

# ETSI TS 123 234 V6.3.0 (2004-12)

---

*Technical Specification*

**Universal Mobile Telecommunications System (UMTS);  
3GPP system to Wireless Local Area Network (WLAN)  
interworking;  
System description  
(3GPP TS 23.234 version 6.3.0 Release 6)**

---



---

Reference

DTS/TSGS-0223234v630

---

Keywords

UMTS

**ETSI**

650 Route des Lucioles  
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° 7803/88

---

**Important notice**

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

[http://portal.etsi.org/chaicor/ETSI\\_support.asp](http://portal.etsi.org/chaicor/ETSI_support.asp)

---

**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.

© European Telecommunications Standards Institute 2004.  
All rights reserved.

DECT™, PLUGTESTS™ and UMTS™ are Trade Marks of ETSI registered for the benefit of its Members.  
TIPHON™ and the TIPHON logo are Trade Marks currently being registered by ETSI for the benefit of its Members.  
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

---

## Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://webapp.etsi.org/IPR/home.asp>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

---

## Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under <http://webapp.etsi.org/key/queryform.asp>.

# Contents

|   |    |
|---|----|
| Intellectual Property Rights .....  | 2  |
| Foreword.....   | 2  |
| Foreword.....   | 7  |
| 1 Scope .....   | 8  |
| 2 References .....  | 8  |
| 3 Definitions, symbols and abbreviations .....                              | 9  |
| 3.1 Definitions .....   | 9  |
| 3.2 Symbols.....  | 10 |
| 3.3 Abbreviations .....   | 10 |
| 4 WLAN Radio networks interworking with 3GPP.....                           | 11 |
| 5 High-level Requirements and Principles .....                              | 12 |
| 5.1 Access Control .....  | 12 |
| 5.1.1 WLAN Impacts.....   | 12 |
| 5.1.2 Existing 3GPP Element Impacts .....                                   | 13 |
| 5.1.3 Requirements for WLAN Direct IP Access .....                          | 13 |
| 5.1.4 Requirements for WLAN 3GPP IP Access.....                             | 13 |
| 5.1.5 WLAN Access Authorization .....                                       | 14 |
| 5.1.5 3GPP WLAN Attach .....  | 14 |
| 5.2 Void.....   | 15 |
| 5.3 User Identity.....  | 15 |
| 5.3.1 General.....  | 15 |
| 5.3.2 NAI Username .....  | 15 |
| 5.3.3 NAI Realm Name .....  | 15 |
| 5.3.4 NAI decoration for roaming.....                                       | 16 |
| 5.4 Network Advertisement and Selection .....                               | 16 |
| 5.4.1 Description of the issue.....   | 16 |
| 5.4.2 I-WLAN Access Network Advertisement and Selection.....                | 17 |
| 5.4.2.1 Case of IEEE 802.11 WLANs.....                                      | 17 |
| 5.4.2.1.1 General .....   | 17 |
| 5.4.2.1.2 WLAN Access Network Advertisement .....                           | 18 |
| 5.4.2.1.3 I-WLAN Access Network Selection .....                             | 18 |
| 5.4.2.2 Case of other WLANs.....  | 19 |
| 5.4.3 PLMN Advertisement and Selection .....                                | 19 |
| 5.4.3.1 General .....   | 19 |
| 5.4.3.2 Network Advertisement .....   | 19 |
| 5.4.3.3 Network Selection.....  | 19 |
| 5.5 Authentication methods.....   | 20 |
| 5.6 Service Authorization Principles for WLAN 3GPP IP Access .....          | 20 |
| 5.6.1 Accessing Home Network provided services .....                        | 20 |
| 5.6.2 Accessing Visited Network provided services.....                      | 20 |
| 5.6.3 External IP Network selection .....                                   | 21 |
| 5.7 IP Connectivity for WLAN 3GPP IP Access .....                           | 21 |
| 5.7.1 Principles .....  | 21 |
| 5.7.2 Tunnelling Requirements.....  | 21 |
| 5.7.3 IMS support over I-WLAN.....  | 22 |
| 5.8 Roaming requirements for WLAN 3GPP IP Access .....                      | 22 |
| 5.9 Routing Enforcement and Policy Enforcement for WLAN 3GPP IP Access..... | 23 |
| 5.9.1 Purpose for routing enforcement and policy enforcement .....          | 23 |
| 5.9.2 Routing Enforcement in the WLAN AN .....                              | 23 |
| 5.9.3 Routing enforcement and policy Enforcement in the HPLMN.....          | 23 |
| 5.9.4 Routing enforcement and policy Enforcement in the VPLMN.....          | 23 |
| 5.10 IP address allocation for the WLAN UE .....                            | 23 |
| 5.10.1 General.....   | 23 |

|          |   |    |
|----------|---|----|
| 5.10.2   | Static and Dynamic Remote IP Address .....                          | 24 |
| 5.11     | Charging .....  | 24 |
| 5.12     | AAA Protocol Requirements .....                                     | 25 |
| 6        | Interworking Architecture .....                                     | 25 |
| 6.1      | Reference Model .....   | 25 |
| 6.1.1    | Non Roaming WLAN Inter-working Reference Model .....                | 25 |
| 6.1.2    | Roaming WLAN Inter-working Reference Model .....                    | 25 |
| 6.2      | Network elements .....  | 27 |
| 6.2.1    | WLAN UE .....   | 27 |
| 6.2.1.1  | Void .....  | 28 |
| 6.2.2    | 3GPP AAA Proxy .....  | 28 |
| 6.2.3    | 3GPP AAA Server .....   | 28 |
| 6.2.4    | HLR/HSS .....   | 29 |
| 6.2.5    | WLAN Access Gateway .....   | 29 |
| 6.2.5.1  | Policy Enforcement .....  | 30 |
| 6.2.5.2  | Per-tunnel Charging Generation .....                                | 30 |
| 6.2.6    | Packet Data Gateway .....   | 30 |
| 6.2.7    | Subscription Locator Function (SLF) .....                           | 31 |
| 6.2.8    | Offline Charging System .....                                       | 32 |
| 6.2.9    | Online Charging System .....  | 32 |
| 6.3      | Reference Points .....  | 32 |
| 6.3.1    | Wa reference point .....  | 32 |
| 6.3.1.1  | General description .....   | 32 |
| 6.3.1.2  | Functionality .....   | 32 |
| 6.3.2    | Wx reference point .....  | 32 |
| 6.3.3    | D'/Gr' reference point .....  | 33 |
| 6.3.4    | Wo reference point .....  | 33 |
| 6.3.5    | Wf reference point .....  | 34 |
| 6.3.6    | Wg reference point .....  | 34 |
| 6.3.7    | Wn reference point .....  | 34 |
| 6.3.8    | Wp reference point .....  | 34 |
| 6.3.9    | Wi reference point .....  | 34 |
| 6.3.10   | Wm reference point .....  | 34 |
| 6.3.11   | Wd reference point .....  | 35 |
| 6.3.11.1 | General description .....   | 35 |
| 6.3.11.2 | Functionality .....   | 35 |
| 6.3.12   | Wu reference point .....  | 35 |
| 6.3.13   | Ww reference point .....  | 36 |
| 6.3.13.1 | General Description .....   | 36 |
| 6.3.13.2 | Functionality .....   | 36 |
| 6.3.14   | Dw reference point .....  | 36 |
| 6.3.15   | Wy reference point .....  | 36 |
| 6.3.16   | Wz reference point .....  | 36 |
| 6.4      | Protocols .....   | 36 |
| 6.4.1    | Remote IP Layer .....   | 37 |
| 6.4.2    | Tunnelling layer .....  | 37 |
| 6.4.3    | Transport IP Layer .....  | 37 |
| 6.5      | WLAN user profile .....   | 37 |
| 7        | Procedures .....  | 39 |
| 7.1      | I-WLAN and VPLMN Selection Procedure .....                          | 39 |
| 7.1.1    | Initial network selection .....                                     | 39 |
| 7.1.2    | Network re-selection .....  | 39 |
| 7.2      | WLAN Access Authentication and Authorisation .....                  | 40 |
| 7.3      | Subscriber Profile Update .....                                     | 41 |
| 7.3.0    | WLAN Direct Access Authorization information update procedure ..... | 41 |
| 7.3.1    | Access and service Authorization information update procedure ..... | 42 |
| 7.4      | Cancelling WLAN Registration .....                                  | 44 |
| 7.5      | Disconnecting a Subscriber by WLAN .....                            | 45 |
| 7.6      | Disconnecting a Subscriber by Online Charging System .....          | 46 |
| 7.6.1    | The OCS initiated WLAN AN access disconnection .....                | 46 |

|   |  |           |
|---|--|-----------|
| 7.6.2   | The OCS initiated tunnel disconnection .....   | 47        |
| 7.7   | Charging offline charged subscribers .....   | 48        |
| 7.8   | Charging online charged subscribers.....   | 49        |
| 7.9   | W-APN resolution and Tunnel establishment .....  | 50        |
| 7.9.1   | Void .....   | 52        |
| 7.9.2   | Subsequent authentication .....  | 52        |
| 7.9.3   | Use of DNS .....   | 52        |
| 7.9.4   | Subsequent tunnel establishment .....  | 52        |
| 7.10  | Tunnel disconnection procedures .....  | 52        |
| 7.10.1  | WLAN UE initiated tunnel disconnection .....   | 53        |
| 7.10.2  | The network initiated tunnel disconnection .....   | 53        |
| 7.10.3  | Disconnection of the last tunnel for a WLAN UE .....   | 54        |
| 7.11  | The WLAN UE initiated WLAN AN Access disconnection .....   | 54        |
| 7.12  | User identity to HSS resolution .....  | 55        |
| 7.12.1  | General.....   | 55        |
| 7.12.2  | SLF query .....  | 56        |
| <b>Annex A (informative): Reference Points Signalling Flows.....</b>                            |  | <b>57</b> |
| A.1   | Signalling Sequences examples for Wa Reference Point .....   | 57        |
| A.1.1   | Authentication, Authorisation and Session Key delivery .....   | 57        |
| A.1.2   | Immediate purging of a user from the WLAN access.....  | 58        |
| A.2   | Signalling Sequences examples for Wx Reference Point .....   | 59        |
| A.2.1   | Authentication Information Retrieval .....   | 59        |
| A.2.2   | Subscriber Profile Retrieval .....   | 59        |
| A.2.3   | Subscriber Profile Update.....   | 60        |
| A.2.4   | WLAN Registration.....   | 61        |
| A.2.5   | Cancel Registration.....   | 62        |
| A.2.6   | Purge Function for WLAN interworking.....  | 63        |
| A.3   | Signalling Sequences examples for D' Reference Point .....   | 63        |
| A.3.1   | Authentication Information Retrieval .....   | 63        |
| A.3.2   | Subscriber Profile Retrieval .....   | 64        |
| A.4   | Gr' Signalling Mechanisms to support WLAN service .....  | 64        |
| A.4.1   | Introduction.....  | 64        |
| A.4.2   | InfoRetrieval procedure: .....   | 65        |
| A.4.2   | GprsLocationUpdate procedure: .....  | 65        |
| A.5   | Example of Authentication procedures .....   | 66        |
| A.5.1   | EAP/AKA Procedure.....   | 66        |
| A.5.2   | EAP SIM procedure.....   | 69        |
| A.5.3   | Alternative EAP initialisation .....   | 72        |
| A.5.4   | Re-authentication message sequence chart .....   | 73        |
| <b>Annex B (informative): WLAN radio technologies .....</b>                                     |  | <b>75</b> |
| <b>Annex C (informative): Possible interworking architectures between WLAN AN and PLMN.....</b> |  | <b>76</b> |
| C.1   | WLAN shared by (or connected to) multiple ISPs and PLMNs.....  | 76        |
| C.2   | Routing packets from WLAN UE when WLAN AN is connected to multiple VPLMNs/ISPs and it provides direct Internet access..... | 76        |
| C.2.1   | Separating traffic for different VPLMNs.....   | 76        |
| C.2.2   | Routing the traffic.....   | 77        |
| C.2.3   | Separating traffic to different VPLMNs using a combined DNS/NAT approach.....  | 78        |
| C.3   | WLAN AN exclusively owned by and connected to a single PLMN .....  | 80        |
| C.4   | WLAN AN connected to a single ISP .....  | 80        |
| <b>Annex D (normative): Short Message Service .....</b>   |  | <b>81</b> |
| D.1   | Architecture for support of SMS .....  | 81        |
| D.1.1   | IP Short Message Gateway (IP-SM-GW).....   | 81        |
| D.1.2   | HLR/HSS .....  | 82        |
| D.1.2.1   | Indication that the terminal is registered with an IP Short Message gateway .....  | 82        |
| D.1.2.2   | The address of the IP-SM-GW .....  | 82        |
| D.1.3   | Reference points .....   | 82        |
| D.2   | Procedures .....   | 82        |
| D.2.1   | Registration with IP Short Message Gateway.....  | 82        |

|  |   |           |
|--|---|-----------|
| D.2.1.1  | General .....   | 82        |
| D.2.1.2  | Information flows for registration .....                              | 83        |
| D.2.2  | De-registration from the IP Short Message Gateway .....               | 83        |
| D.2.2.1  | General .....   | 83        |
| D.2.2.2  | Information flows for UE-initiated de-registration .....              | 83        |
| D.2.2.3  | Information flows for automatic de-registration .....                 | 83        |
| D.2.3  | Delivery of short messages .....                                      | 83        |
| D.2.3.1  | Message Information flows for IP terminated short messages .....      | 83        |
| D.2.4  | Short message origination.....  | 84        |
| D.2.4.1  | Message Information flow for IP originated short messages .....       | 84        |
| D.3  | Support of SMS over WLAN interworking.....                            | 85        |
| <b>Annex E (informative): Information on the discussed tunnel switching alternative.....</b>     |   | <b>86</b> |
| E.1  | Non Roaming WLAN Inter-working Reference Model .....                  | 86        |
| E.2  | Roaming WLAN Inter-working Reference Model.....                       | 86        |
| E.3  | WAG Description.....  | 87        |
| E.4  | Wu Reference Point.....   | 87        |
| E.5  | Wn Reference Point.....   | 88        |
| E.6  | Wp Reference Point.....   | 88        |
| <b>Annex F (normative): Information on re-using the GGSN to implement the PDG function .....</b> |   | <b>89</b> |
| F.1  | Introduction .....  | 89        |
| F.2  | Mapping between E2E tunnel and GTP tunnel .....                       | 89        |
| F.3  | Gn' considerations .....  | 90        |
| F.3.0  | General.....  | 90        |
| F.3.1  | Interworking procedure over Gn" - Tunnel establishment procedure..... | 91        |
| F.3.2  | Interworking procedure over Gn" - Tunnel disconnection procedure..... | 92        |
| F.3.2.1  | UE initiated tunnel disconnection .....                               | 92        |
| F.3.2.2  | Network initiated tunnel disconnection.....                           | 93        |
| F.4  | Void.....   | 93        |
| F.5  | Tunnel Terminating Gateway (TTG) functionality .....                  | 93        |
| <b>Annex G (informative): Consideration on supporting IMS over I-WLAN .....</b>                  |   | <b>95</b> |
| <b>Annex H (informative): Change history .....</b>   |   | <b>96</b> |
| History .....  |   | 98        |

---

## Foreword

This Technical Specification has been produced by the 3<sup>rd</sup> Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.



---

# 1 Scope

This document specifies system description for interworking between 3GPP systems and WLAN Local Area Networks (WLANs). The intent of 3GPP-WLAN Interworking is to extend 3GPP services and functionality to the WLAN access environment. The 3GPP-WLAN Interworking System provides bearer services allowing a 3GPP subscriber to use a WLAN to access 3GPP PS based services.

This specification defines a 3GPP system architecture and procedures to do the following:

- Provide Access, Authentication and Authorisation (AAA) services to the 3GPP-WLAN Interworking System based on subscription.
- Provide access to the locally connected IP network (e.g. the Internet) if allowed by subscription.
- Provide WLAN UEs with IP bearer capability to the operator's network and PS Services, if allowed by subscription.

---

# 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] void

[2] void

[3] void

[4] void

[5] 3GPP TS 23.003: "Numbering, addressing and identification".

[6] 3GPP TS 23.040: "Technical Realisation of the Short Message Service (SMS)".

[7] 3GPP TS 23.060: "GPRS; Service description".

[8] void

[9] 3GPP TS 24.234: "3GPP System to WLAN Interworking; UE to Network protocols; Stage 3".

[10] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[11] void

[12] 3GPP TS 31.102: "Characteristics of the USIM Application."

[13] 3GPP TS 32.225: "Telecommunication management; Charging management; Charging data description for the IP Multimedia Subsystem (IMS)."

[14] 3GPP TS 33.234: "WLAN Interworking Security."

[15] 3GPP TS 23.125: "Overall High Level Functionality and Architecture Impacts of Flow Based Charging"

[16] void

- [17] RFC 2486: "The Network Access Identifier"
- [18] void
- [19] IEEE Std 802.1X-2001 IEEE Standard for Local and metropolitan area networks— Port-Based Network Access Control
- [20] IETF Internet-Draft: "Network Discovery and Selection within the EAP Framework". draft-adrangi-eap-network-discovery-and-selection-03, work in progress.
- [21] IEEE Std 802.11-1999, Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, IEEE, Sep. 1999.
- [22] IETF Internet-Draft: "EAP AKA Authentication" draft-arkko-pppext-eap-aka-12 (April 2004).
- [23] IETF Internet-Draft: "EAP SIM Authentication" draft-haverinen-pppext-eap-sim-13 (April 2004).
- [24] 3GPP TS 23.228: " IP Multimedia Subsystem (IMS); Stage 2".
- [25] 3GPP TS 22.234: "Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking".
- [26] 3GPP TS 32.252: "Telecommunication management; Charging management; Wireless Local Area Network (WLAN) charging".
- [27] 3GPP TS 32.296: "Telecommunication management; Charging management; Online Charging System (OCS) applications and interfaces".
- [28] 3GPP TS 29.060: "GPRS; GTP across the Gn and Gp interface".

---

## 3 Definitions, symbols and abbreviations

### 3.1 Definitions

**Available SSID:** An SSID that the WLAN UE has found after active and/or passive scanning which meets certain conditions as specified in IEEE 802.11 [19].

**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.

**External IP Network/External Packet Data Network:** An IP or Packet Data network with access provided by the 3GPP – WLAN Interworking, rather than directly from the WLAN AN.

**Home WLAN:** A WLAN which interworks with the HPLMN without using a VPLMN.

**Interworking WLAN (I-WLAN) :** A WLAN that interworks with a 3GPP system.

**I-WLAN selection:** Procedure to select a specific I-WLAN from the available I-WLANs.

**Local Service Identifier:** An identifier used within the 3GPP system for a service available directly from the I-WLAN, for example Internet access or access to a specific corporate network.

**Offline charging:** Mechanism for collecting and forwarding charging information concerning I- WLAN and core network resource usage without affecting the service rendered in real-time.

**Online charging:** Mechanism for collecting and forwarding charging information concerning I- WLAN and core network resource usage where the service may be affected in real-time.

**Policy Enforcement:** Functionality implemented in a WAG to ensure packets coming from or going to the WLAN AN are allowed based on unencrypted data within the packets. (e.g., source and destination IP address and port number)

**PS based services:** General term to refer to the services provided by a PLMN using the IP bearer capability between a WLAN UEs and the PLMN when WLAN 3GPP IP Access is used. Examples include bearer services such as Internet access, and Corporate IP network access and higher level services such as SMS and LCS.

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

**Routing Enforcement:** Routing Enforcement ensures all packets sent to/from the WLAN UE for 3G PS based service are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case). Routing Enforcement is implemented between a WLAN AN and a WAG.

**Selected W-APN:** The W-APN selected by the network as a result of the **WLAN -UE** subscriber request.

**Service Authorization:** Authorization allowing a subscriber to access the requested service based on subscription.

**Tunnel Identifier:** Identifier of a tunnel between a WLAN UE and a PDG. It is contained in the unencrypted part of a packet.

**User Identifier:** Identifier of a user which may be used, for example, in charging functionality

**WLAN Access Point Name (W-APN):** Is used to identify a specific IP network and a point of interconnection to that network (Packet Data Gateway)

**WLAN 3GPP IP Access:** Access to an IP network via a PLMN via a tunnel. A related term is WLAN 3GPP Direct IP Access.

**WLAN coverage:** The area where a WLAN UE can connect to a WLAN.

**WLAN Direct IP Access:** Access to an IP network directly from a WLAN AN without passing data to a PLMN via a tunnel. A related term is WLAN 3GPP IP Access.

**WLAN UE's local IP address:** The address used to deliver a packet to a WLAN UE in a WLAN AN. It identifies the WLAN UE in the WLAN AN. The WLAN UE's local IP address may be translated by a Network Address Translation prior to being received by any other IP network, including a PLMN.

**WLAN UE's remote IP address:** The address used by the data packet encapsulated inside the WLAN UE to PDG tunnel. It represents the address of the WLAN UE in the network which the WLAN UE is accessing via the PDG.

