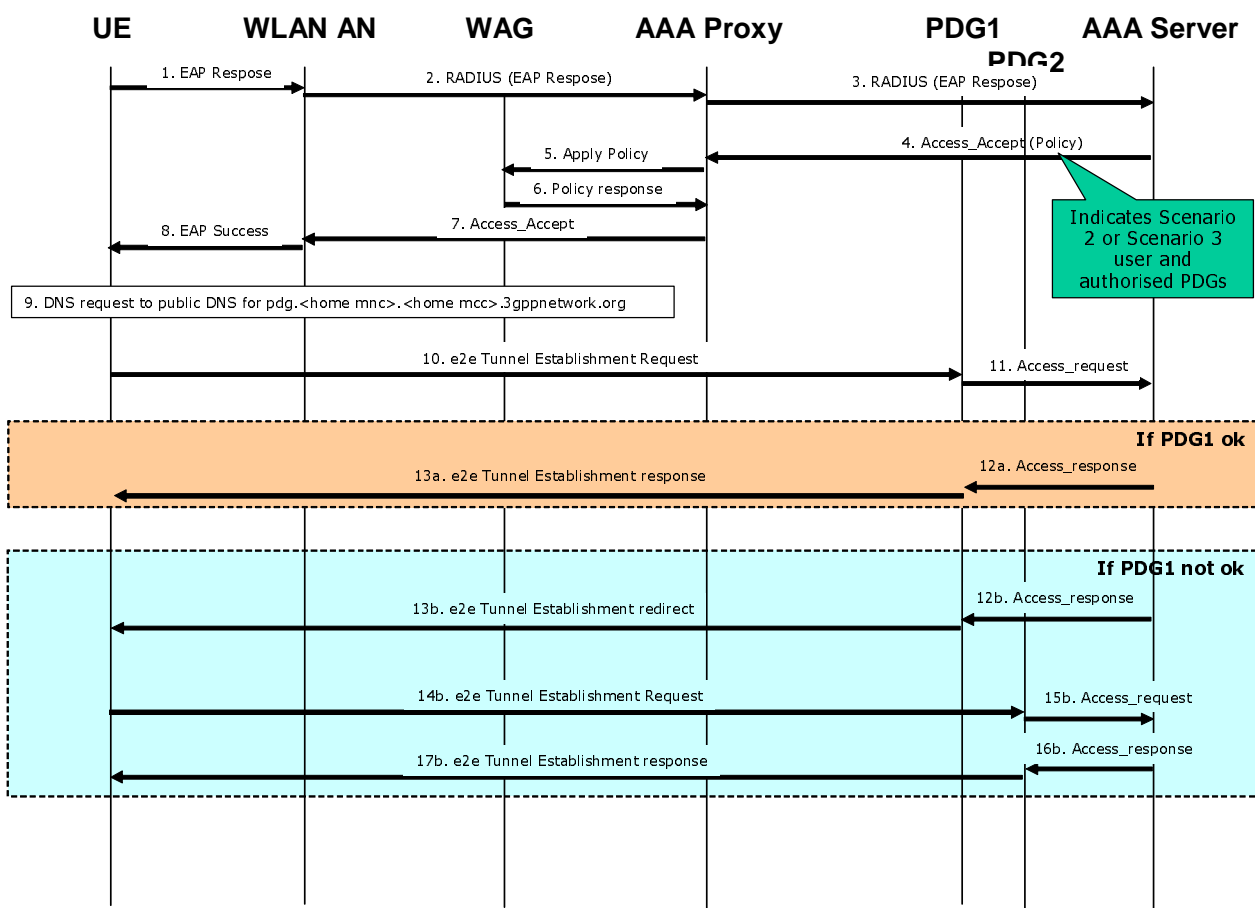


Figure E.1.1 - UE DNS client based W-APN resolution

E.1.2 WAG DNS Client

In this solution, a mechanism is required for the UE to discover the address of the WAG in the VPLMN. (This could be achieved through Public DNS, DHCP or other means).

Once the UE has obtained the address of the WAG, a new protocol may be used to send a “request for W-APN access” to the WAG. This new protocol will need to be standardised in 3GPP.

The WAG processes this request and, by reference to the Home Network AAA server, determines whether the user is authorised for this APN according to their subscription. If the user is authorised, the Home Network provides the FQDN of the PDG which should be used. The WAG performs a lookup in the 3GPP private DNS system to resolve this FQDN into an IP address for the PDG.

In order to meet Requirements 1 and 2, before this authorisation process, packets from the WLAN towards GRX are blocked by the WAG. Once the authorisation has taken place, the WAG automatically installs policy, which will allow packets to flow from the WLAN AN to the selected PDG.

Due to the possible existence of NATs in the WLAN AN, the source address of these filters must be wildcarded. This means that any authenticated UE on the WLAN can send packets to the PDG. The strength of this policing is therefore the same as in the UE DNS based approach.

This solution supports Requirement 3 because it is the Home Network which supplies the PDG address.