## 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  |
| Dw  | Reference point between a 3GPP AAA Server and an SLF  |
| Gr' | Reference point between a pre-R6 HSS/HLR and a 3GPP AAA Server  |
| Wa  | Reference point between a WLAN Access Network and a 3GPP AAA Server/Proxy (charging and control signalling) |
| Wd  | Reference point between a 3GPP AAA Proxy and a 3GPP AAA Server (charging and control signalling)            |
| Wf  | Reference point between an Offline Charging System and a 3GPP AAA Server/Proxy                              |
| Wg  | Reference point between a 3GPP AAA Server/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 or 3GPP AAA proxy                       |
| 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  |
| Wu  | Reference point between a WLAN UE and a Packet Data Gateway   |
| Wx  | Reference point between an HSS and a 3GPP AAA Server  |
| Wy  | Reference point between a PDG and an OCS  |
| Wz  | Reference point between a PDG and an Offline Charging System  |

## 3.3 Abbreviations

|     |  |
|-----|--|
| AAA | Authentication, Authorisation and Accounting |
| ACL | Access Control List                          |

|          |   |
|----------|---|
| AKA      | Authentication and Key Agreement                  |
| AP       | Access Point                                      |
| APN      | Access Point Name                                 |
| DHCP     | Dynamic Host Configuration Protocol               |
| DNS      | Domain Name System                                |
| EAP      | Extensible Authentication Protocol                |
| FQDN     | Fully Qualified Domain Name                       |
| GGSN     | Gateway GPRS Support Node                         |
| GTP      | GPRS Tunnelling Protocol                          |
| HLR      | Home Location Register                            |
| HPLMN    | Home PLMN   |
| HSS      | Home Subscriber Server                            |
| IEEE     | Institute of Electrical and Electronics Engineers |
| IP       | Internet Protocol                                 |
| IP-SM-GW | IP Short Message Gateway                          |
| ISP      | Internet Service Provider                         |
| I-WLAN   | Interworking WLAN                                 |
| NAI      | Network Access Identifier                         |
| NAT      | Network Address Translation                       |
| OCS      | Online Charging System                            |
| PDA      | Personal Digital Assistant                        |
| PDG      | Packet Data Gateway                               |
| PLMN     | Public Land Mobile Network                        |
| SIM      | Subscriber Identity Module                        |
| SSID     | Service Set ID                                    |
| VLAN     | Virtual Local Area Network                        |
| UE       | User Equipment                                    |
| UMTS     | Universal Mobile Telecommunications System        |
| USIM     | UMTS SIM  |
| SSID     | Service Set Identifier                            |
| VPLMN    | Visited PLMN                                      |
| 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:

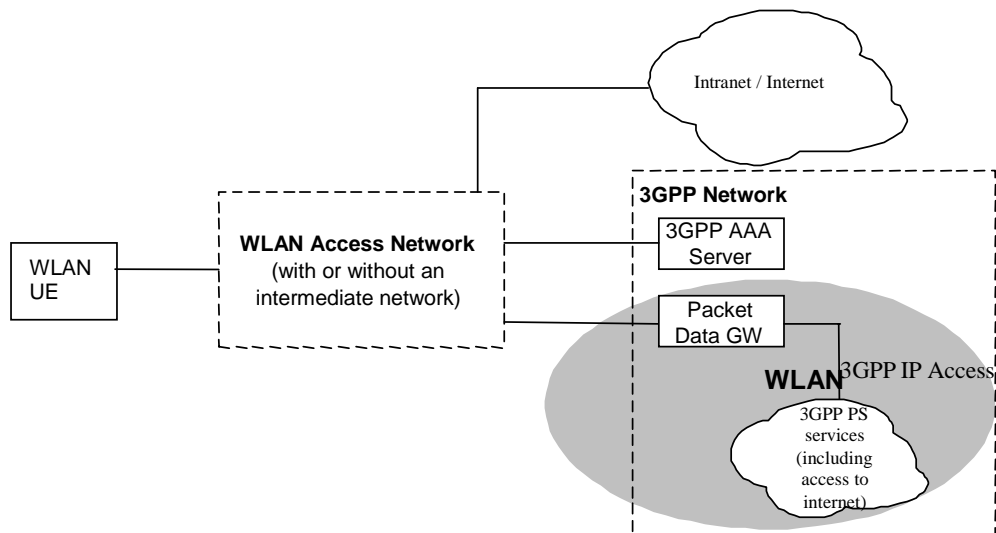
- WLAN Access, Authentication and Authorisation, which provides for access to the WLAN and the locally connected IP network (e.g. Internet) to be authenticated and authorised through the 3GPP System. Access to a locally connected IP network from the WLAN, is referred to as WLAN Direct IP Access.
- WLAN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

WLAN 3GPP IP Access should, as far as possible, be technically independent of WLAN Access Authentication and Authorisation. However, WLAN 3GPP IP 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 WLAN GPP IP Access may rely on information derived in the procedure for WLAN Access Authorization.

Figure 4.1 illustrates WLAN networks from the point of view of 3GPP interworking.

The Packet Data Gateway supports WLAN 3GPP IP Access to External IP networks. 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 WLAN 3GPP IP Access 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

Access Control is the capability to permit or deny a subscriber the use of a resource, in this case the WLAN and/or the interworking to the 3GPP system. The following functional requirements and principles have guided the development of this standard with regard to Access Control.

#### 5.1.1 WLAN Impacts

The following requirements should be satisfied by the WLAN 3GPP Interworking function with regard to the WLAN itself:

- Legacy WLAN terminals should be supported. However software upgrades may be required for e.g. to access a (U)SIM.
- Existing client hardware and software should be used where ever possible
- Minimal impact on existing WLAN networks.
- The need for operators to administer and maintain WLAN UE software shall be minimized.
- Methods for key distribution to the WLAN access network to allow secure tunnels to be established shall be supported. Note: This does not mean Wireless Equivalent Privacy (WEP) keys in the case of a 802.11 network.
- WLAN Access Authorization shall occur upon the success of the authentication procedure. It may take into account the user's subscription profile and optionally information about the WLAN AN, such as WLAN AN operator name, WLAN AN location information (e.g., country, telephone area code, city), WLAN AN throughput (e.g., maximum and minimum bandwidth guarantees for both ingress and egress traffic).

- Results of WLAN Access Authorization requests shall be indicated to the WLAN, so that the WLAN can take appropriate action.
- It shall be possible to indicate to the user of the results of authorization requests.
- The WLAN Access Authorization mechanism shall be able change service provisioning dynamically, and inform the user and WLAN of any change.
- **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.

### 5.1.2 Existing 3GPP Element Impacts

The following requirements should be satisfied by the 3GPP-WLAN Interworking System function with regard to existing 3GPP network elements:

- 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.
- The Service Location Function (SLF) node shall be used in the same way as defined in 3GPP TS 23.228 [24] to find the address of a subscriber's HSS, if necessary.
- 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. (e.g. the HLRSS shall not deregister a PS subscriber when the UE registers on a WLAN)
- This TS proposes solutions for operators who want to interwork their WLAN with an existing pre-R6 HLR/HSS. Please refer to Annex A.

### 5.1.3 Requirements for WLAN Direct IP Access

The following requirements should be satisfied by the WLAN 3GPP-WLAN Interworking function with regard to allowing direct access to the IP network to which the WLAN is connected (e.g. the Internet):

- A WLAN supporting both WLAN Direct IP Access and WLAN 3GPP IP Access shall be able to support a WLAN UE operating in the WLAN Direct IP Access mode only, e.g. according to subscription.

### 5.1.4 Requirements for WLAN 3GPP IP Access

The following requirements should be satisfied by the WLAN 3GPP-WLAN Interworking function with regard to allowing access to a WLAN 3GPP IP network (e.g. the operator's intranet which allows IMS access):

- Service Authorization for 3GPP services shall occur after successful Authentication.
- It shall be possible to use Service Based Policy Control.
- Access to 3GPP PS based services shall be provided via WLAN. The interworking architecture shall be able to support all 3GPP PS based services.
- Quality of Service shall be supported when accessing these services via WLAN, although some limitations may exist because of the WLAN AN.
- A combined access capable user with the subscription for both services should be able to choose between "WLAN Direct IP Access only" or "WLAN 3GPP IP Access".

The WLAN UE shall be able to detect if a 3GPP-WLAN does not support access to 3GPP PS based services.

- Data flows must be able to be routed to the HPLMN or the VPLMN, e.g. according to subscription. The enforcement of this routing shall not rely on the WLAN UE client.

Note: This routing enforcement may require additional functionality in the WLAN AN

- **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. Details of End-to-End Authentication is covered in 3GPP TS 33.234 [10].
- **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. If a user chooses to access the Internet directly using the local IP network, no service selection information is passed to the PLMN. In all other cases, where WLAN 3GPP IP Access is desired, the service selection information shall contain the name of the 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 PDG. The PDG shall then seek authentication/authorisation from the 3GPP AAA Proxy or Server in the same network.
- The results of the authorisation decision shall be communicated to the Visited Network. All subscription-based authorisation decisions are made in the Home network.
- In the case of a request for access to services provided in the Visited Network, the 3GPP AAA Proxy shall also authorise access based on local policy.

### 5.1.5 WLAN Access Authorization

WLAN Access Authorization 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 stage after 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, local agreements or information about the WLAN AN.

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, or other methods.

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.

### 5.1.5 3GPP WLAN Attach

3GPP WLAN attach status indicates whether the WLAN UE is now being served by the 3GPP-WLAN Interworking System.

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 3GPP 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 3GPP 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.

## 5.2 Void

## 5.3 User Identity

### 5.3.1 General

The network authentication procedure is based on the use of EAP method where user identification is based on Network Access Identifier (NAI), whose format is specified in RFC 2486 [17]. A NAI is composed of a username part and a realm part. In the following, the term of "identity" includes both the NAI username part and the realm part, while the term of "username" only refers to the NAI username part.

### 5.3.2 NAI Username

The NAI username part format shall comply with IETF EAP-SIM [23] and EAP-AKA [22]. Three types of usernames are,

1. a Permanent username,
2. a Pseudonym username
3. a Fast re-authentication username.

Both of the Pseudonym and the Fast re-authentication usernames are used in temporary identities, but the purpose and usage of them are different. The first two types of usernames are only used on full authentication and the last one only on fast re-authentication.

The Permanent username, which is specified in IETF EAP-SIM [23] and EAP-AKA [22], shall be derived from IMSI, which resides in the UICC. Details of these are covered in 3GPP TS 33.234 [14], 3GPP TS 24.234 [9] and 3GPP TS 23.003 [5].

The Pseudonym username is used for user identity protection. The use of the Pseudonym username is necessary to replace the Permanent username derived from IMSI in radio transmissions, so that it protects the user against tracing from unauthorized access networks.

The Fast re-authentication username is used in fast re-authentication. It also provides user identity protection. For the fast re-authentication, a WLAN UE shall use the previously allocated Fast re-authentication identity as specified in the IETF EAP-SIM [23] and EAP-AKA [22] Internet-Drafts

Temporary identities (pseudonyms and fast re-authentication identities) are allocated by the 3GPP AAA Server. The format and the procedure for deriving the temporary identities are defined in TS 33.234 [14].

### 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 and shall identify the user's HPLMN, based on its MCC and MNC. Details on NAI realm construction are specified in 3GPP TS 23.003 [5].



### 5.3.4 NAI decoration for roaming

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 details on Roaming NAI construction are specified in 3GPP TS 23.003 [5].

## 5.4 Network Advertisement and Selection

### 5.4.1 Description of the issue

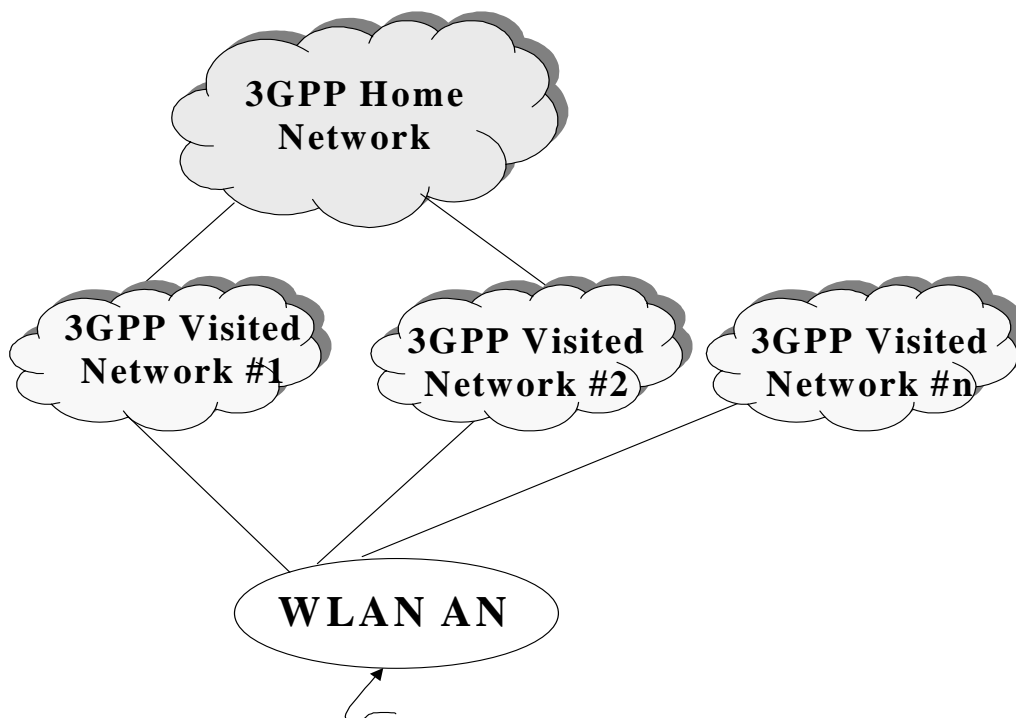
If the WLAN radio technology allows for features enabling radio access network sharing or provider selection these shall be reused for WLAN Access Network (WLAN AN) selection in 3GPP-WLAN interworking.

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.

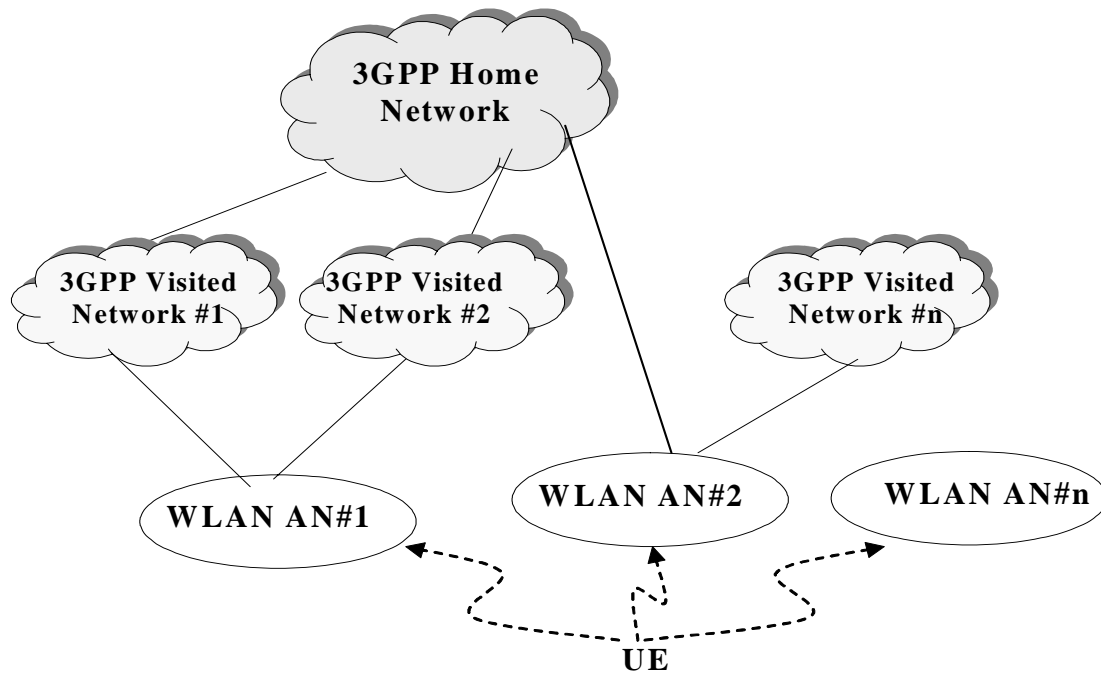
The generic Network Advertising and Selection scenario is illustrated in Figures 5.1 and 5.2.



**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 WLAN 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 I-WLAN Access Network Advertisement and Selection

### 5.4.2.1 Case of IEEE 802.11 WLANs

#### 5.4.2.1.1 General

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.
- The WLAN UE should be able to select the I-WLAN Access Network supporting the preferred PLMN.

In the case of IEEE 802.11 WLANs:

- Modification of current broadcast SSIDs shall not be required;
- Active scanning should be supported by the WLAN UE;
- Passive scanning shall be supported by the WLAN UE;
- Multiple SSIDs may be supported (i.e. only standard 802.11 capable APs are required).

#### 5.4.2.1.2 WLAN Access Network Advertisement

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. Active and passive scanning are defined in IEEE 802.11 [21].

A WLAN AN may indicate that it provides 3G interworking without the involvement of any other network than the WLAN AN.

The above requirement may be met through explicit EAP-based procedures or through the generic Preferred SSID list procedures – for example Preferred SSID lists could include SSID formats defined by operators for the above purposes.

#### 5.4.2.1.3 I-WLAN Access Network Selection

For purpose of selecting the preferred I-WLAN AN the WLAN UE may contain lists of I-WLAN identities' preferences. One list will contain the SSIDs preferred by the Home Network operator and one list contains the SSID's preferred by the user.

The Operator's preferred SSID list would be populated, for example, with the SSIDs commonly used by major hotspot operators with whom the Home Operator has a direct or indirect (through VPLMN in a roaming case) relationship.

There are two modes in network selection, i.e. Manual mode and automatic mode.

##### **Manual mode**

In the manual mode, the WLAN UE shall try to find all available SSIDs through passive scanning and/or active scanning (when it is supported).

Once a list of all available SSIDs has been obtained, it shall be possible for the WLAN UE to obtain a list of all available PLMNs from each SSID. When a list of PLMNs has been obtained from all SSIDs it shall present them to the user to select one. The WLAN UE shall then associate with the SSID that supports the PLMN that is selected by the user.

##### **Automatic Mode**

In the automatic mode the procedure is as follows:

0. The WLAN UE scans for all available SSID using passive scan and/or active scans. If the WLAN UE contains the I-WLAN identities' preference lists, the scan should be done in the order of these lists. It is not required to continue the scanning after the highest priority SSID is found.
1. Start association and perform Network Discovery. When there is more than one available SSID and the WLAN UE contains I-WLAN identities' preference lists, the association shall be done in the order of these lists.

1a) If authentication to HPLMN succeeds (i.e. EAP-Success is received), then stop this procedure.

1b) If Network Advertisement information is received (i.e. EAP-Identity/Request is received), then store the list and start again step 1.

Repeat step 1 for all available SSIDs. If the scanning in step 0 was stopped due to the discovery of the highest priority SSID, but the HPLMN has not been found (e.g. because the SSID list is not updated or the selected SSID was a fake one), then the user should go back to step 0 and scan for all remaining SSIDs.

Note that if an AP supporting HPLMN is found in the middle of the procedure, step 1a, then step 1 is stopped and association with the remaining available APs will not take place.

2. Use the lists of "User Controlled PLMN Selector list for I-WLAN" and "Operator Controlled PLMN Selector list for I-WLAN" and the lists from step 1b) to select the best matching PLMN. Note that the "User Controlled PLMN Selector list for I-WLAN" has higher priority than the "Operator Controlled PLMN Selector list for I-WLAN". Then select the I-WLAN AN that supports the best match PLMN. If more than one I-WLAN AN supports the best matched PLMN, the I-WLAN AN having the highest priority SSID is selected, if "I-WLAN identities' preference lists are available.

3. Associate with the AP selected in step 2 and attempt authentication with the best match PLMN. A WLAN AN may indicate that it provides 3G interworking without the involvement of any other network than the WLAN AN.

If such an indication is provided by the WLAN AN and if the WLAN UE supports the indication, then the WLAN UE shall use it at SSID selection as defined in 3GPP TS 24.234 [9].

The above requirement may be met through explicit EAP-based procedures or through the generic "I-WLAN identities" preference lists procedures – for example I-WLAN identities preference lists could include SSID formats defined by operators for the above purposes.

#### 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 PLMN Advertisement and Selection

#### 5.4.3.1 General

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

- This procedure takes place after association with an AP
- 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.

#### 5.4.3.2 Network Advertisement

Network advertisement information enumerates the roaming partners and associated NAI realms. This information shall be provided to the WLAN UE when the WLAN is unable to route an authentication request from the WLAN UE based on the initial NAI (e.g. when the WLAN AN receives a NAI with an unknown realm) and when the WLAN UE explicitly requests Network advertisement information. The network advertisement information is returned from the first hop AAA functionality. The first hop AAA functionality may be located either in the WLAN AN or in the PLMN in case no AAA functionality is in the WLAN AN. The provisioning of this AAA functionality is an implementation issue and does not put new requirements on 3GPP AAA Proxy/Server. Details on the usage and coding of Network advertisement information are included in 3GPP TS 24.234 [9].

#### 5.4.3.3 Network Selection

The automatic and manual mode PLMN selection procedures are defined in 3GPP TS 22.234 [25]. The detailed procedure in case of IEEE 802.11 WLAN is described in 5.4.2.

The WLAN UE shall indicate its home network through the use of an initial NAI. The realm part of this initial NAI shall be derived from the IMSI, as described in section 5.3.3. Optionally, if there is preference for a roaming network, the initial NAI then takes the form of a Roaming NAI, as described in section 5.3.4; e.g., for optimizing user access experience in re-access case, the WLAN UE may include information of preferred roaming network from previous successful authentication while it is associated to the same AP.

For the manual selection case allowed by some operator, initial NAI can include the roaming network decided by the user, e.g. using a preferred PLMN list stored in the UICC.

If the WLAN AN is able to route authentication request based on the initial NAI, then no special processing for network advertisement/selection is needed.

If the WLAN AN is unable to route authentication request from WLAN UE based on the initial NAI, 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 and VPLMN selection is performed, the WLAN UE attempts to authenticate with the new NAI determined in the prior step.

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

## 5.5 Authentication methods

Authentication methods are discussed in TS 33.234 [14].

## 5.6 Service Authorization Principles for WLAN 3GPP IP Access

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 successful authentication.
- 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 to the PDGs used for access to external IP networks.
- It shall be possible to permit access to different services simultaneously.
- It shall be possible to provide IP related configuration parameters to the WLAN UE during or after successful service authorisation. These configuration parameters may include e.g. the WLAN UE's remote IP address and addresses of DHCP and DNS servers in the HPLMN.
- 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 based on the requested W-APN and subscription information retrieved from the HSS/HLR, which includes e.g. the subscribed W-APNs).
  - 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 shall be performed under control of the 3GPP Home Network by means of answers to DNS queries for the requested W-APN. The selection is based on the requested W-APN and user subscription information. The WLAN UE shall choose an IP address of the PDG, if there is more than one PDG address in the answer to the DNS queries.

The mechanism to select the PDG by the home network is out of scope of this specification, since it depends on the operator's preference.
- The PDG needs to know the authorized W-APN to select the external network, i.e. Wi interface.

### 5.6.2 Accessing Visited Network provided services

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

- In order for the WLAN 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 shall be under control of the 3GPP Visited Network by means of answers to DNS query for the requested W-APN. The selection is based on the authorized W-APN and service related information. The WLAN UE shall choose the IP address of the PDG if there is more than one PDG address in the answer to DNS query.

The mechanism to select the V-PDG by the Visited Network is out of scope of this specification, since it depends on the operator's preference.

- The selected PDG in the Visited Network needs to know the authorized W-APN to select the external network, i.e. Wi interface.
- It shall be possible to provide IP related configuration parameters to the WLAN UE during or after successful service authorisation. These configuration parameters may include e.g. the WLAN UE's remote IP address and addresses of DHCP and DNS servers in the VPLMN.

### 5.6.3 External IP Network selection

The WLAN UE can connect to different External IP networks, such as the Internet, an operator's IP network or 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 a PDG. It is then forwarded to the 3GPP AAA server/proxy in the same network as the PDG.

## 5.7 IP Connectivity for WLAN 3GPP IP Access

### 5.7.1 Principles

The WLAN UE initiates the establishment of tunnels and is involved in packet encapsulation/decapsulation. The tunnel shall reside between the WLAN UE and the PDG. In the non roaming case, the PDG shall reside in the Home PLMN; in the roaming case, the PDG may reside 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 procedures described in clause 7.9.
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 Wa reference point. The WLAN Access Network 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 tunnelling 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 Access Network
- 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):
  - The tunnel protocol shall be able to support IPv4 and IPv6 transport addresses
  - The tunnel protocol shall support private WLAN UE's local IP addresses, which are non-routable in the public Internet.
- The protocol should be fully specified and 3GPP should define its usage to enable multi-vendor inter-operability.

### 5.7.3 IMS support over I-WLAN

IMS over I-WLAN in this release is supported without charging correlation and QoS support, i.e. SBLP for I-WLAN is not supported.

See Annex G about alternatives of implementing these functions for IMS over I-WLAN.

## 5.8 Roaming requirements for WLAN 3GPP IP Access

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 Home/Visited 3GPP network conforms to QoS and roaming agreement(s).
- The roaming architecture shall provide the ability to allow the user to access services provided by the visited network, e.g. local PS services.
- The roaming architecture shall allow the home network to limit the set of 3GPP services available for a given roaming user.
- All packets of PS based services sent to/from a WLAN UE are routed via a VPLMN in a 3GPP network; however basic Internet access may be routed directly from the WLAN.

## 5.9 Routing Enforcement and Policy Enforcement for WLAN 3GPP IP Access

### 5.9.1 Purpose for routing enforcement and policy enforcement

In order to ensure operator policies, e.g. QoS, Charging can be applied to user traffic, WLAN 3GPP IP Access requires routing enforcement and 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 based service are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case). However, this routing enforcement shall not prevent a WLAN AN from routing non 3G PS based service traffic to another network (e.g. the Internet) other than a PLMN, when provision of such services (e.g. direct Internet access from the WLAN) is agreed between the WLAN and the PLMN.

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

If a WLAN UE user subscription allows a WLAN Direct IP Access the WLAN AN should be capable of routing packets directly to the external packet data network.

Routing enforcement in the WLAN AN shall ensure that packets sent between a PDG and a WLAN UE 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 a WLAN Direct IP Access only capable WLAN UE or a WLAN 3GPP IP Access capable WLAN UE opting for a WLAN Direct IP Access, and non 3G interworking WLAN terminals. Routing enforcement should have minimal impact on the WLAN AN.

### 5.9.3 Routing enforcement and policy Enforcement in the HPLMN

When supporting WLAN 3GPP IP Access and access is via a tunnel endpoint (PDG) in the HPLMN, the HPLMN shall be able to provide the VPLMN with suitable policy enforcement information. The HPLMN may also provide suitable routing enforcement information to WLAN.

### 5.9.4 Routing enforcement and policy Enforcement in the VPLMN

When supporting WLAN 3GPP IP Access, 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 information to WLAN.

## 5.10 IP address allocation for the WLAN UE

### 5.10.1 General

When using WLAN Direct IP Access, a WLAN UE needs to use its local IP address only. When using WLAN 3GPP IP Access, a WLAN UE shall use two IP addresses; its local IP address and remote IP address.

A WLAN UE's local IP address identifies the WLAN UE in the WLAN AN. In systems supporting only WLAN Direct IP Access, the WLAN UE's local IP address is assigned by the WLAN AN; in a WLAN 3GPP IP Access enabled system, 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.

When using WLAN 3GPP IP Access, a WLAN UE's remote IP address identifies the WLAN UE in the network that the WLAN UE is accessing for the 3G PS service. It shall be used for the inner packet of the WLAN UE-initiated tunnel. It



can be assigned by HPLMN, VPLMN or an external IP network. The remote IP address can be statically or dynamically assigned. The only case where VPLMN assigns the remote IP address for the WLAN UE is when the WLAN 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. For the WLAN UE's remote IP address, IPv4 addresses shall be supported. When the WLAN UE accesses 3G PS based services using an IPv6 network such as IMS services, IPv6 addresses shall be supported for the WLAN UE's remote IP address. To avoid any clashes between addresses used in WLAN AN and PLMN and to enable correct routing of packets sent out by the WLAN UE the PLMN operator should allocate public addresses to network nodes, which are addressed by WLAN UEs.

When a WLAN UE accesses several 3G PS based services with different W-APNs simultaneously, the WLAN UE can get several remote IP addresses. There may be several WLAN UE-initiated tunnels for the services.

## 5.10.2 Static and Dynamic Remote IP Address

Remote IP address can be allocated to a WLAN UE in four different ways:

- The HPLMN operator assigns a Remote IP address permanently to the WLAN UE (static remote IP address).
- The HPLMN operator assigns a Remote IP address to the WLAN UE when the tunnel is established to the PDG in the home network (dynamic HPLMN remote IP address).
- The VPLMN operator assigns a Remote IP address to the WLAN UE when the tunnel is established to the PDG in the visited network (dynamic VPLMN remote IP address).
- The external IP network operator assigns a permanent or dynamic Remote IP address to the WLAN UE (external Remote IP address allocation).

It is the HPLMN operator that defines in the subscription whether static IP address allocation is used.

When static IP address allocation is used, a WLAN UE either can include its static IP address in the tunnel setup request message, or indicate in the tunnel setup request message that the network should configure the static IP address of the WLAN UE or the network simply provides the static address to the WLAN UE.

## 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 control a specific ongoing WLAN access session for online charging purposes.
- It shall be possible for an operator to maintain a single prepaid account for WLAN, PS, CS, and IMS for a user.
- The 3GPP system shall be able to process the WLAN access resource usage information, and convert it into the format used in 3GPP networks (e.g. CDR).
- It shall be possible to correlate charging and accounting records generated in WLAN Access related nodes and records generated in 3GPP nodes.
- It shall be possible to apply offline charging and online charging mechanisms for the WLAN interworking with 3GPP network.

Additionally, for WLAN 3GPP IP Access:

- It shall be possible to generate per user charging information in the HPLMN and in the VPLMN irrespective of whether the service is provided in the HPLMN or in the VPLMN.
- WLAN Charging Information shall be collected for each WLAN UE by the WAG and the PDG that are serving the WLAN UE. The operator can control whether charging information shall be collected in the PDG on an individual WLAN UE and/or W-APN context basis by appropriately setting the Subscribed Charging

Characteristics and/or W-APN Charging Characteristics in the HSS. The Charging Characteristics on the WLAN subscription and individually subscribed W-APNs are specified in 3GPP TS 32.252 [26].

## 5.12 AAA Protocol Requirements

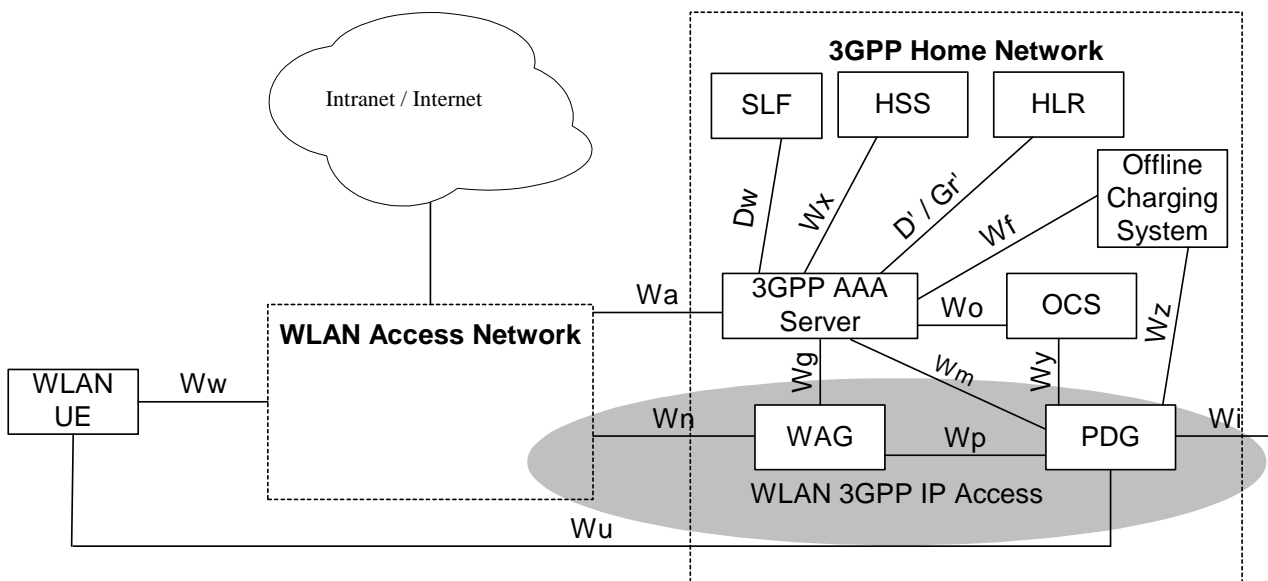
- As far as possible, a common AAA protocol shall be used across all AAA interfaces. This may not be possible for the Wa and Wd interfaces when the WLAN AN is using a legacy AAA protocol.
- If protocol interworking is needed, then in the non-roaming case it shall be performed at the edge of the 3GPP network. For roaming, such interworking shall be performed either in the visited network or in the home network (dependent upon inter-operator roaming agreements).

# 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



Note: The shaded area refers to WLAN 3GPP IP Access functionality.

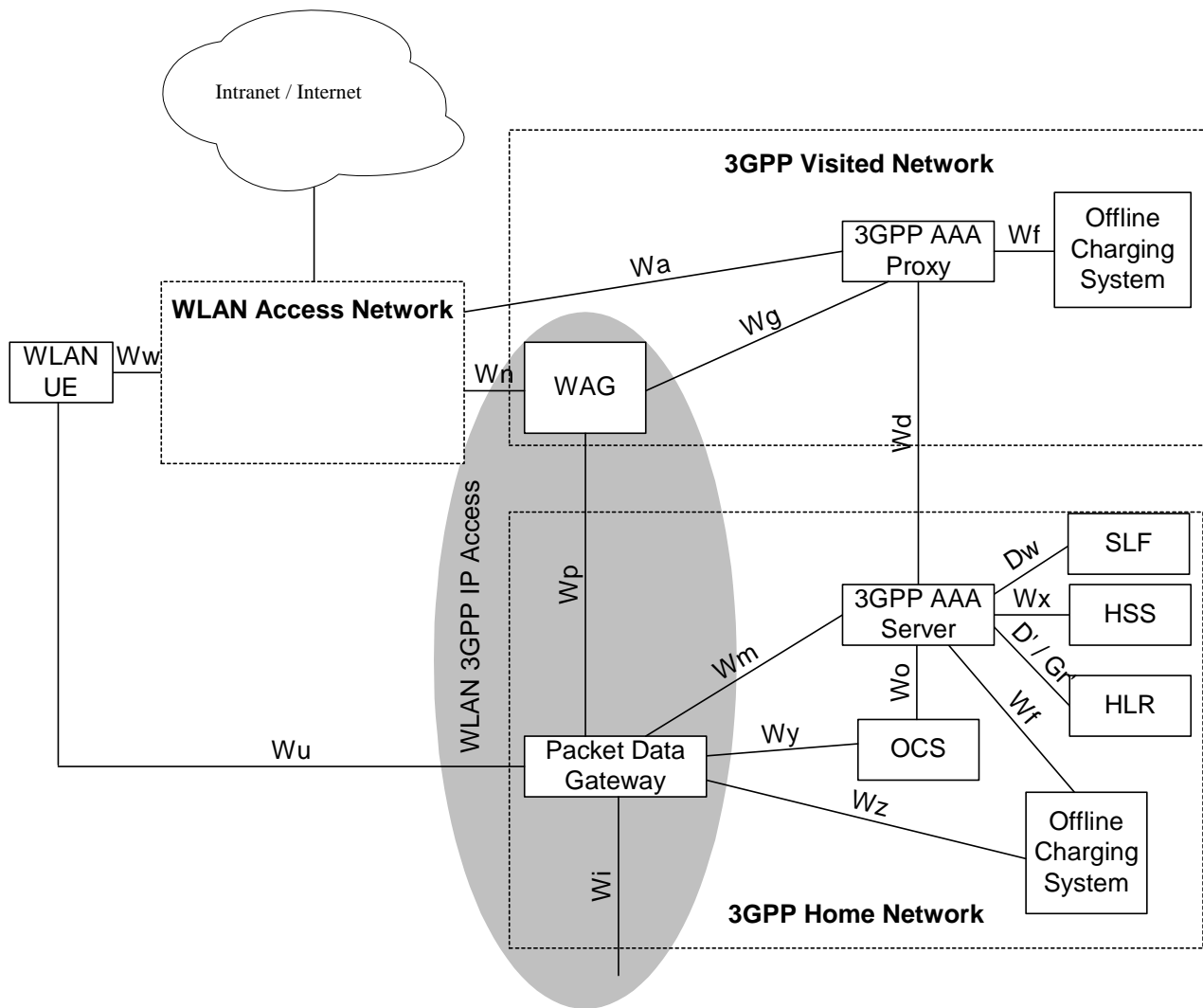
**Figure 6.1: Non-roaming reference model**

### 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 reference points are intra-operator. The home 3GPP network interfaces to other 3GPP networks via the inter-operator Wd reference point.

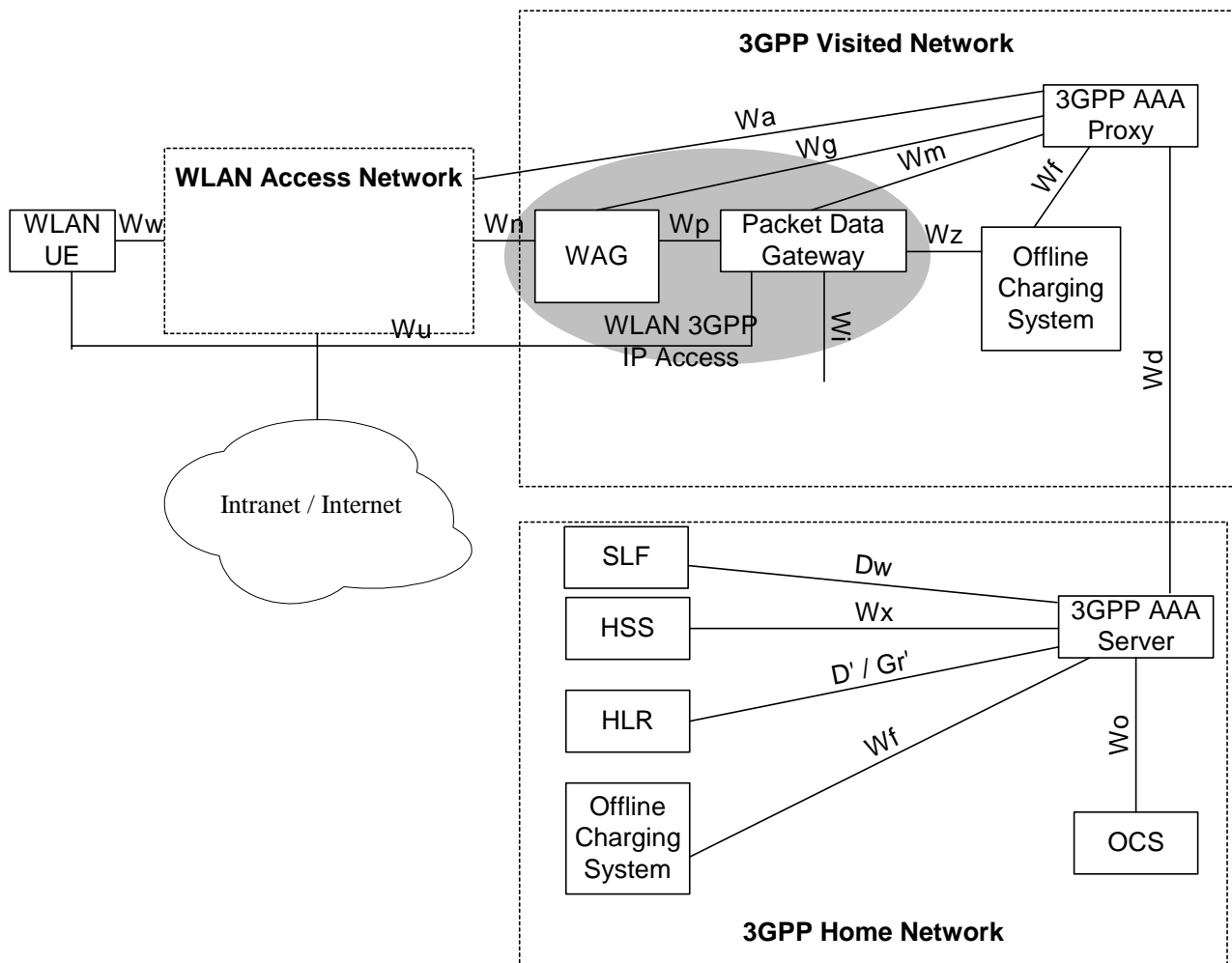
The 3GPP AAA proxy relays access control signalling and accounting information to the home 3GPP AAA Server using the Wd reference point.

It can also issue charging records to the visited network Offline Charging System when required. The 3GPP network interfaces to WLAN Access Networks via the Wa reference point.



Note: The shaded area refers to WLAN 3GPP IP Access functionality.

**Figure 6.2a: Roaming reference model - 3GPP PS based services provided via the 3GPP Home Network**



Note: The shaded area refers to WLAN 3GPP IP Access functionality.

**Figure 6.2b: Roaming reference model - 3GPP PS based services provided via the 3GPP Visited Network**

## 6.2 Network elements

### 6.2.1 WLAN UE

A WLAN UE is the User Equipment using a UICC card utilized by a 3GPP subscriber to access the WLAN AN for 3GPP interworking purpose. The WLAN UE may be capable of WLAN access only, or it may be capable of both WLAN and 3GPP radio access. Some WLAN UE's may be capable of simultaneous access to both WLAN and 3GPP radio access. A 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.

The WLAN UE functions include:

- Associating to an I-WLAN.
- WLAN access authentication based on EAP methods.
- Selection of a suitable VPLMN in the roaming case.
- Building an appropriate NAI.
- Obtain a local IP address. If the WLAN UE is intended for use with WLAN ANs supporting IPv4 only as well as with WLAN ANs supporting IPv6 only, it shall be equipped with a dual IP stack.

For WLAN 3GPP IP Access enabled WLAN UE:

- Building an appropriate W-APN to be used for External IP network selection.
- Request the resolution of a W-APN to a PDG address.
- If IPv4 and IPv6 addresses are returned during the resolution process, the WLAN UE shall select the address that has the same format as its own local IP address (IPv4 or IPv6).
- Establish a secure tunnel to a PDG.
- Obtain a remote IP address.
- Accessing services provided in the operators PS domain.
- Allowing users to select the type of network access, i.e. WLAN 3GPP IP Access or WLAN Direct IP Access.

#### 6.2.1.1 Void

### 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
- Providing access scope limitation information to the WLAN based on authorization information from the Home network
- Reporting per-user charging/accounting information to the VPLMN Offline Charging System for roaming users
- Service termination (O&M initiated termination from visited network operator)
- Protocol conversion when the Wa and Wd reference points do not use the same protocol

For WLAN 3GPP IP Access only:

- Receiving per-tunnel charging information based on the tunnel identifier from the WAG and mapping of a user identifier and a tunnel identifier from the PDG; generating per user charging records for roaming users.
- 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
- Receiving the suitable policy enforcement information from AAA-Server and provides it to the WAG in VPLMN.
- May provide suitable routing enforcement information to WLAN AN.

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. There should be only one 3GPP AAA Server for a WLAN attached subscriber. 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 about WLAN Direct IP Access to the HPLMN Offline Charging System.
- Transfer a subscriber's authentication to a 3GPP AAA Server when it is requested by HSS/HLR.

For WLAN 3GPP IP Access:

- Communicates service authorization information (e.g. authorized W-APN, necessary keying material for tunnel establishment and user data traffics) to the PDG. AAA proxies if the PDG is located in VPLMN.
- Provides the PDG with the WLAN UE's remote IP address, received from the HSS, when static remote IP address allocation is used.
- Provides the AAA-Proxy with suitable policy enforcement information.
- Provides suitable policy enforcement information to WAG in HPLMN.
- May provide suitable routing enforcement information to WLAN AN.

## 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. To this end, the HSS shall store the IP address of the 3GPP AAA server to which the WLAN UE is registered.

When a 3GPP AAA Server other than the registered 3GPP AAA Server of a subscriber, requests authentication information or the profile of the subscriber, the HSS should request it transfer the authentication to the registered 3GPP AAA Server by providing the registered 3GPP AAA Server address to it.

## 6.2.5 WLAN Access Gateway

The WLAN Access Gateway applies to a WLAN 3GPP IP Access enabled system.

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 a WLAN 3GPP IP Access enabled system.

The WLAN Access Gateway shall reside 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.
- Performs collection of per tunnel accounting information, e.g. volume count (byte count) and elapsed time, to be used for inter-operator settlements.
- Filters out packets based on unencrypted information in the packets. Packets should only be forwarded if they:

1. are part of an existing tunnel or
2. are expected messages from the WLAN UEs. This includes service requests, and tunnel establishment messages.

Since the WAG does not have a full trust relationship with the WLAN UE, it is not able to stop all messages. However, messages from an unknown IP address can easily be discarded. Other approaches may be used as well. Additional types of message screening are left to the operators' control. Furthermore, Network Address Translators within the WLAN may modify the source address of IP packets from the WLAN UEs. The modified source address can be reliably associated to a WLAN UE by the PDG during tunnel establishment and provided to the WAG via the 3GPP AAA Server/Proxy. Before this point, all tunnel establishment packets shall be routed by the WAG except those which are possibly discarded due to certain Firewall rules implemented on the WAG.

Note: per tunnel accounting 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 may implement policy enforcement before tunnel establishment to enhance the firewall against unwanted packets go through the PLMN, for example, to forbid the roaming WLAN UE from sending tunnel establishment to PLMN other than its HPLMN; to forbid packets from unauthorized WLAN UE.

The WAG shall implement policy enforcement after tunnel establishment.

After tunnel establishment, the following procedures apply at the WAG:

- 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.

### 6.2.5.1 Policy 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, 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 (before the tunnel establishment) will be bound to a user's AAA signalling. The WAG requires functionality to be able to associate this information to a user's traffic. As an implementation option, this functionality can be achieved by allocating the local IP Address by VPLMN.

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-tunnel Charging Generation

*Editor's Note: The details of per-tunnel charging generation in the WAG is FFS.*

## 6.2.6 Packet Data Gateway

The Packet Data Gateway applies to a WLAN 3GPP IP Access enabled system.

3GPP PS based services 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 or by the visited network. 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). If the PDG is intended to support connections from WLAN UEs using IPv4 and IPv6 local addresses, it shall be equipped with a dual IP stack.

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 to the WLAN UE (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;
- accepts or rejects the requested W-APN according to the decision made by the 3GPP AAA Server;
- 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.
- Delivers the mapping of a user identifier and a tunnel identifier to the AAA Proxy.
- Generates charging information related to user data traffic for offline and online charging purposes.
- May apply IP flow based bearer level charging [13], [15], e.g. in order to differentiate or suppress WLAN bearer charging for 3GPP PS based services.

Annex F describes how PDG functionality can be provided by re-using existing unmodified GGSN functionality.

## 6.2.7 Subscription Locator Function (SLF)

The SLF is located within the 3GPP subscriber's home network and enables the 3GPP AAA Server to find the address of the HSS which holds the subscriber data for a given user identity in a configuration with multiple separately addressable HSS'es. The SLF should be used in the same way for WLAN as for IMS, which is specified in 3GPP TS 23.228 [24].