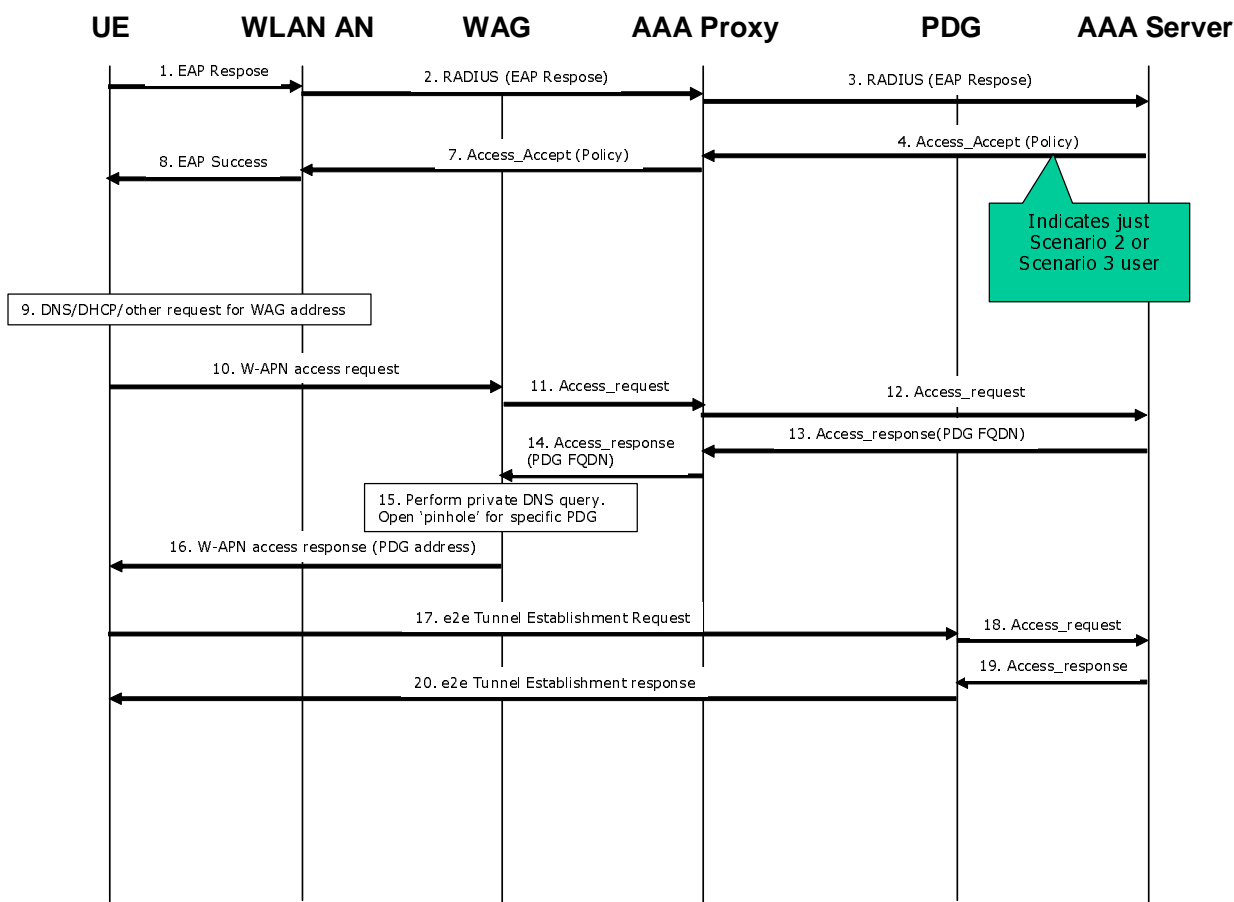


Figure E.1.2 - WAG DNS client based W-APN resolution

E.2 Visited Network Services

This section describes the enhancements to the two proposals above needed to access PDGs in the Visited network

E.2.1 Enhancements to UE DNS Client approach

There are two possibilities for providing access to visited network services with the DNS-based approach:

1. The UE contacts the HPDG first, but includes a request for visited network access if available. If visited network access is available and allowed, the UE is redirected to a VPDG
2. The UE contacts the VPDG first, but is redirected to the HPDG if visited network access is not available or allowed

In approach 1, the Home Network will need to contact the AAA Proxy in the VPLMN in order to determine whether the APN is available in the visited network and obtain the VPDG address that should be used. This is a slightly 'backwards' AAA exchange.

In approach 2, the UE will need to know the VPLMN identity. This could be obtained from the network advertisement information.

E.2.2 Enhancements to WAG DNS client approach

Visited services access is obtained in the WAG-based approach by including a request for visited access in the W-APN access request sent to the WAG. The HPLMN indicates to the VPLMN whether or not visited network access to this W-APN is allowed according to the user's subscription.

If visited network access is both allowed and available in the VPLMN, then the VPLMN AAA Proxy server constructs an FQDN for an appropriate VPDG, which is then resolved in the private DNS by the WAG as before.

Annex F (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2002-08					<i>Converted TR23.934v0.5.0 into this TS</i>	<i>0.0.0</i>	<i>0.1.0</i>
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
2003-08	SA2#34	S2-033183			Editorial clarifications; inclusion of tunnelling solution. Sent to SA for approval	1.10.0	1.14.0
2003-09	SA #21	SP-030391			Presentation to SA #21 plenary for approval	1.14.0	2.0.0