## 6.2.8 Offline Charging System

The Offline Charging System is within the 3GPP network. The mapping of the Offline Charging System in the Release 6 charging architecture is specified in 3GPP TS 32.252 [26].

## 6.2.9 Online Charging System

The Online Charging System (OCS) is located within the 3GPP network. The OCS is described in 3GPP TS 32.296 [27].

# 6.3 Reference Points

## 6.3.1 Wa reference point

### 6.3.1.1 General description

The Wa 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 charging-related information in a secure manner. The reference point has to accommodate also legacy WLAN Access Networks.

Legacy logical nodes outside of 3GPP scope that terminate or proxy the Wa reference point signalling and do not support 3GPP AAA protocol shall require signalling conversion between the legacy AAA protocol and the 3GPP AAA protocol.

EAP authentication shall be transported over the Wa reference point.

### 6.3.1.2 Functionality

The functionality of the reference point is to transport AAA frames:

- Carrying data for authentication signalling between WLAN UE and 3GPP Network.
- Carrying data for authorization signalling between WLAN AN and 3GPP Network. These data may include a well-defined identification of the WLAN AN.
- Carrying charging signalling per WLAN user to enable offline and/or online charging. To minimize the requirements put on the WLAN Access Network, the use of online charging over Wa is optional and depends on the agreement between the operators of the WLAN AN and the 3GPP PLMN.
- 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.
- May carry Routing Enforcement information from the PLMN to ensure that all packets sent to/from the WLAN UE for PS based services are routed to the interworking VPLMN (roaming case) or HPLMN (no roaming case) appropriately.
- When such functionality is supported by the WLAN AN, purging a user from the WLAN access for immediate service termination
- Providing access scope limitation information to the WLAN based on the authorised services for each user (for example, IP address filters)

## 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 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 and the data defined for the W-APNs in the WLAN UE's profile) 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 based upon the D/Gr reference points defined in 3GPP TS 29.002 [10]. Support of the D'/Gr' reference points requires no modifications to the MAP protocol at the HLR.

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.

The functions provided on the D'/Gr' reference points are a subset of the functions provided on the D/Gr reference points described in 3GPP TS 29.002 [10].

If a 3GPP AAA Server supports the D' reference point, it will appear to the HLR/HSS as a VLR and shall behave according to the description of the behaviour of a VLR supporting the D reference point as described in 3GPP TS 29.002 [10].

If a 3GPP AAA Server supports the Gr' reference point, it will appear to the HLR/HSS as an SGSN and shall behave according to the description of the behaviour of an SGSN supporting the Gr reference point as described in 3GPP TS 29.002 [10].

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

### 6.3.4 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 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.

### 6.3.5 Wf reference point

The Wf reference point is located between 3GPP AAA Server/Proxy and 3GPP Offline Charging System. The prime purpose of the protocols crossing this reference point is to transport/forward offline charging information towards 3GPP operator's Offline Charging System located in the visited network or home network where the subscriber is residing.

The information forwarded to the Offline Charging System 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 functionality of the reference point is to transport:

- WLAN access-related charging data per WLAN user.

### 6.3.6 Wg reference point

The Wg reference point applies to WLAN 3GPP IP Access.

This is an AAA interface between the 3GPP AAA Server/Proxy and the WAG. It is used to

- Provide information needed by the WAG to perform policy enforcement functions for authorised users.
- Transport per-tunnel based charging information from the WAG to the AAA Proxy, only for roaming scenario.

### 6.3.7 Wn reference point

The Wn reference point applies to WLAN 3GPP IP Access.

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. There can be several different ways to implement this interface as shown in Annex C. The specific method to implement this interface is subject to local agreement between the WLAN AN and the PLMN.

### 6.3.8 Wp reference point

The Wp reference point applies to WLAN 3GPP IP Access.

This is the reference point between the WAG and PDG.

### 6.3.9 Wi reference point

The Wi reference point applies to WLAN 3GPP IP Access.

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 operator's public addressing scheme or through the use of a private addressing scheme.

### 6.3.10 Wm reference point

The Wm reference point applies to WLAN 3GPP IP Access.

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

- The 3GPP AAA Server/Proxy to retrieve tunneling attributes and WLAN UE's IP configuration parameters from/via Packet Data Gateway.
- The 3GPP AAA Server to provide the PDG with the WLAN UE's remote IP address, received from the HSS, when static remote IP address allocation is used.
- The 3GPP AAA Server to provide the PDG with charging data (subscribed Charging Characteristics or W-APN Charging Characteristics) for 3GPP PS based services charging
- Carrying messages between PDG and AAA Server in support of the user authentication exchange which takes place between WLAN UE and 3GPP AAA server/proxy.
- Carrying messages for user authorization between PDG and 3GPP AAA server/proxy. These messages transport e.g. the requested W-APN from PDG to 3GPP AAA server/proxy and eventually the authorized W-APN from 3GPP AAA server/proxy to PDG.
- Carrying authentication data for the purpose of tunnel establishment, tunnel data authentication and encryption.
- Carrying mapping of a user identifier and a tunnel identifier sent from the PDG to the AAA Proxy through the AAA Server.

## 6.3.11 Wd reference point

### 6.3.11.1 General description

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

EAP authentication shall be transported over the Wd reference point.

### 6.3.11.2 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 charging signalling per WLAN user- Carrying keying data for the purpose of radio interface integrity protection and encryption
- Carrying authentication data for the purpose of tunnel establishment, tunnel data authentication and encryption, for the case in which the PDG is in the VPLMN.
- Carrying mapping of a user identifier and a tunnel identifier sent from the PDG to the AAA Proxy through the AAA Server.
- 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 Wu reference point

The Wu reference point applies to WLAN 3GPP IP Access.

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 Ww, Wn and Wp reference points, which ensure that the data are routed via the WLAN Access Gateway where routing 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

## 6.3.13 Ww reference point

### 6.3.13.1 General Description

The reference point Ww connects the WLAN UE to the WLAN Access Network per IEEE 802.1x [19] specifications. The definition of IEEE Physical and Medium Access Control layers protocols (e.g. Layer 1 and Layer 2 defined by IEEE 802.11 standards) is out of the scope of 3GPP.

### 6.3.13.2 Functionality

The functionality of the reference point is based on IEEE 802.1x specifications [19] and it is intended to transport signalling messages including:

- parameters for authentication signalling between the 3GPP AAA Server and the WLAN UE;
- parameters for identification of the operator networks for roaming purposes (i.e. PLMN list).

## 6.3.14 Dw reference point

This reference point is between the 3GPP AAA Server and the SLF. The prime purpose of the protocol(s) crossing this reference point is to enable the 3GPP AAA Server to find the address of the HSS which holds the subscriber data for a given user identity in a configuration with multiple separately addressable HSS'es.

## 6.3.15 Wy reference point

The Wy reference point is used by a PDG to communicate with an Online Charging System (OCS). The purpose of the protocol(s) crossing this reference point is to transport online charging related information about WLAN 3GPP IP Access so as to perform credit control for the online charged subscriber.

## 6.3.16 Wz reference point

The Wz reference point is used by a PDG to communicate with an Offline Charging System. The purpose of the protocol(s) crossing this reference point is to transport offline charging related information about WLAN 3GPP IP Access.

## 6.4 Protocols

The protocol stack between the WLAN UE and the PDG is shown on figure 6.3

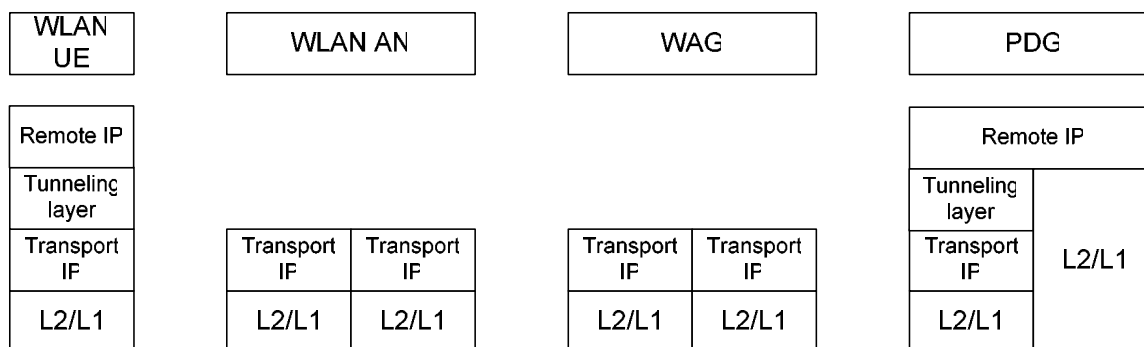


Figure 6.3: Protocol stack between the WLAN UE and the Packet Data Gateway

## 6.4.1 Remote IP Layer

The remote IP layer is used by the WLAN UE to be addressed in the external packet data networks (i.e. on the Wi reference point).

On this layer, the WLAN UE is addressed by its remote IP address and the packets are exchanged between the WLAN UE and an external entity. The PDG routes the remote IP packets without modifying them.

## 6.4.2 Tunnelling layer

The tunnelling layer consists of a tunnelling header, which allows end-to-end tunnelling between a WLAN UE and a PDG. It is used to encapsulate IP packets with the remote IP layer.

When encapsulated IP packets are encrypted, the tunnelling header contains a field which is used to identify the peer and decrypt the packets.

## 6.4.3 Transport IP Layer

The transport IP layer is used by the intermediate entities/networks and WLAN AN in order to transport the remote IP layer packets.

Between the WLAN UE and the WAG, the transport IP layer is used by the WLAN UE to be addressed within the WLAN AN, the intermediate networks (if any) and 3G networks.

On this layer, the WLAN UE is addressed by its local IP address.

For example this local IP address can be:

- a private IPv4 address allocated by the WLAN AN; in this case a NAT is required in the WLAN AN and used to make the WLAN UE's local IP address routable in the intermediate networks (if any), the VPLMN and the HPLMN;
- a public (either IPv4 or IPv6) address allocated by the WLAN AN; in this case no NAT is needed;
- an IP address allocated by the WAG in an address space that is routable in the WLAN AN as well as in the intermediate networks (if any) and the 3G network; in this case no NAT is needed.

## 6.5 WLAN user profile

The WLAN user profile shall reside in HSS (if the operator is using a legacy HLR, the WLAN user profile may reside in the 3GPP AAA Server) and be retrieved from 3GPP AAA server via Wx reference point. The profile shall contain the following data items: Detailed work on these parameters is expected in stage 3 work.

1. IMSI
2. MSISDN

3. Operator determined barring of 3GPP–WLAN Interworking subscription
4. Operator determined barring of 3GPP WLAN 3GPP IP Access

This allows operator to disable all W-APNs at one time. If there is a conflict between this item and the "operator determined barring" of any W-APN, the most restrictive will prevail.

5. Maximum session duration (*optional*)

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

6. Subscribed Charging Characteristics and Accounting Server Identifier(s)

The Subscribed Charging Characteristics will implicitly define the charging mode to be applied and, for every case, the accounting server where the accounting information is to be reported.

7. List of authorized W-APNs (*optional*)

List of W-APNs for which the user will have services available. These W-APNs may correspond to services in the home network or in the visited network.

For each W-APN it shall be possible to define:

- W-APN Charging Characteristics and Accounting Server Identifier (*optional*)

If these parameters are not present, the W-APN Charging Characteristics and Accounting Server Identifier defined in item 6 must be considered.

- W-APN remote IP address (*optional*)

Indication of the static remote IP address. If this parameter is present, the 3GPP AAA Server shall download it to the PDG in the W-APN authorization procedure, so the PDG shall use this static IP address. Otherwise, the remote IP address shall be allocated dynamically.

Operator determined barring for W-APN. As the service requirements defined in 3GPP TS 22.234. Those W-APNs which have a complete barring, shall not be sent to the 3GPP AAA Server from HSS.

8. WLAN Direct IP access allowed

Indication if the user is allowed to use WLAN Direct IP access.

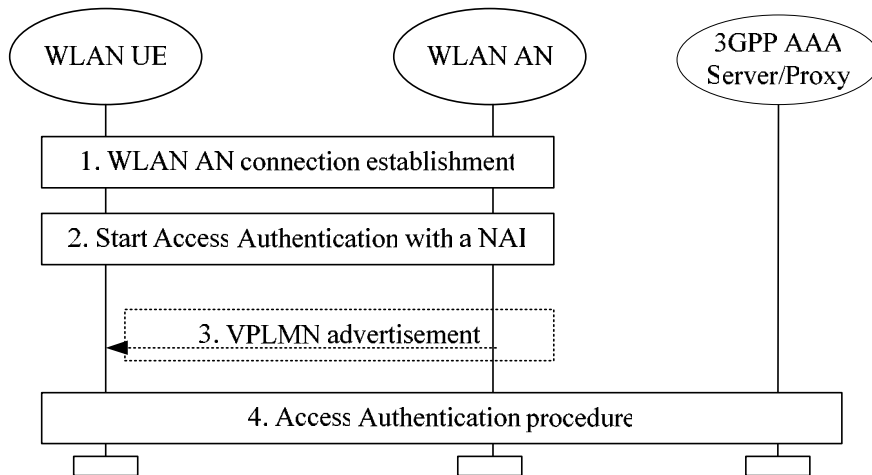
9. Roaming allowed

Indication if the user is allowed to use a WLAN AN connected to an VPLMN.

## 7 Procedures

### 7.1 I-WLAN and VPLMN Selection Procedure

#### 7.1.1 Initial network selection



**Figure 7.1: I-WLAN and VPLMN selection procedure**

1. The WLAN UE selects a WLAN AN and establishes the WLAN connection with a WLAN technology specific procedure (e.g. in IEEE 802.11 it starts an association procedure). The details of the selection of the WLAN AN are specified in 3GPP TS 24.234 [9].
2. The Authentication procedure is initiated in a WLAN technology specific way and as a part of this process, the WLAN UE sends a NAI to the WLAN AN. The NAI shall be constructed as it is specified in 3GPP TS 23.003 [5].
3. If the WLAN AN is not able to route the authentication request (e.g. in the case where the WLAN AN receives an initial NAI with an unknown realm), the WLAN AN sends a response to the WLAN UE that provides information about the 3GPP networks to which the WLAN AN is able to route authentication requests.

From this point the WLAN UE may continue the access authentication with the selected WLAN AN using a different NAI (step 2) or may start access authentication with another available WLAN AN (step 1) or may stop. The details of the WLAN UE behaviour are specified in 3GPP TS 24.234 [9]. If the WLAN UE continues the access authentication with the selected WLAN AN, it shall select a VPLMN among the 3GPP networks indicated in the response received from the WLAN AN and build the new NAI as a roaming NAI indicating this VPLMN.

4. The WLAN AN routes the AAA message to the 3GPP AAA Server or 3GPP AAA Proxy based on the NAI and the access authentication is performed as it is specified in 3GPP TS24.234 [9].

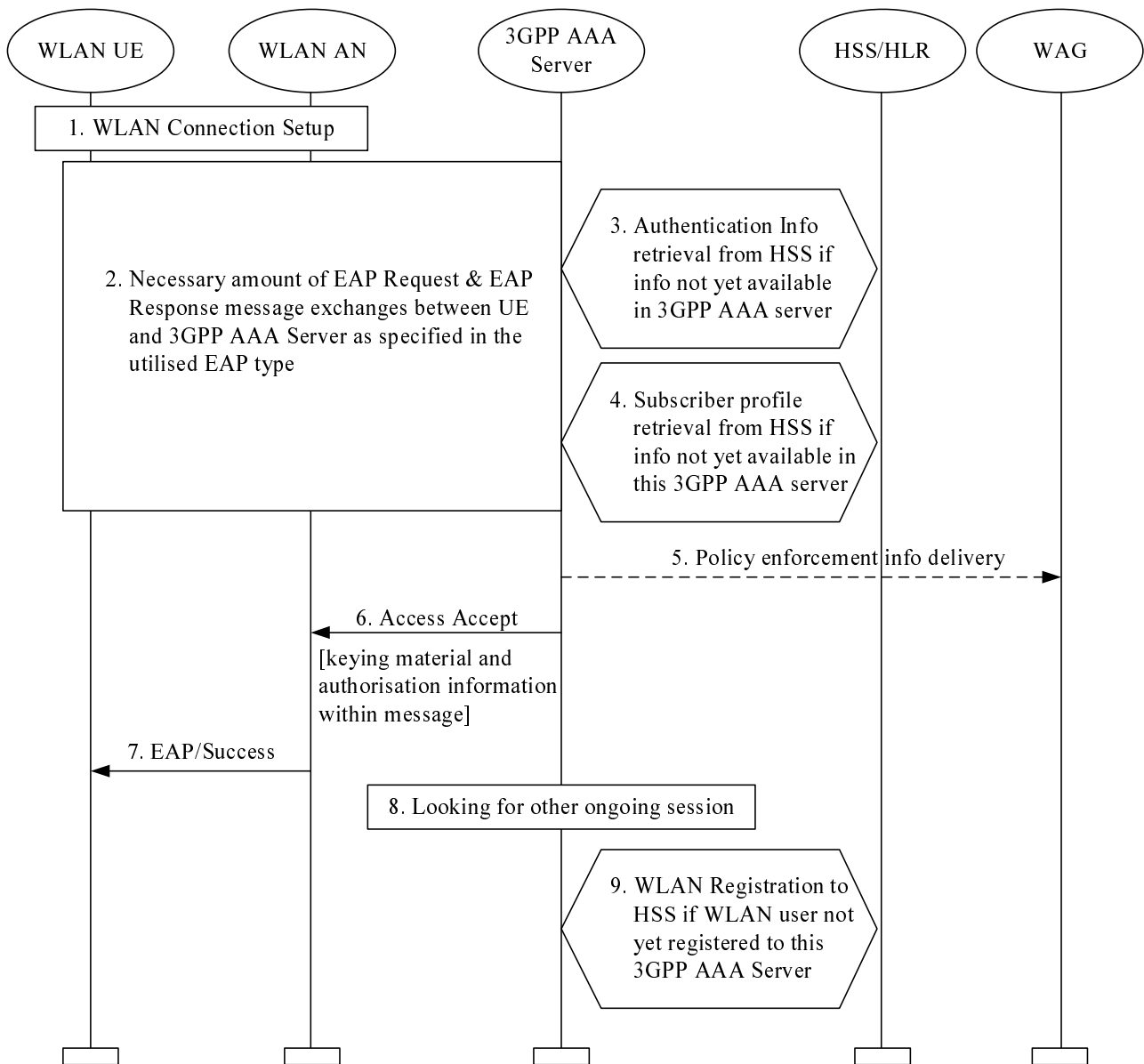
#### 7.1.2 Network re-selection

When the WLAN UE changes from the current serving PLMN to another PLMN with or without change of the WLAN AN, it needs to use a new NAI corresponding to the new PLMN in a new authentication initiated by the WLAN UE or the WLAN AN.

The 3GPP AAA Server may then receive a new authentication with PLMN selection different from the current active connection. For example, the WLAN UE lost radio in the first WLAN AN, then it changed to another WLAN AN with a different PLMN selection before the previous WLAN AN detected that the user is lost, or the WLAN UE started the new authentication before the disconnection of the previous connection. In this case, the 3GPP AAA Server shall initiate a disconnection to the currently active connection after the success of the new authentication and authorization process.



## 7.2 WLAN Access Authentication and Authorisation



**Figure 7.2: 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 Wa 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. During the information retrieval the HSS/HLR checks if there is a 3GPP AAA Server already registered to serve for the user. In case the HSS/HLR detects that another 3GPP AAA Server has already registered for this user, it shall provide the current 3GPP AAA Server with the previously registered 3GPP AAA Server address. The authentication signalling is then routed to the previously registered 3GPP AAA Server.

- 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. Optionally, the 3GPP AAA Server (or the 3GPP AAA Proxy in roaming case) may send the policy enforcement information to the WAG in the PLMN that the WLAN UE selected in case VPLMN is to allocate the local IP Address for the WLAN UE.

Note: Additional process, such as allocating the IP address, may be necessary during or before this step to be performed.

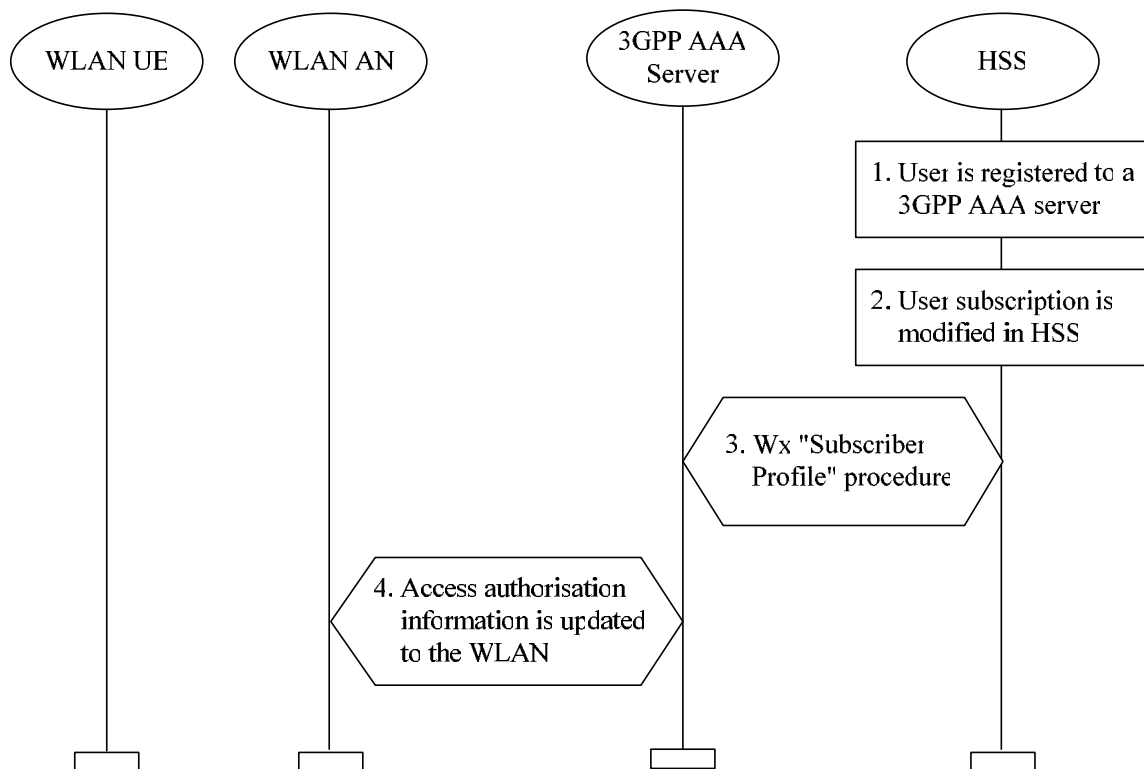
- 6 If the EAP authentication and authorisation was successful, then 3GPP AAA Server sends Access Accept message to WLAN. In this message 3GPP AAA Server includes EAP Success message, keying material derived from the EAP authentication as well as connection authorisation information (e.g. NAS Filter Rule or Tunneling attributes) to the WLAN.  
WLAN stores the keying material and authorisation information to be used in communication with the authenticated WLAN UE.

NOTE: In the roaming case, authorisation information is passed from 3GPP AAA Server to 3GPP AAA Proxy in the form of Local service identifiers (see Section 6.5)

- 7 WLAN informs the WLAN UE about the successful authentication and authorisation with the EAP Success message.
- 8 The 3GPP AAA Server checks if there is a different previously established authentication session of the WLAN user, e.g., a session that uses a different WLAN UE or roaming in a different WLAN AN or in a different VPLMN. If yes then 3GPP AAA Server shall close the previously established session ("Session abort procedure" over Wa) to avoid multiple WLAN direct IP access sessions.
- 9 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.

## 7.3 Subscriber Profile Update

### 7.3.0 WLAN Direct Access Authorization information update procedure

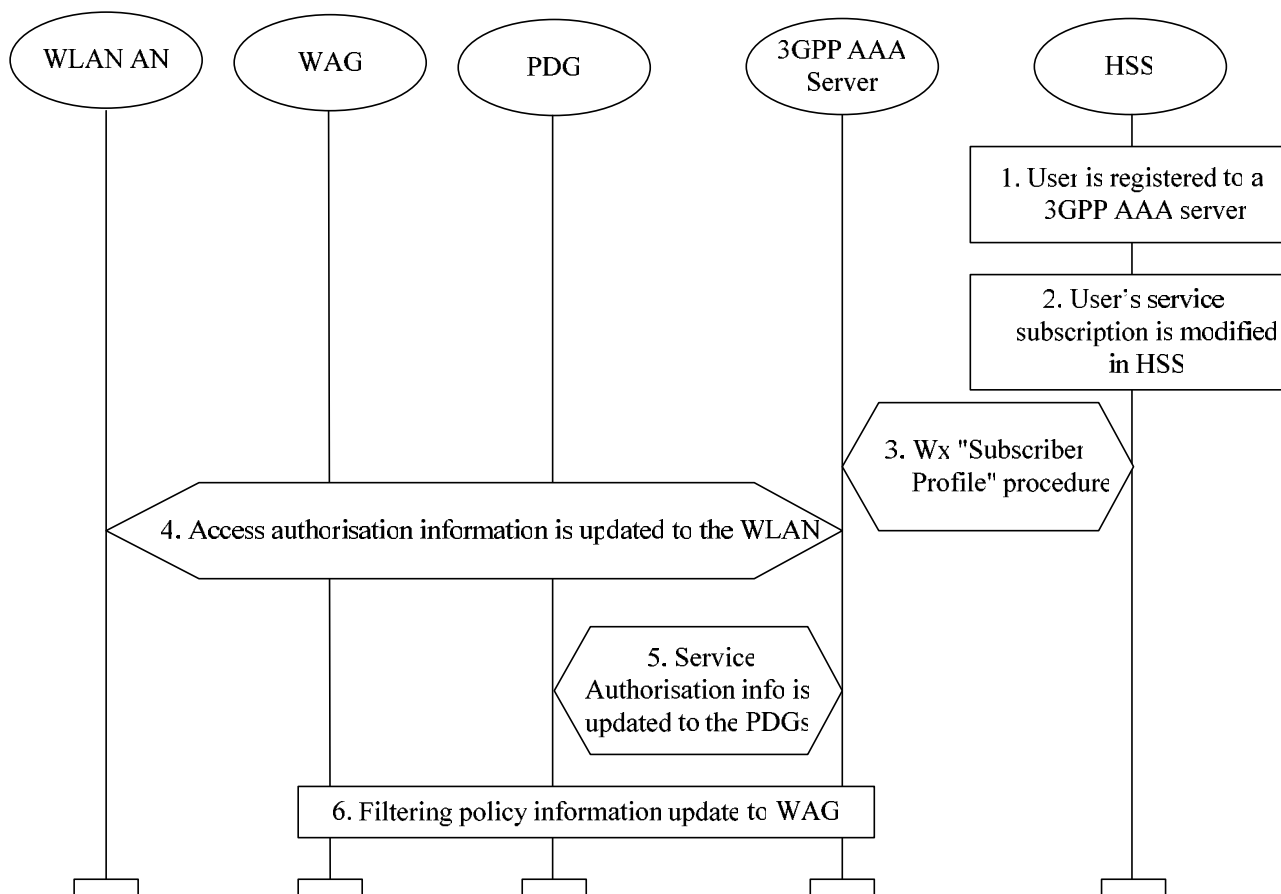


**Figure 7.3: Subscriber Profile and access authorization info Update Procedure**

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 WLAN access authorisation information of the associated connection is updated to WLAN as necessary. If the subscriber loses the authorization of the WLAN access, WLAN shall disconnect the radio interface connection by WLAN technology specific mechanisms.

### 7.3.1 Access and service Authorization information update procedure

This procedure is for WLAN 3GPP IP Access.

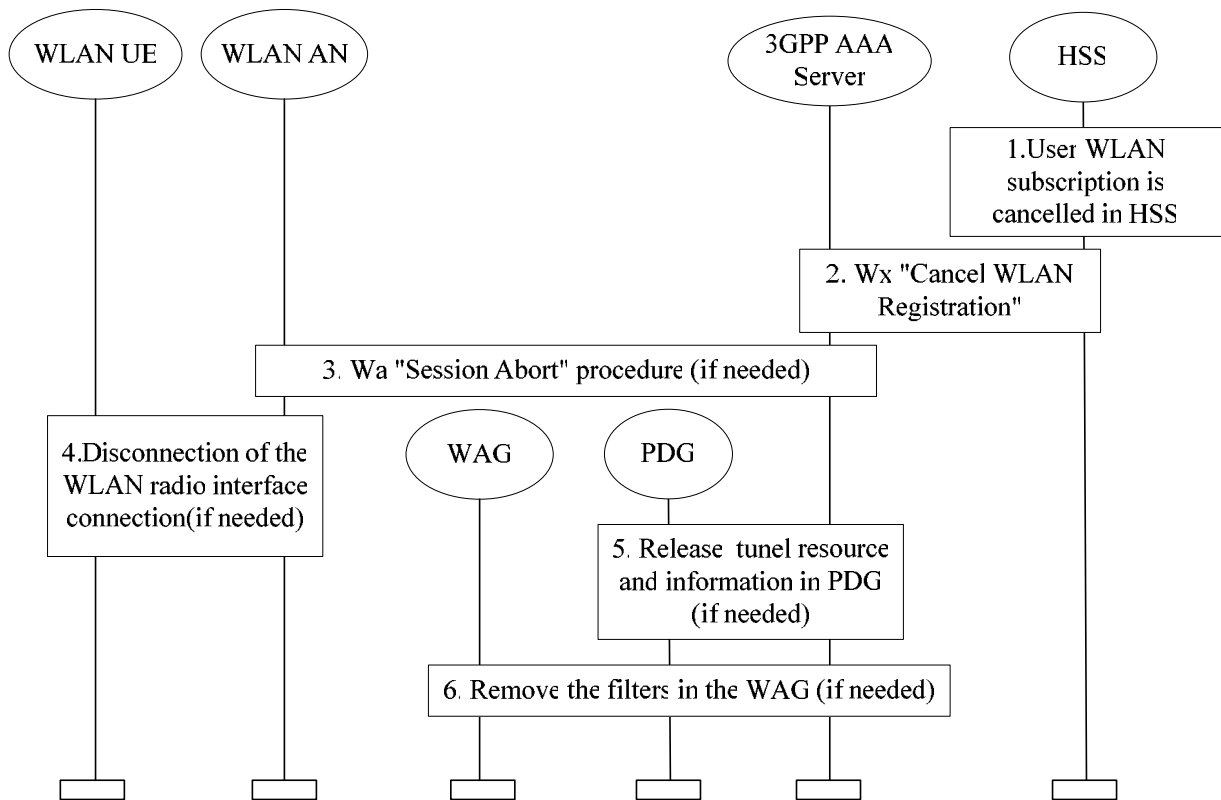


**Figure 7.4: Authorization information Update Procedure**

1. User is registered to a 3GPP AAA Server
2. User's service 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 WLAN access authorisation information of the associated connection is updated to WLAN AN if necessary. If the subscriber loses the authorization of the WLAN access, WLAN shall disconnect the radio interface connection by WLAN technology specific mechanisms.
5. The service authorisation information of the activated services is updated to PDGs if necessary. A deactivation of service may be initiated if the subscriber lost the authorization of the activated service.
6. The filtering policy information of the activated services is updated to WAG if necessary.

**Note:** The de-registration may be initiated by the 3GPP AAA Server to the HSS as necessary, i.e., the 3GPP AAA Server determines that the WLAN UE is unable to access any service upon the updated authorization.

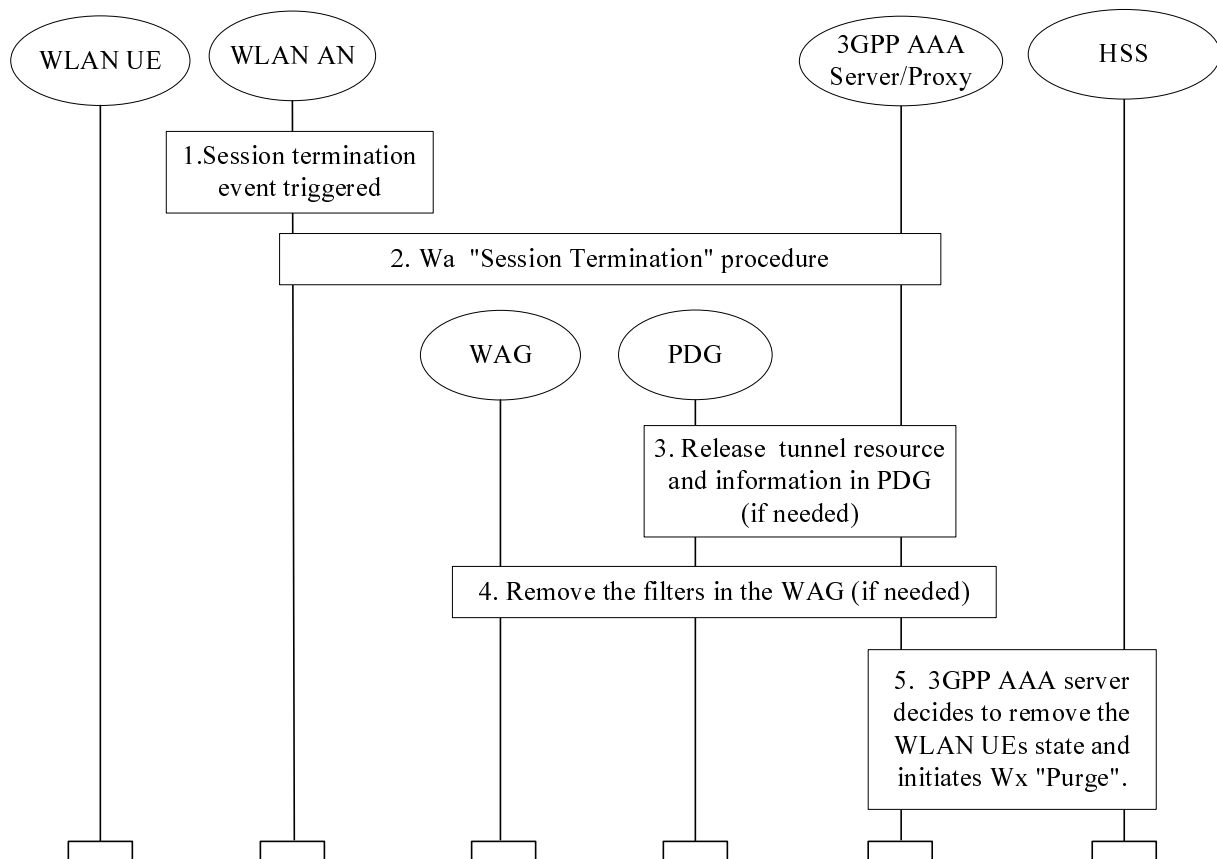
## 7.4 Cancelling WLAN Registration



**Figure 7.5: 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 WLAN access connection still exists, Wa 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.
5. If the subscriber's tunnel connection with one or several PDG(s) exists, the 3GPP AAA Server/Proxy informs the PDG(s) over the Wm reference point, to remove the tunnel related information and resource.
6. The filters, which were deployed to WAG for the tunnel(s) during the tunnel establishment, are removed.

## 7.5 Disconnecting a Subscriber by WLAN

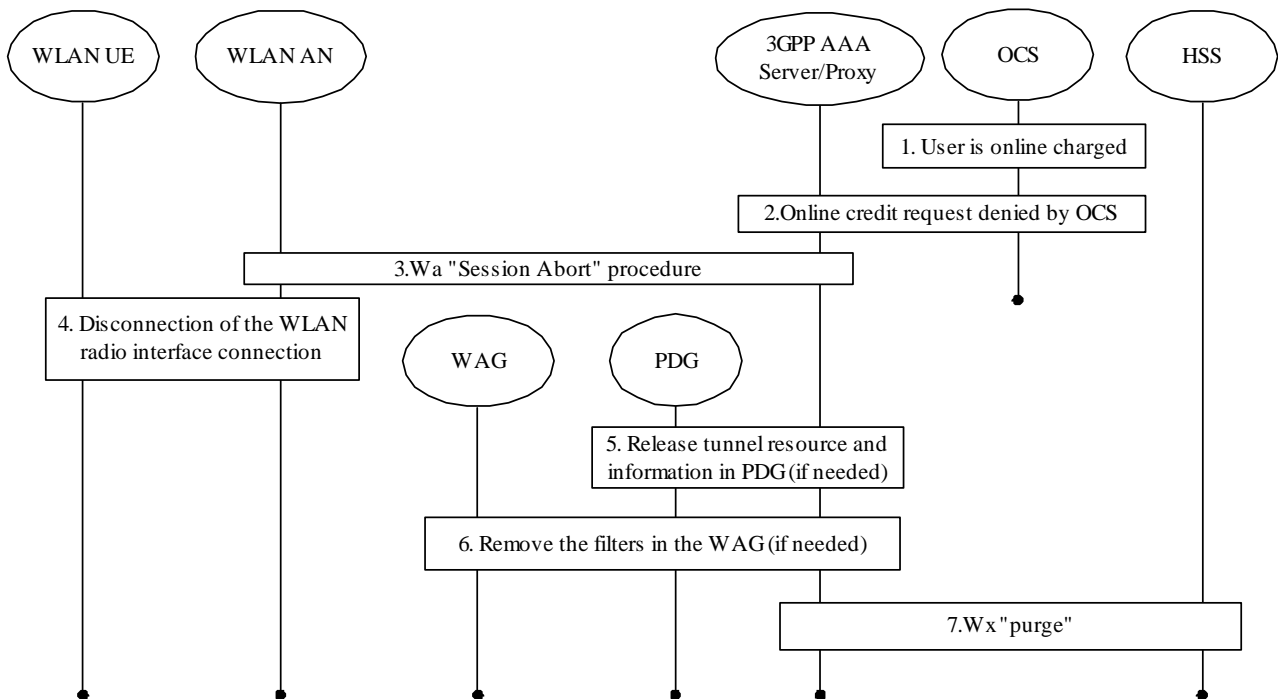


**Figure 7.6: WLAN initiated disconnection procedure**

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.
2. WLAN initiates Wa Session Termination procedure towards 3GPP AAA Server.
3. If the subscriber has a tunnel connection with one or more PDGs, and the 3GPP AAA Server/Proxy needs to remove the connections, it informs the PDG(s) over the Wm reference point to remove the tunnel related information and resource.
4. The filters, which were deployed to WAG for the tunnel(s) during the tunnel establishment, are removed.
5. 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.

## 7.6 Disconnecting a Subscriber by Online Charging System

### 7.6.1 The OCS initiated WLAN AN access disconnection

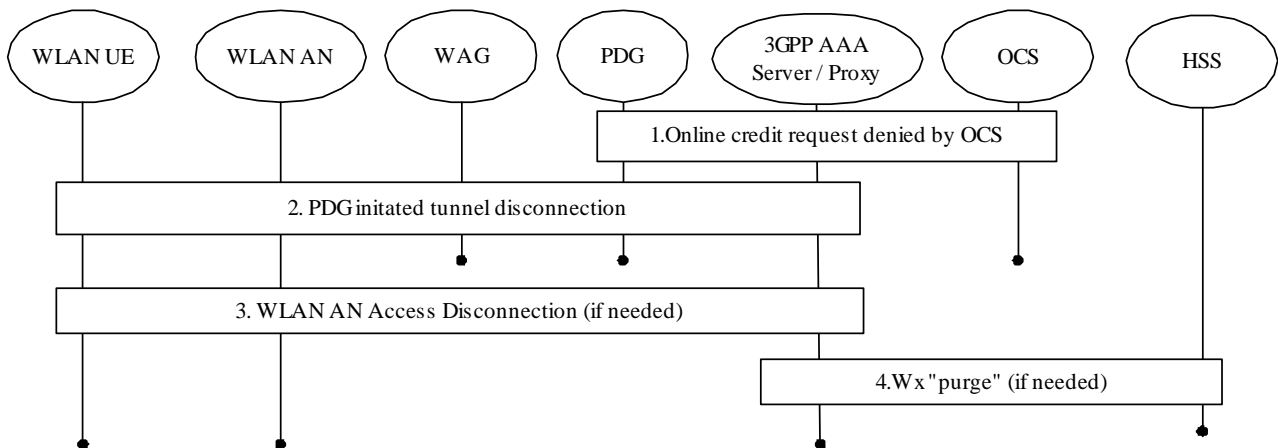


**Figure 7.7: The OCS initiated WLAN AN access disconnection procedure**

This section applies to the case when an online charged user runs out of credit and is totally disconnected from WLAN.

1. A subscriber is online charged by 3GPP AAA Server for WLAN access.
2. The 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, Wa reference point procedure "Session Abort" procedure is executed towards the WLAN AN.
4. The WLAN AN disconnects the radio interface connection by WLAN technology specific mechanisms.
5. If the subscriber's tunnel connection with one or several PDG(s) exists, the 3GPP AAA Server/Proxy informs the PDG(s) over the Wm reference point, to remove the tunnel related information and resource.
6. If filters were deployed to WAG for the tunnel(s) during the tunnel establishment, then they are removed.
7. If no Wx "Purge" procedure was already initiated in step 3, then the 3GPP AAA Server notifies HSS that WLAN registration in the 3GPP AAA Server has been cancelled, by means of Wx procedure "Purge"

## 7.6.2 The OCS initiated tunnel disconnection



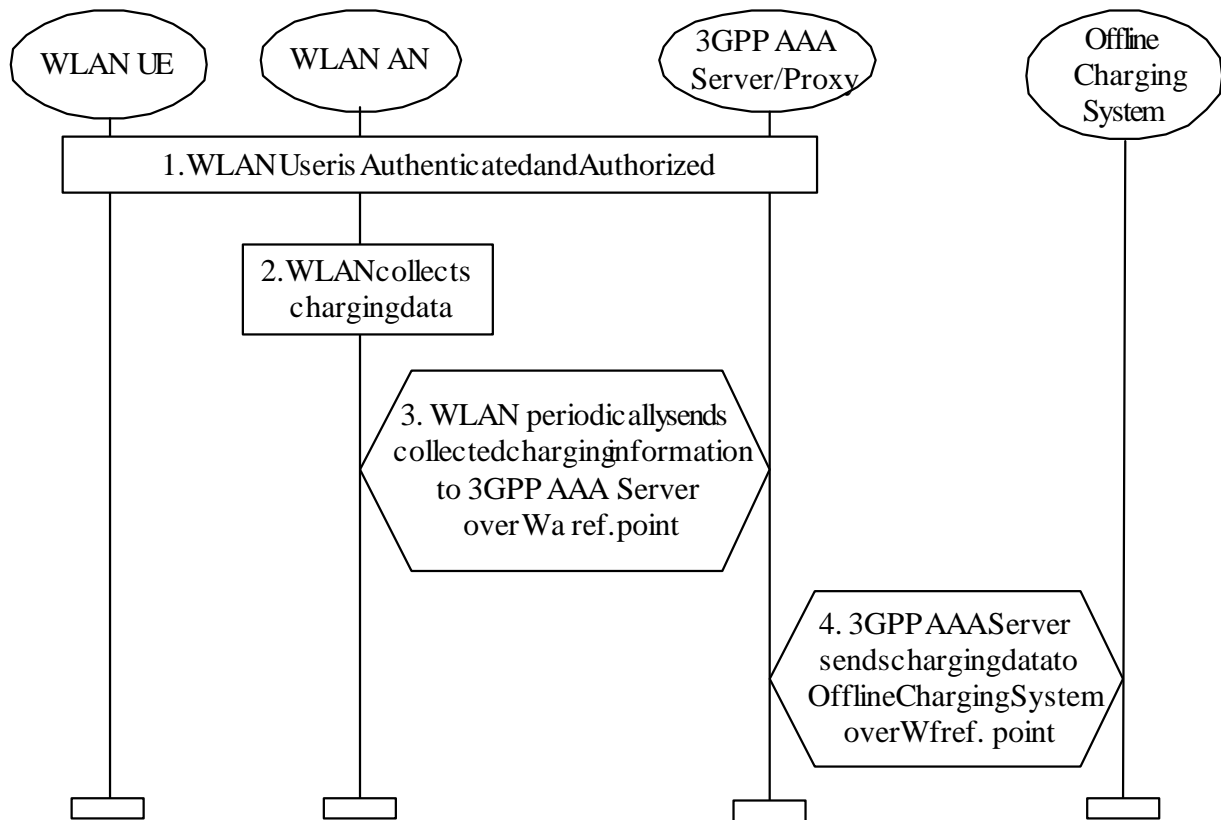
**Figure 7.8a: The OCS initiated tunnel disconnection procedure**

This section applies to the case when the tunnels of an online charged user are disconnected due to the lack of credits.

1. The Online Charging System (OCS) denies the credit request from the PDG. The possibly already retrieved online credit runs out.
2. The PDG disconnects the tunnels that require new credits using the network initiated tunnel disconnection procedure (clause 7.10.2). The tunnels that do not require new credits (e.g., the tunnels using free of charge W-APNs) will not be disconnected.
3. If all tunnels of the subscriber have been disconnected in the previous step then the 3GPP AAA Server may decide to totally disconnect the subscriber by performing 'Session Abort' towards the WLAN AN (i.e. step 3 and 4 of clause 7.6.1).
4. If the subscriber is disconnected from the WLAN AN in step 3 and no Wx "Purge" procedure was already initiated, then the 3GPP AAA Server notifies HSS that WLAN registration in the 3GPP AAA Server has been cancelled, by means of Wx procedure "Purge".



## 7.7 Charging offline charged subscribers

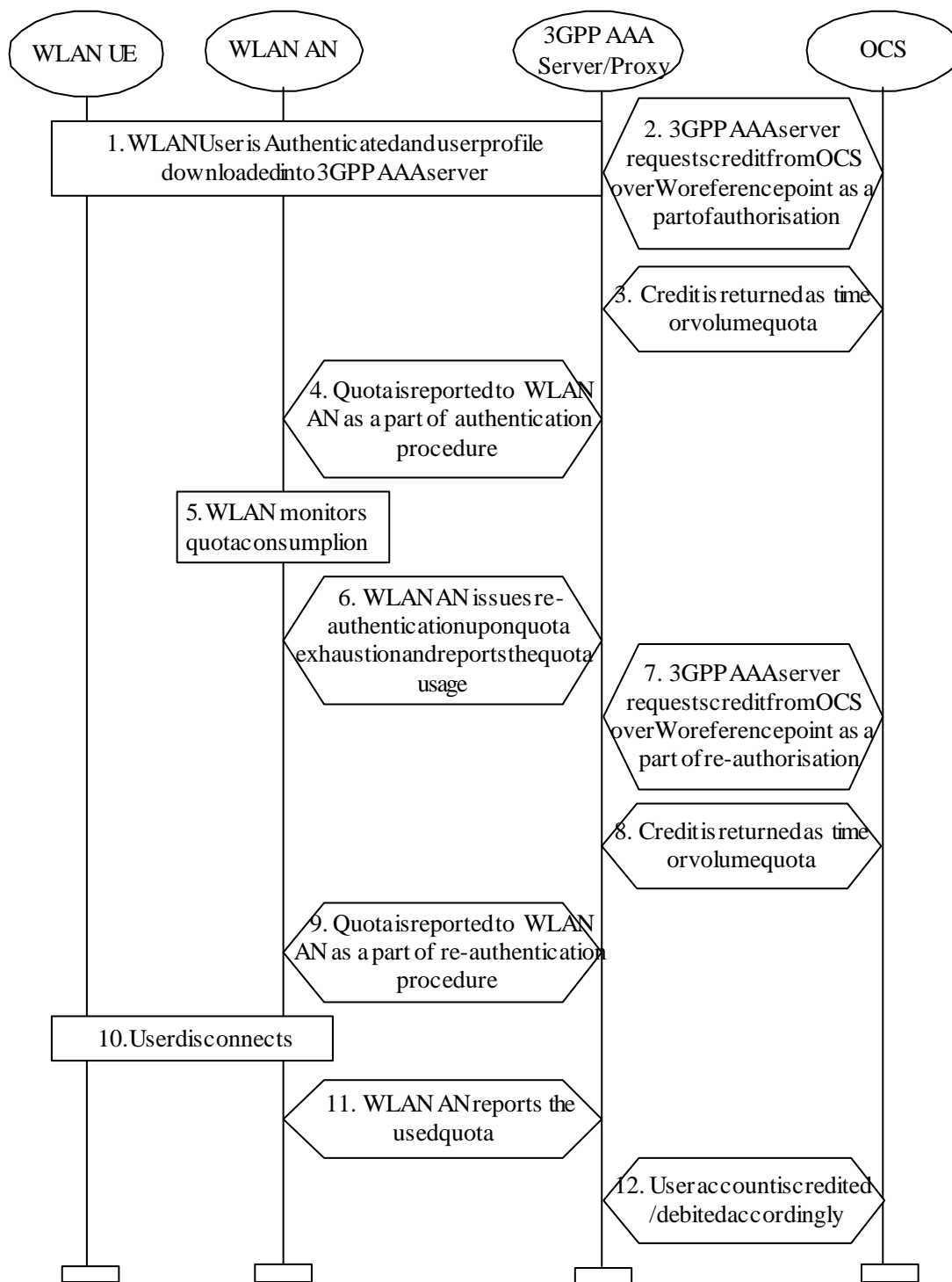


**Figure 7.8: Charging Procedure for Offline Charged Subscribers**

1. The 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. The WLAN AN collects charging data related to access or services locally consumed.
3. The WLAN AN periodically forwards collected charging information to the 3GPP AAA Server over Wb reference point.
4. The 3GPP AAA Server forwards charging information to the Online Charging System over the Wf reference point.

Note: In visited network the 3GPP AAA Proxy may also periodically report the usage of resources to the local Online Charging System over the Wf reference point.

## 7.8 Charging online charged subscribers



**Figure 7.9: Charging Procedure for Online Charged Subscribers**

1. The 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. The 3GPP AAA Server requests online charging credit from the OCS.
3. The OCS returns credit as time and/or volume quota.
4. The allocated quota is indicated to the WLAN AN.

5. The WLAN AN monitors the quota consumption.
6. When quota is almost used, the WLAN AN issues re-authentication message over Wa reference point. Used quota is indicated in the request.
7. The 3GPP AAA Server requests more credit from the OCS.
8. The OCS returns credit as time and/or volume quota.
9. The allocated new quota is indicated to the WLAN AN.
10. The user disconnects from WLAN AN.
11. The WLAN AN reports the used quota to the 3GPP AAA Server over Wa reference point.
12. The user account is debited / credit according the usage information in the final message.

Note: In visited network the 3GPP AAA Proxy may also periodically report the usage of resources to the local Online Charging System over Wf reference point. In home network the 3GPP AAA Server may also report the usage to the Online Charging System over the Wf reference point using offline charging procedures for statistical or other purposes.

## 7.9 W-APN resolution and Tunnel establishment

This information flow presents the generic message exchange necessary in order to resolve the selected W-APN and establish a WLAN UE-Initiated tunnel for WLAN 3GPP IP Access purposes.

As a prerequisite of these procedures it is necessary to perform the following:

1. WLAN Access Authentication and Authorisation and provisioning of the WLAN UE's local IP address

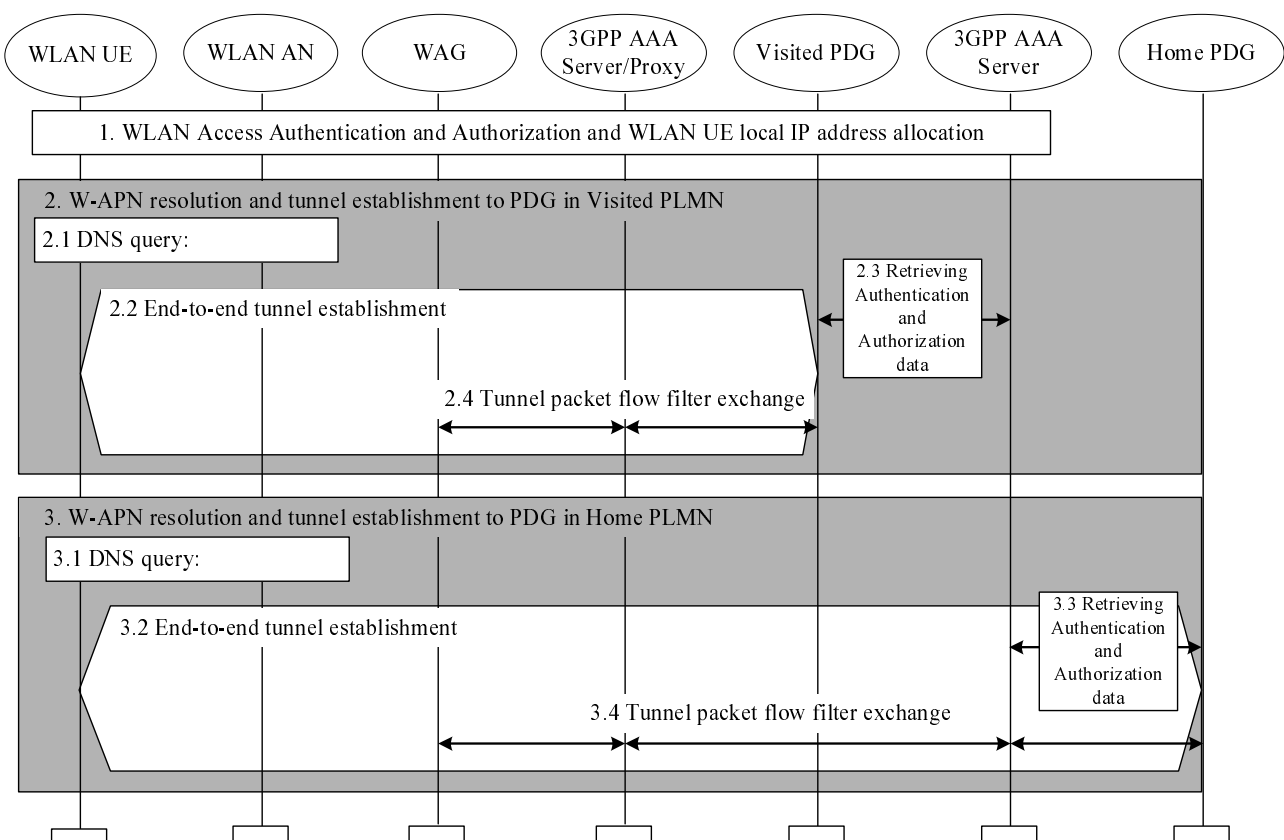


Figure 7.10: Example message flow to WLAN UE-Initiated tunnel establishment

When the user decides that he wants to access a service, the WLAN UE selects the W-APN network ID associated to the service requested by the user.

A detailed description of the W-APN resolution and the WLAN UE-Initiated Tunnel Establishment is given below.

2. Depending on internal configuration, the WLAN UE initiates W-APN resolution and tunnel establishment with a PDG in VPLMN.

Note: The configuration of the WLAN UE regarding W-APNs can be controlled by e.g. USIM Application Toolkit-based mechanisms.

- 2.1 WLAN UE constructs an FQDN using the W-APN Network Identifier and VPLMN ID as the Operator Identifier and performs a DNS query to resolve it. The DNS response will contain one or more IP addresses of equivalent PDGs that support the requested W-APN in the VPLMN according to standard DNS procedures.  
If the VPLMN does not support the W-APN, then the DNS query returns a negative response. In this case, the WLAN UE continues with step 3.
- 2.2 The WLAN UE selects a PDG from the list received in step 2.1. If the DNS response contains IPv4 and IPv6 addresses, the WLAN UE has to select an address that has the same format as its own local IP address. If a PDG is finally selected, the establishment of an end-to-end tunnel is performed between the WLAN UE and this PDG. The WLAN UE shall include the W-APN and the user identity in the initial tunnel establishment request.
- 2.3 During the tunnel establishment, the PDG contacts the 3GPP AAA Server in the HPLMN via the 3GPP AAA Proxy for authorization of the WLAN UE for the W-APN being requested by the WLAN UE and to retrieve the information required for the mutual authentication part of the tunnel establishment. As a result of successful mutual authentication the 3GPP AAA Server registers itself at the HSS (WLAN registration procedure). This action may be omitted, if the 3GPP AAA Server is already registered at the HSS. The 3GPP AAA Server shall be able to check that the user requesting the tunnel establishment has been already successfully WLAN Access Authorized. Based on operator policy it shall be possible to turn this check on and off. The check may be based on the user's subscription data, e.g. the user's subscribed services. If the check is not successful, the tunnel establishment request is rejected.  
If the WLAN UE is not allowed to use a visited-PDG to access the given W-APN, the 3GPP AAA Server shall send a rejection message to the PDG and then the tunnel establishment shall be rejected by the PDG. The 3GPP AAA Server shall provide PDG with the subscribed Charging Characteristics or W-APN Charging Characteristics. If it is not possible to establish the tunnel with any of the PDGs received from step 2.1, or the tunnel establishment failure reason is that the WLAN UE is not allowed to use a visited-PDG to access the given W-APN, then the WLAN UE continues with step 3.
- 2.4 During the tunnel establishment procedure, the PDG and the WAG exchange information via the 3GPP AAA Proxy in order to establish a filtering policy to allow the forwarding of tunnelled packets to the PDG. The 3GPP AAA Proxy requests the WAG to apply filtering policy based on information obtained from the PDG. The 3GPP AAA Proxy decides which filtering policy could be applied by the WAG according to local information (e.g. based on number of users, WAG capabilities, roaming agreement policy, etc).
3. Depending on internal configuration, or due to the failure of step 2.1 or 2.3, the WLAN UE initiates W-APN resolution and tunnel establishment with a PDG in HPLMN.
  - 3.1 WLAN UE constructs an FQDN using W-APN Network Identifier and the HPLMN ID as the Operator Identifier, and performs a DNS query to resolve it. The DNS response will contain one or more IP addresses of equivalent PDGs that support the requested W-APN in the HPLMN according to standard DNS procedures.
  - 3.2 The WLAN UE selects a PDG from the list received in step 3.1. If the DNS response contains IPv4 and IPv6 addresses, the WLAN UE has to select an address that has the same format as its own local IP address. If a PDG is finally selected, establishment of an end-to-end tunnel is performed between the WLAN UE and this PDG. The WLAN UE shall include the W-APN and the user identity in the initial tunnel establishment request.
  - 3.3 During the tunnel establishment, the PDG contacts the 3GPP AAA Server in the HPLMN for authorization of the WLAN UE for the W-APN being requested by the WLAN UE and to retrieve the information required for the mutual authentication part of tunnel establishment. As a result of successful mutual authentication the 3GPP AAA Server registers itself at the HSS (WLAN registration procedure). This action may be omitted, if the 3GPP AAA Server is already registered at the HSS. The 3GPP AAA Server shall be able to check that the user requesting the tunnel establishment has been already WLAN Access Authorized. Based on operator policy it shall be possible to turn this check on and off. The check may be based on the user's subscription

data, e.g. the user's subscribed services. If the check is not successful, the tunnel establishment request is rejected.

If the WLAN UE is not allowed to use a Home PDG to access the given W-APN according to his subscription, the 3GPP AAA Server shall send a rejection message to the PDG and then the tunnel establishment shall be rejected by the Home PDG. The 3GPP AAA Server shall provide the PDG with the WLAN UE's remote IP address, received from the HSS, when static remote IP address allocation is used. The 3GPP AAA Server shall provide PDG with the subscribed Charging Characteristics or W-APN Charging Characteristics.

3.4 During the tunnel establishment, the PDG and the WAG exchange information via the 3GPP AAA Server and 3GPP AAA Proxy in order to establish a filtering policy to allow the forwarding of tunnelled packets to the PDG. The 3GPP AAA Server requests to the WAG to apply filtering policy based on information obtained from the PDG. The 3GPP AAA Server decides which filtering policy could be applied by the WAG according to local information (e.g. based on number of user, WAG capabilities, roaming agreement policy, etc). The applied filtering policy is communicated to the Home-PDG.

### 7.9.1 Void

### 7.9.2 Subsequent authentication

In the case that the user attempts a subsequent tunnel establishment to a different PDG, it should be possible to avoid repeating the full authentication process and to perform fast re-authentication. Fast re-authentication is an optional feature and its activation is performed in the home operator's network.

### 7.9.3 Use of DNS

It shall be possible to restrict the propagation of DNS information used for the above mechanism to DNS servers controlled by the PLMNs and to DNS servers available only to authorised 3GPP WLAN UEs (i.e. those WLAN UEs which have successfully connected to a 3GPP Interworking WLAN.)

It shall be possible to configure multiple PDG addresses against a single FQDN in a manner which allows the load to be shared across these PDGs.

It shall be possible to configure IPv4 and IPv6 addresses against a single FQDN and to return these addresses together to the WLAN UE.

Note: The above shall be achieved by standard DNS mechanisms. The usage of TLD and the DNS query performed by the WLAN UE to resolve the W-APN are left to stage 3. Further details are in [5].

### 7.9.4 Subsequent tunnel establishment

The subsequent tunnel establishment should follow the same procedure as in the first tunnel establishment.

## 7.10 Tunnel disconnection procedures

Tunnel disconnection can be either:

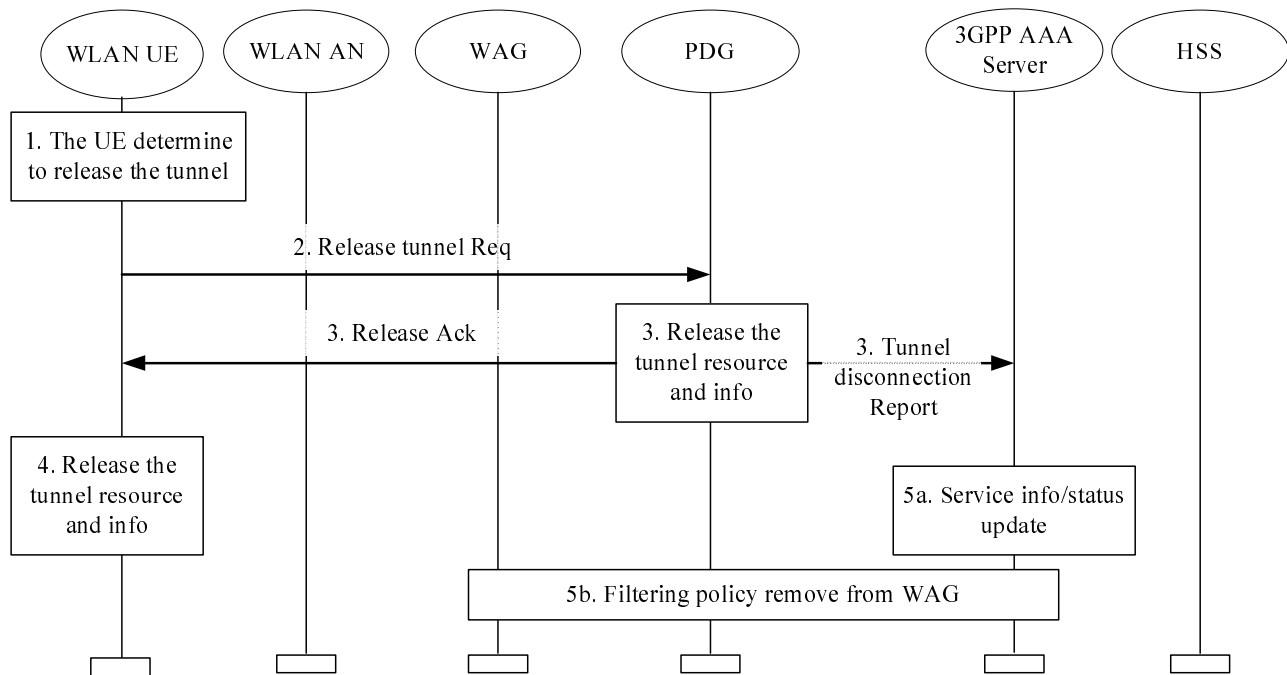
- Initiated from the WLAN UE, as a result of an explicit deactivation/de-registration from the service.
- Initiated from the PDG, e.g. due to timeout of the tunnel connection or request from the 3GPP AAA Server or other network entities.

Tunnel disconnection is specified for the following situations:

- Normal service termination resulting from an end user requesting termination of the end-to-end tunnel connection using tunnel control signalling or deletion of the IP bearers associated with a service,
- Service termination resulting from network operator intervention,
- Loss of radio connections which are used to transport the tunnel signalling.

The tunnel disconnection message exchanges between the WLAN UE and the PDG are performed basing on the specific tunnel control signalling protocol. The WLAN UE and the PDG release the control information associated with the tunnel during the exchange, and the PDG should send a tunnel release report to the 3GPP AAA Server to update the corresponding subscriber's service connection information and status in the 3GPP AAA Server, e.g. the service/tunnel connection activation info, the allocated IP address, etc. The filtering policy information applied on the WAG should also be removed, if necessary.

### 7.10.1 WLAN UE initiated tunnel disconnection



**Figure 7.12: WLAN UE initiated tunnel disconnection**

1. The WLAN UE determine to release the tunnel, e.g. due to the normal service termination operation.
2. The WLAN UE send a Release tunnel request to the PDG.
3. Upon receiving the Release tunnel request, the PDG sends a Release acknowledgement to the WLAN UE, releases the resources and the associated control information of the tunnel, and sends a Tunnel disconnection report to the 3GPP AAA Server.
4. Upon receiving the Release acknowledgement, the WLAN UE releases the resources and the control information of the tunnel.
5. Upon receiving the Tunnel disconnection report, the 3GPP AAA Server updates the related service information and/or status of the subscriber; and removes the filtering policy related to the disconnected tunnel from WAG if necessary.

### 7.10.2 The network initiated tunnel disconnection

1. The PDG determines to release the tunnel, e.g. due to timeout of the tunnel connection or a request from the 3GPP AAA Server, or due to a network initiated normal service termination or a service termination resulting from network operator intervention.
2. The PDG sends a Release tunnel request to the WLAN UE.
3. Upon receiving the Release tunnel request, the WLAN UE releases the resources and the associated control information of the tunnel, and sends the Release acknowledgement to the PDG.

4. Upon receiving the release acknowledgement, the PDG releases the resources, the associated control information of the tunnel, and the related service authorization information; and sends a Tunnel disconnection report to the 3GPP AAA Server.
5. Upon receiving the Tunnel disconnection report, the 3GPP AAA Server updates the related service information and/or status of the subscriber; and removes the filtering policy related to the disconnected tunnel from WAG if necessary.

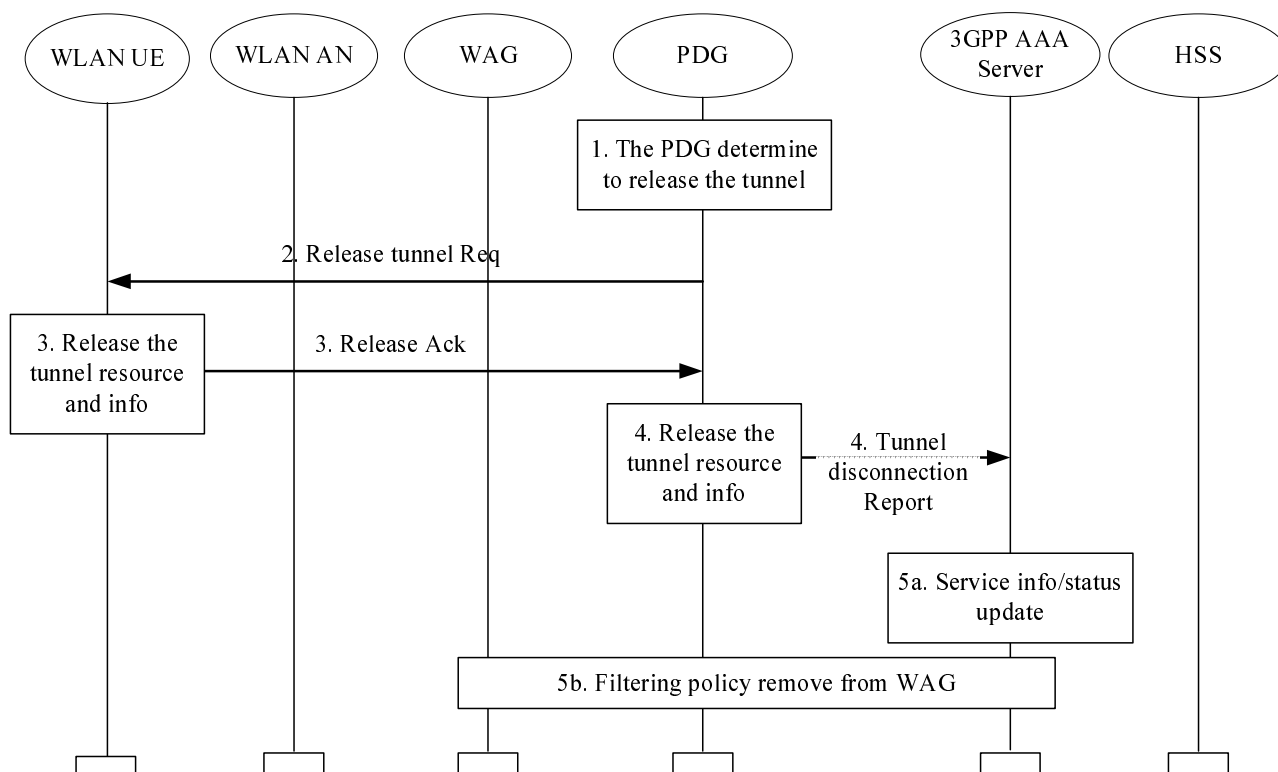


Figure 7.13: The network initiated tunnel disconnection

### 7.10.3 Disconnection of the last tunnel for a WLAN UE

If the PDG detects that the disconnected tunnel is the last tunnel between the PDG and the WLAN UE, then all the WLAN UE related authorization and profile information could be removed from the PDG during the tunnel disconnection process.

In case the 3GPP AAA Server decides to disconnect the WLAN UE from the WLAN after disconnection of the tunnel, a disconnection procedure will proceed as described in section 7.6.1 (steps 3-4).

After the WLAN UE was disconnected from the WLAN, the 3GPP AAA Server notifies the HSS using the Wx procedure "Purge" that the WLAN UE's registration in the 3GPP AAA Server has been deleted. In this case the HSS de-registers the 3GPP AAA Server (WLAN de-registration procedure).

## 7.11 The WLAN UE initiated WLAN AN Access disconnection

The WLAN UE may disconnect the from WLAN AN by:

- initiating a disconnection of the WLAN radio connection;
- initiating a disconnection of the WLAN IP connectivity.

### Disconnection of the WLAN radio connection

Upon receiving a WLAN radio disconnection request (e.g., Disassociation in case of IEEE802.11 WLAN AN) from the WLAN UE with the WLAN access connection, the WLAN AN should perform the 'disconnecting a subscriber by

WLAN AN' (section 7.5) during or after the WLAN radio disconnection, with or without confirm message to the WLAN UE.

### Disconnection of the WLAN IP connectivity

The UE initiated disconnection of the WLAN IP connectivity is usually performed before the disconnection of the WLAN radio connection and after the disconnection of the 3GPP PS access tunnels. However the WLAN UE may initiate a WLAN IP connectivity disconnection before the 3GPP PS access tunnels are disconnected. This will trigger the tunnel disconnection procedure specified in section 7.10.2.

If the WLAN UE initiates a disconnection of the WLAN IP connectivity:

1. The WLAN UE may initiate a disassociation after the disconnection procedure.
2. The WLAN AN stops the connection under the request of the WLAN UE, e.g. close the opened port to the WLAN UE.
3. The WLAN AN should perform the 'disconnecting a subscriber by WLAN AN' during or after the disconnection of WLAN access connection.

The WLAN AN should initiate an authentication or a disconnection of WLAN radio connection with this WLAN UE, if the WLAN UE keeps the WLAN radio connection without subsequent indication or requests in a certain period of time.

### The 3GPP PS Access tunnel disconnection

The UE initiated tunnel disconnection is usually performed before the disconnection of WLAN IP connectivity and the disconnection of the WLAN radio connection. However, the WLAN UE may directly initiate a disconnection of the WLAN radio connection as a fast disconnection option when tunnel connections with PDG exist. This will trigger the tunnel disconnection procedure specified in section 7.10.2.

## 7.12 User identity to HSS resolution

### 7.12.1 General

This section describes the resolution mechanism, which enables the 3GPP AAA Server to find the address of the HSS, that holds the subscriber data for a given user identity when multiple and separately addressable HSSs have been deployed by the network operator. This resolution mechanism is not required in networks that utilise a single HSS. An example for a single HSS solution is a server farm architecture. The NAI will be used as user identifier towards the SLF.

The subscription locator is accessed via the Dw reference point. The Dw reference point is the standard interface between the 3GPP AAA Server and the SLF. The synchronisation between the SLF and the different HSSs is an O&M issue.

The subscription locator is already defined in 3GPP TS 23.228 [24] for Cx and Sh interfaces.

The Dw interface provides:

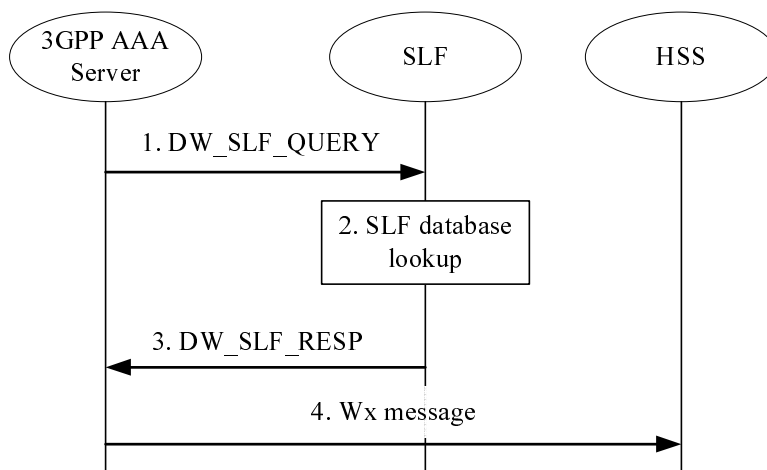
- an operation to query the subscription locator from 3GPP AAA Server
- a response to provide the HSS name towards 3GPP AAA Server.

By sending the Dw-operation DW\_SLF\_QUERY the 3GPP AAA Server indicates a user identity of which it is looking for an HSS. By the Dw-operation DW\_SLF\_RESP, the SLF responds with the HSS address. The 3GPP AAA Server may optionally store the HSS address for a given subscriber so subsequent queries to the SLF are not needed.

Subclause 7.12.2 presents an example of the session flow when the 3GPP AAA Server needs to query the SLF.



## 7.12.2 SLF query



**Figure 7.14: Query through SLF**

1. 3GPP AAA Server detects that it requires the user profile, the registration or new authentication vectors for a given 3GPP subscriber, so has to query for the location of the user's subscription data. The 3GPP AAA Server sends a DW\_SLF\_QUERY to the SLF and includes as parameter the user identity of the subscriber.
2. The SLF looks up its database for the queried user identity.
3. The SLF answers with the HSS address in which the user's subscription data can be found.
4. The 3GPP AAA Server can proceed by querying the appropriate HSS by Wx protocol.

# Annex A (informative): Reference Points Signalling Flows

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

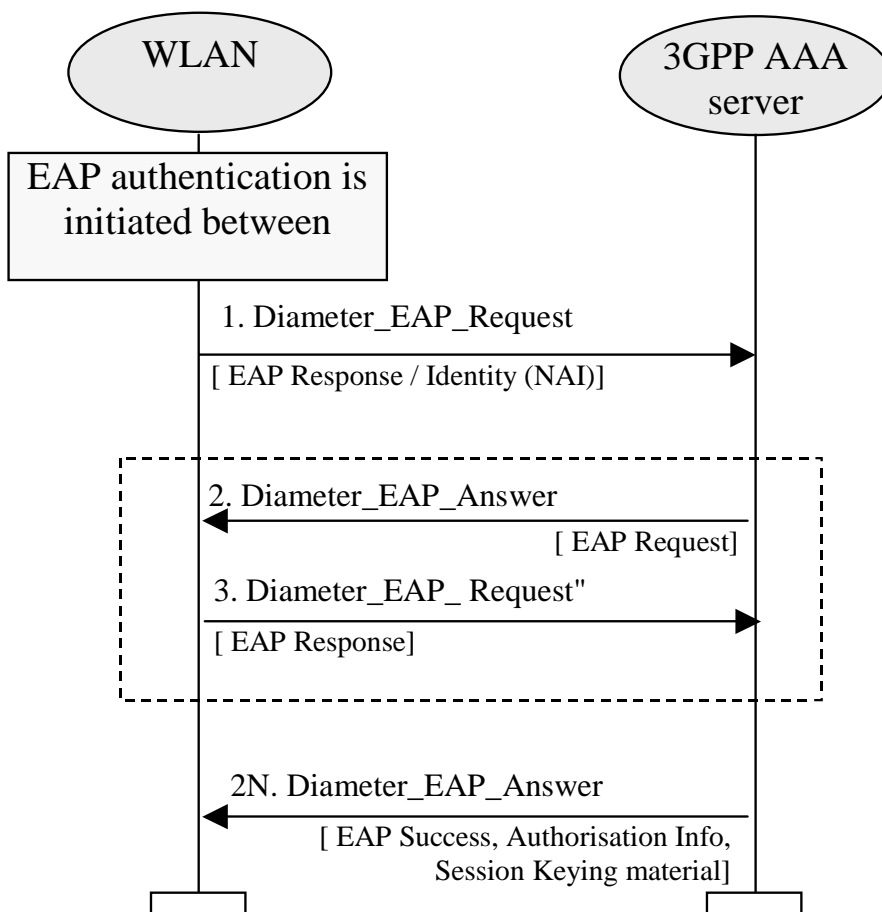
## A.1 Signalling Sequences examples for Wa Reference Point

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

The purpose of this signalling sequence is to carry WLAN UE - 3GPP AAA Server authentication and authorisation signalling over the Wa 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 Wa signalling sequence is initiated by the WLAN when authentication and authorisation 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 Wa 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. This message also carries a Session-ID used to identify the session within the WLAN and optionally a well-defined identification of the WLAN AN (e.g. transported in the NAS-Identifier parameter).

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 and authorised 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.

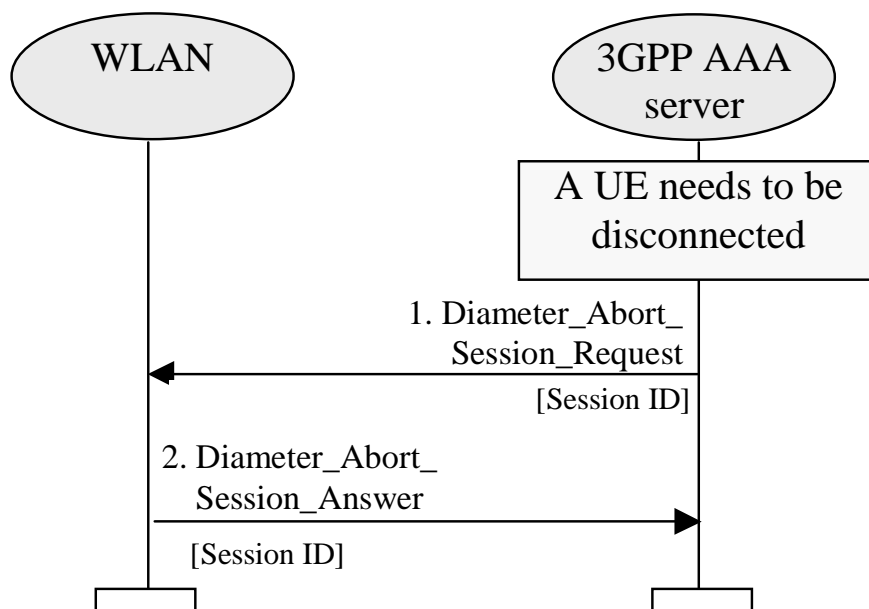
This `Diameter_EAP_Answer` message also carries the authorisation information (e.g. NAS Filter Rule or Tunnelling attributes) for the authenticated session. Message also carries the keying material from 3GPP AAA Server to WLAN to be used for the authenticated session by WLAN.

### 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.



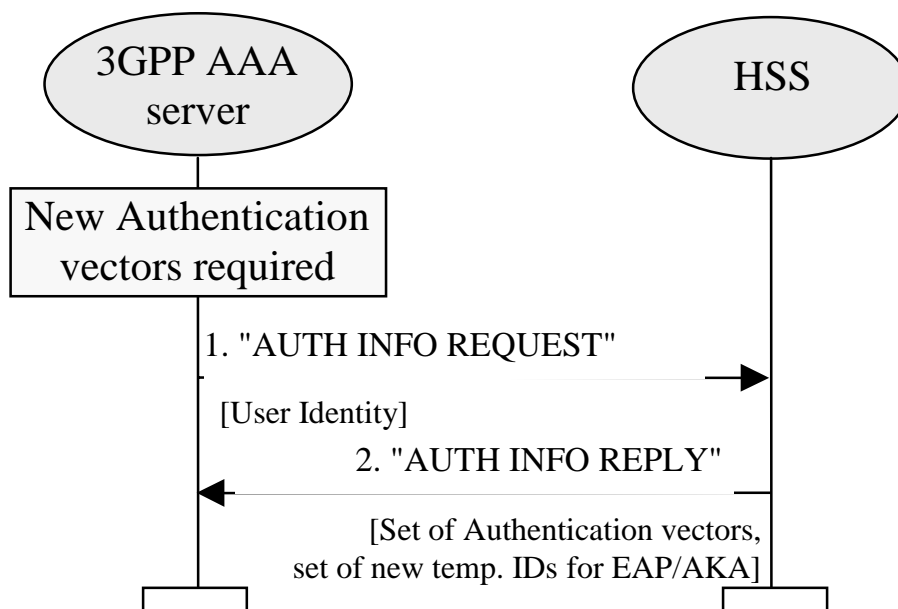
**Figure A.1.2: Signalling example on Wa Reference Point for User Purging**

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 *the IMSI, which is derived by the 3GPP AAA server from the username part of the NAI*

**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

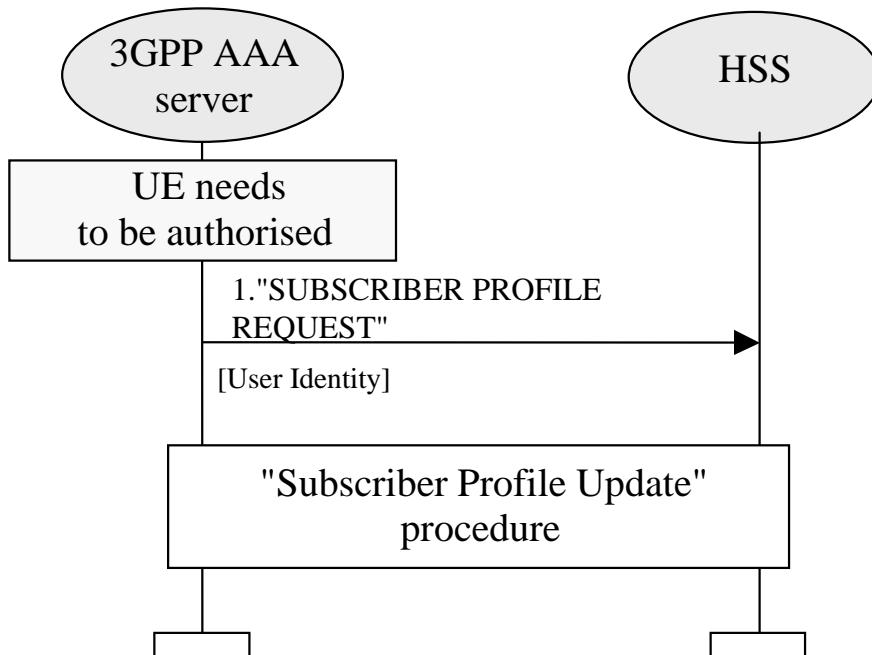
In case of UMTS AKA authentication, each authentication vector consists of RAND, XRES, AUTN, CK, and IK.

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.

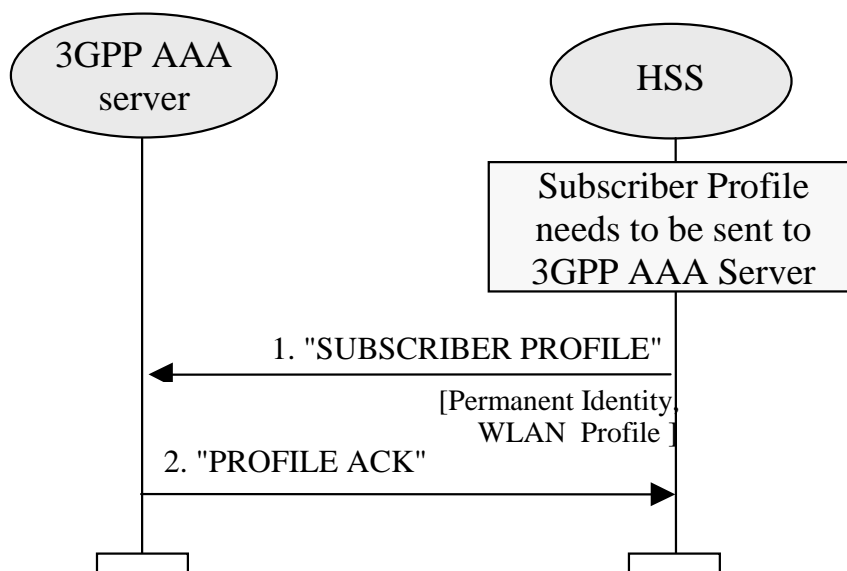
In case of USIM authentication (EAP/AKA) the utilised unique identifier shall be the pseudonym (associated with the IMSI) allocated in the previous authentication or, in case of the very first authentication, the IMSI.

*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

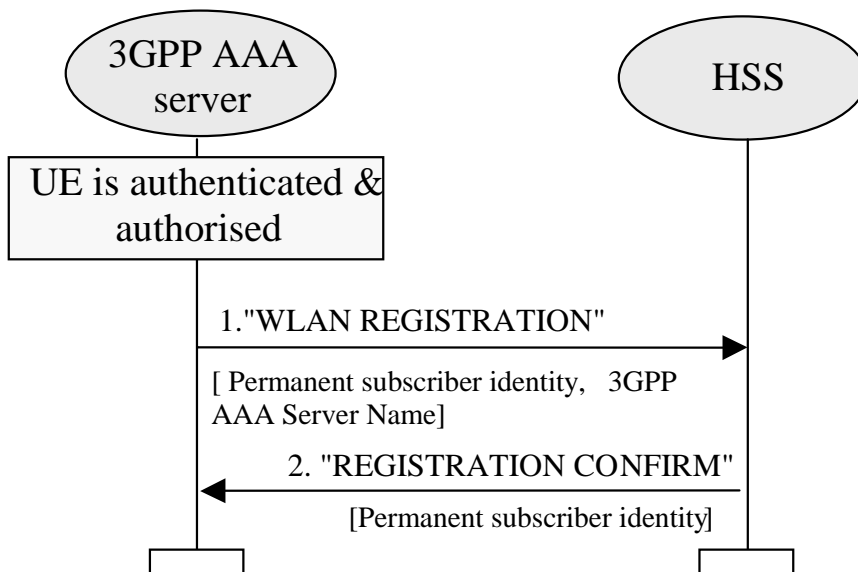
- Users permanent unique identifier. In case of USIM authentication (EAP/AKA) the utilised unique identifier shall be the IMSI
- service authorisation information,
- charging mechanism (offline / online),
- in case of online charging the DNS name of the subscribers online charging system

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.

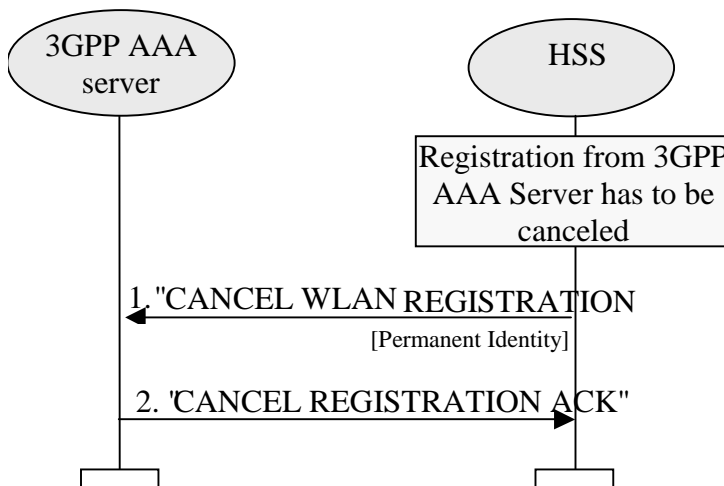


**Figure A.2.4: Signalling example on Wx Reference Point for Subscriber Registration**

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.



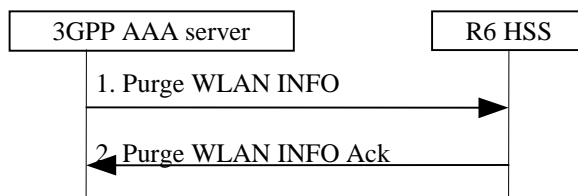
**Figure A.2.5: Signalling example on Wx Reference Point for Registration Cancellation**

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.

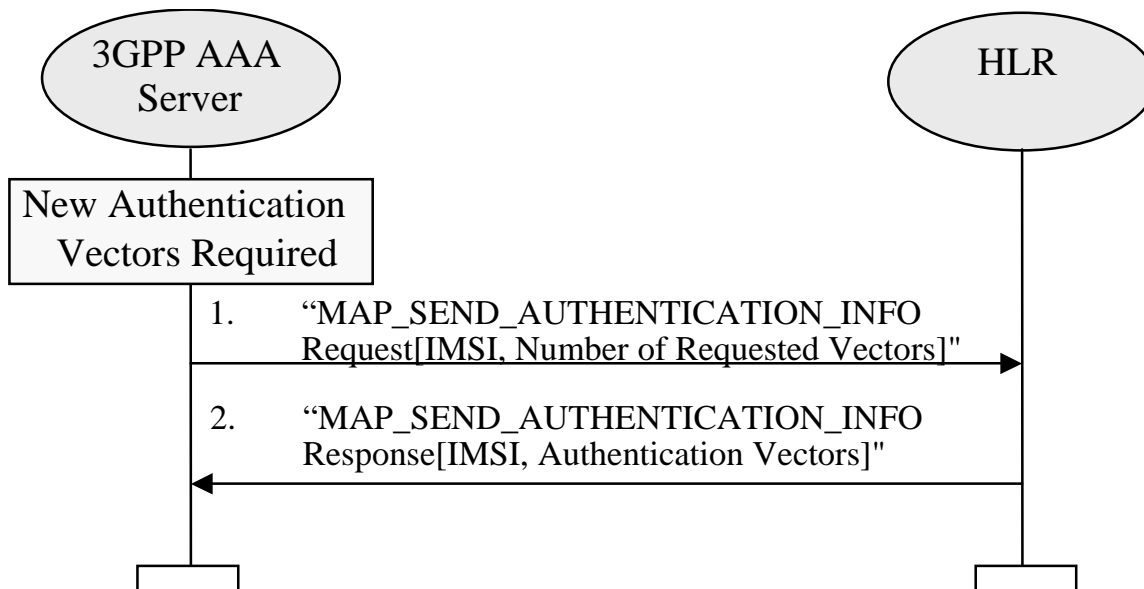


**Figure A.2.6: Signalling example on Wx Reference Point for Purge Procedure**

- 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.

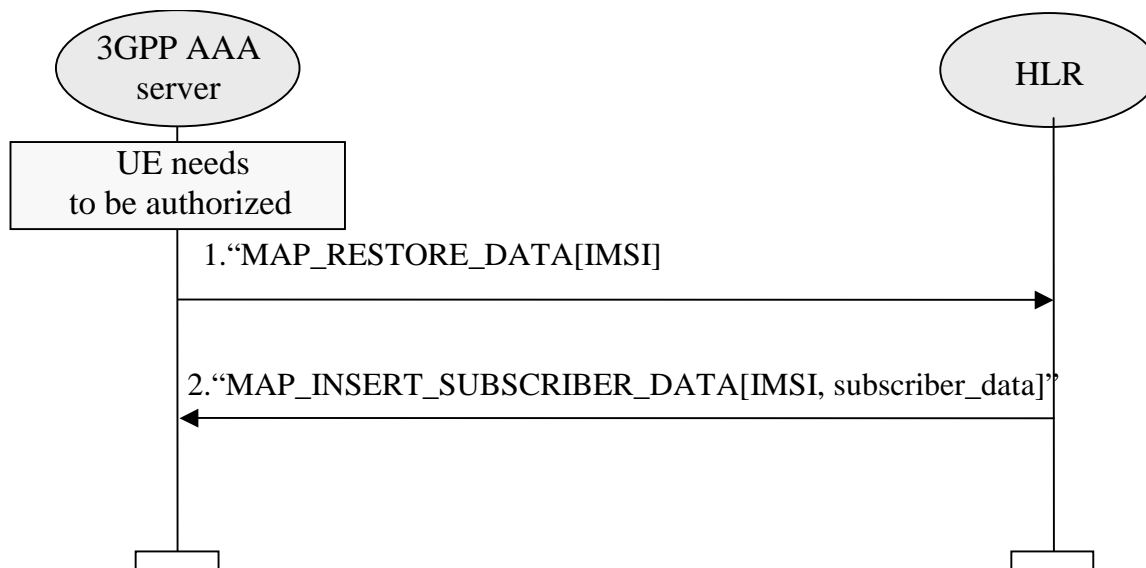
3GPP AAA server sends "MAP\_SEND\_AUTHENTICATION\_INFO Request" message to the HSS/HLR requesting a set of authentication vectors. In the message, the subscriber is identified by a unique identifier, IMSI.



- 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**

- 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.

- 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.

**Table A.4.1: HLR Parameters and use for WLAN Interworking**

| 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.

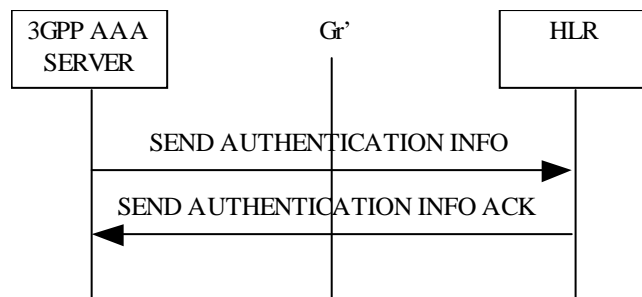


Figure A.4.1: infoRetrieval procedure

### 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.

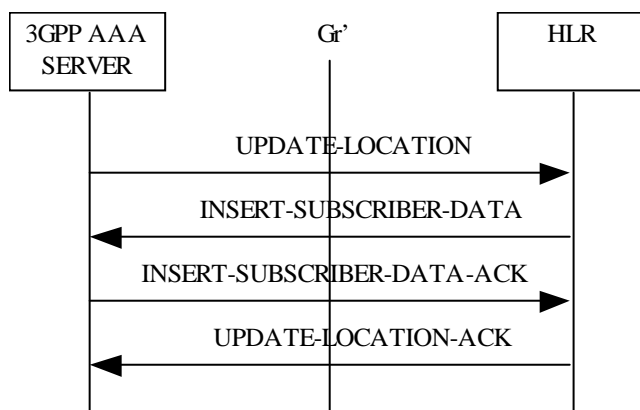


Figure A.4.2: gprsLocationUpdate procedure

## 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:

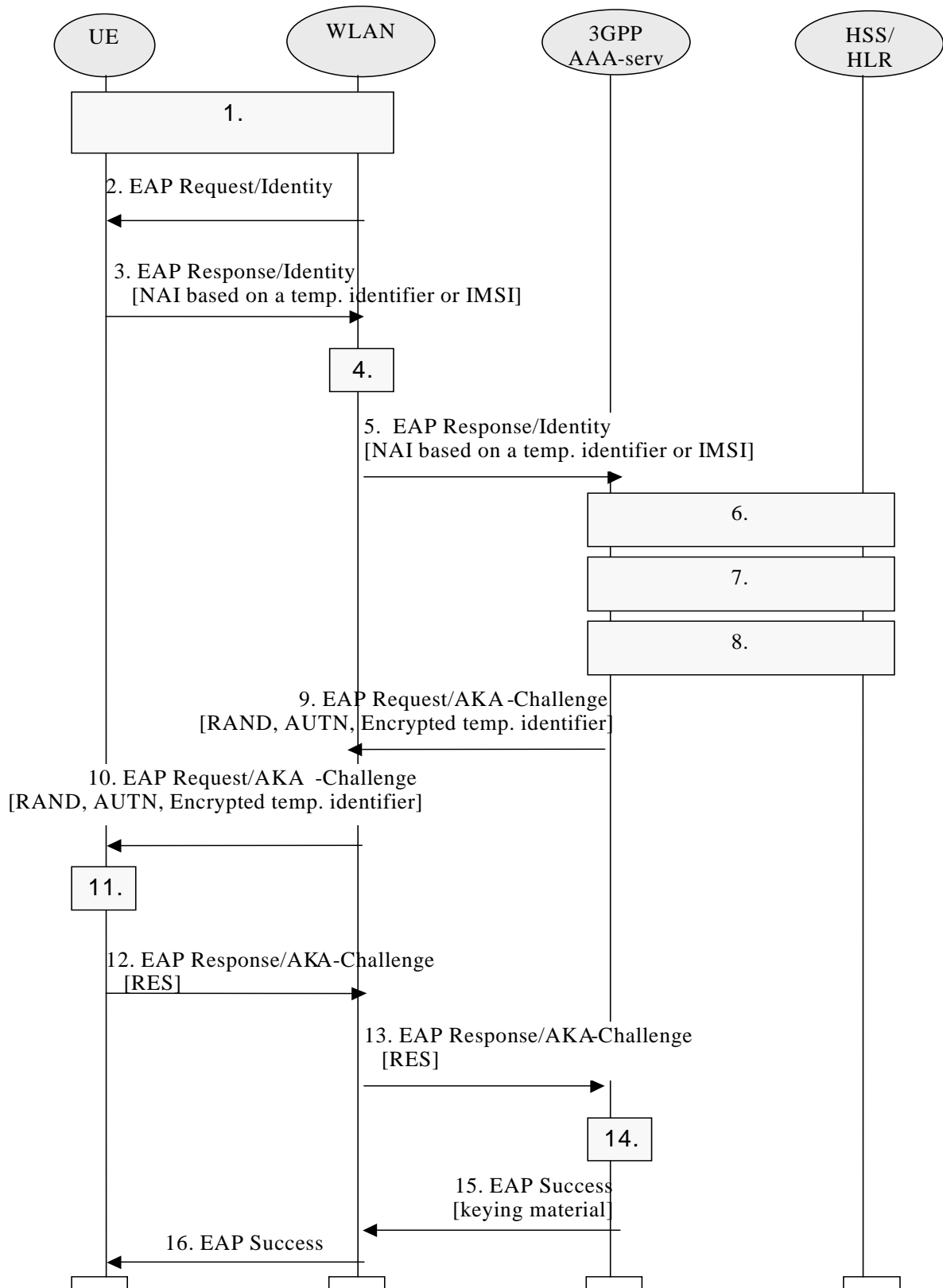


Figure A.5.1: Authentication based on EAP AKA scheme

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 [17]. 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:

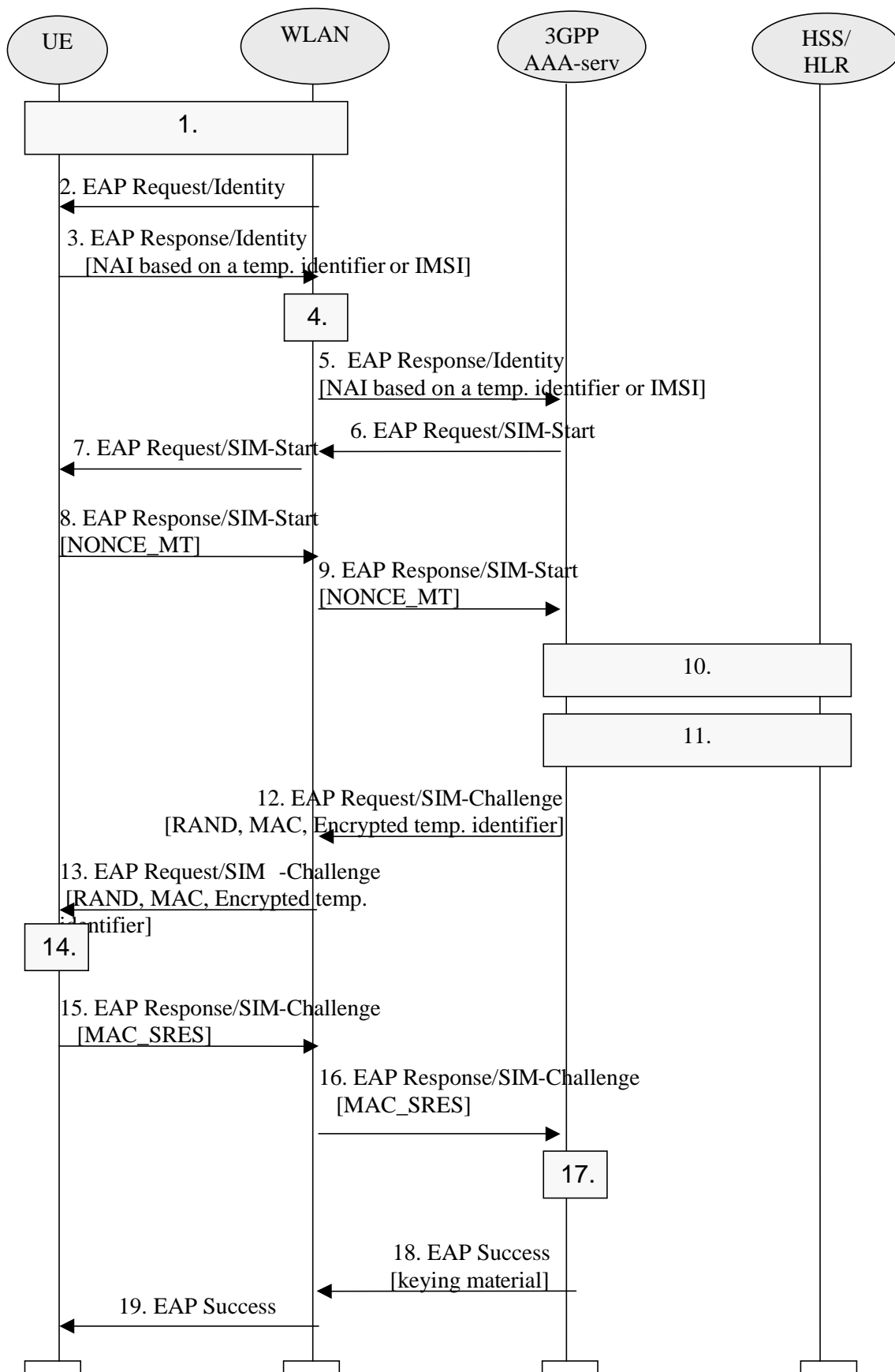


Figure A.5.2: Authentication based on EAP SIM scheme

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-pppext-eap-sim-06.txt).

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

NOTE 2: Diameter/RADIUS proxy chaining and/or Diameter referral can be applied to find the AAA server.

5. The 3GPP AAA server receives the EAP Response/Identity packet that contains the subscriber identity.
6. The 3GPP AAA Server guesses, based on the NAI, that the subscriber is a GSM user; hence it sends the EAP Request/SIM-Start packet to WLAN.
7. WLAN sends the EAP Request/SIM-Start packet to 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.**

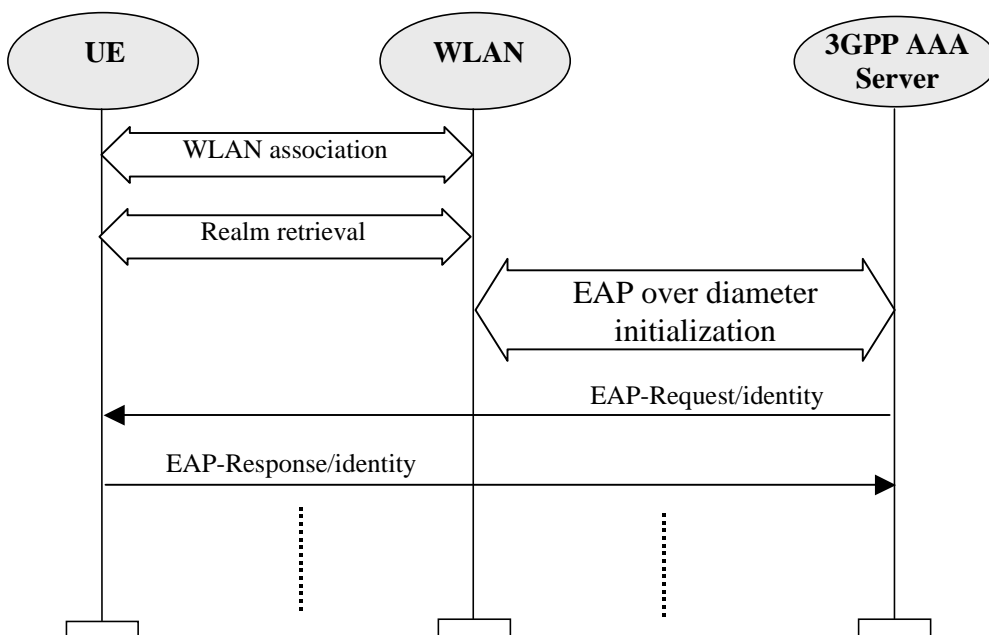


Figure A.5.3 : End-to-end EAP initialisation session

### A.5.4 Re-authentication message sequence chart

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

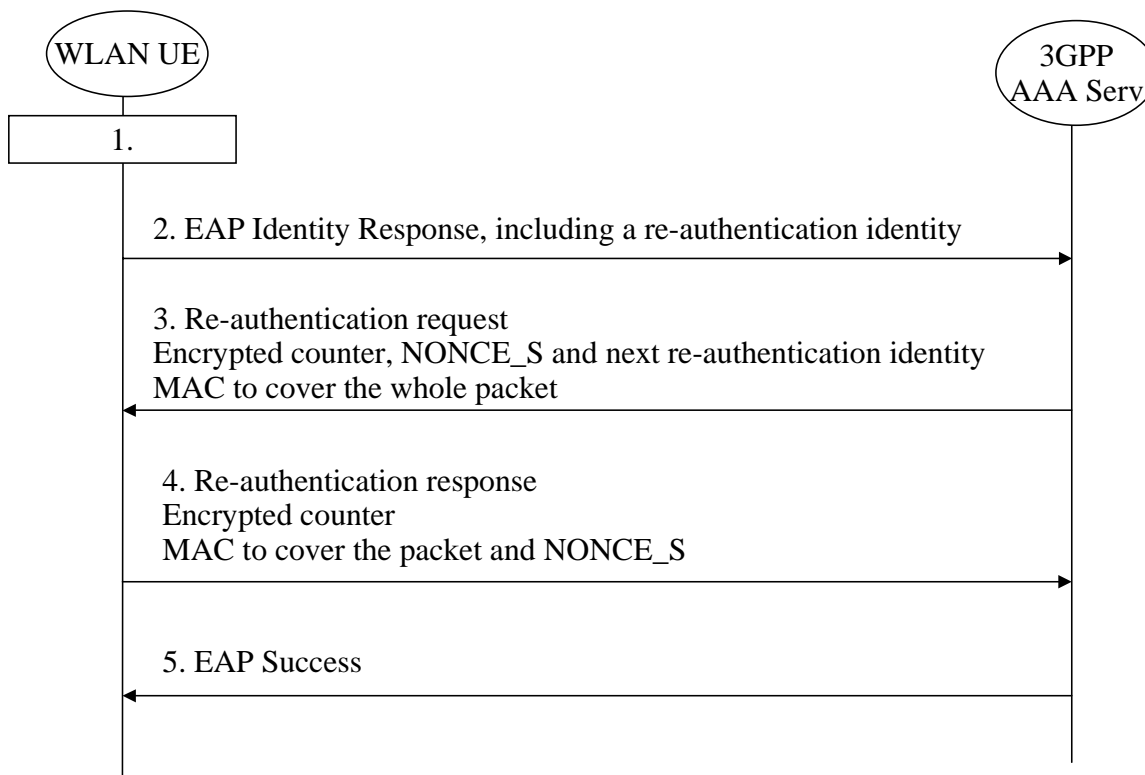


Figure A.5.4: Re-authentication signalling sequence

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<br><br>OFDM/CCK |
| Channel Width    | 22 MHz  | 1MHz   | 22 MHz  | 22 MHz                         | 22 MHz   |
| Range            | 150 ft (indoors)<br><br>300 ft (outdoors)   | 30 ft (with 1mW)   | 100 ft (indoors)<br><br>200 ft(outdoors)                          | Expected to be same as 802.11a | 150 ft (indoors)<br><br>(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)<br><br>(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<br><br>Susceptible to interference from Bluetooth and other devices                            | Wire Replacement;<br><br>Inexpensive<br><br>Low component count<br><br>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): Possible interworking architectures between WLAN AN and PLMN

### C.1 WLAN shared by (or connected to) multiple ISPs and PLMNs

This is typically when a WLAN AN is owned by an independent entity such as a hotel and the owner allows subscribers of ISPs to use their WLAN AN by using the ISP network. However, WLAN AN owned by an ISP or a PLMN may also allow other ISP/PLMN subscribers to use the WLAN in a similar way.

In this situation, the WLAN AN may be connected to multiple ISPs and PLMNs in the layer 2 for WLAN 3GPP IP Access as shown in Figure C.1.1. Another solution using DNS and NAT is described in C.2.3.

To this end, VLAN or other layer 2 tunnelling capabilities may be implemented in APs or access controller in WLAN AN in order to separate traffic of different networks.

The interface between the WLAN AN and the PLMN may be a Layer 2 tunnel, such as VLAN, Martini, or VPLS, etc. The WAG takes the role of the access router of the WLAN AN. This enables end to end tunnelling for WLAN 3GPP IP Access, even when the IP address of the PDG is not routable on the Internet.

The local IP address of a WLAN UE, when using WLAN 3GPP IP Access, belongs to the PLMN's IP address space. So, all the packets to a WLAN UE shall pass through the PLMN.

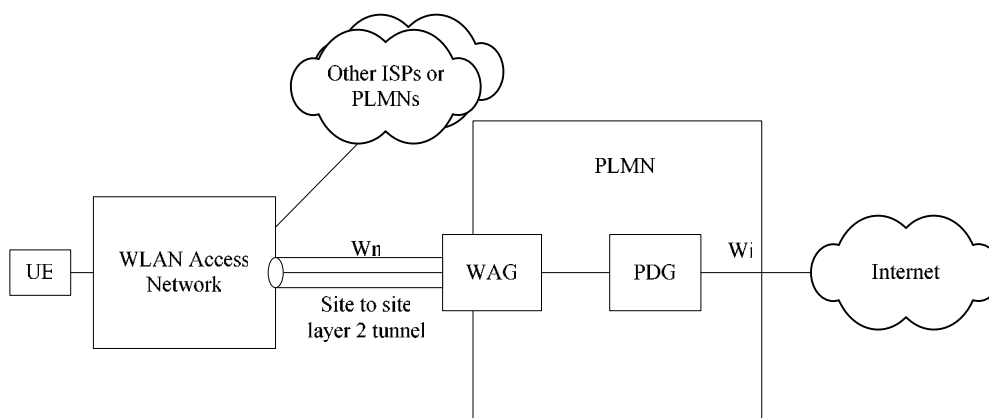


Figure C.1.1: Wn Interface when WLAN is connected to multiple ISPs and PLMNs

### C.2 Routing packets from WLAN UE when WLAN AN is connected to multiple VPLMNs/ISPs and it provides direct Internet access

#### C.2.1 Separating traffic for different VPLMNs

When a WLAN AN providing direct Internet access has connections to multiple VPLMNs it is necessary to route all the users' non-Internet traffic to the correct VPLMN whilst Internet traffic is routed directly to the Internet. The VPLMN identity is known to the WLAN AN at initial user authentication/authorisation, since the AAA signalling is routed to that VPLMN, and the Access-Accept received from that VPLMN.

Therefore, for each VPLMN there must be a separate (logical) router in the WLAN AN which has a connection to that VPLMN and also to the Internet (note: this is a 'logical' router – it doesn't represent a restriction on WLAN AN's

physical architecture). This router will receive all the traffic from WLAN UEs that are authenticated through that VPLMN. We call this the "WLAN AN Border Router for VPLMN X".

Various techniques could be used to ensure that all the WLAN UEs traffic is sent to the correct (logical) router, including:

- VLANs

A separate VLAN is defined for each VPLMN. The WLAN AN Border Router for a given VPLMN is only accessible from that VPLMN's VLAN. Appropriate RADIUS AVPs can be used to place the user onto a particular VLAN. On receiving this instruction, the WLAN AP performs VLAN tagging of all frames from the user. Since the WLAN AN knows the identity of the correct VPLMN at initial authentication/authorisation time, this instruction can be sent to the AP at this time.

As a result, all traffic from the user will be sent to the correct router.

- Compulsory tunnelling

Standard RADIUS AVPs are used to request the WLAN AP to establish a compulsory tunnel for the WLAN UEs frames towards the correct router. Again, this can be done at initial authentication/authorisation time.

Other techniques may also exist, but since there is no requirement for signalling from VPLMN to WLAN AN, the technique chosen is entirely a matter for the WLAN AN operator.

## C.2.2 Routing the traffic

The WLAN AN Border Router for a given VPLMN must distinguish Internet traffic (which should be sent directly to the Internet) from non-Internet traffic (i.e. packets to PDGs – which should be sent to the VPLMN).

One way to achieve this is for the WLAN AN to recognise the addresses of PDGs. Traffic to a known PDG address is routed to the VPLMN and other traffic to the Internet. There are several ways the WLAN AN could discover the PDG addresses:

- Statically – HPLMNs inform VPLMNs of their PDG addresses and VPLMNs inform WLAN ANs of these addresses together with any VPLMN PDG addresses. The addresses are statically configured in the routing tables of the WLAN AN Border Router.
- Dynamically - using standard IP routing protocols – HPLMNs must advertise routes to their PDGs across the inter-operator backbone. VPLMNs simply pass these advertisements to WLAN ANs along with advertisements of their own PDG addresses.

Configuration or advertisement of these addresses into the WLAN AN does not make these addresses routable from the Public Internet. Only users who are Authenticated and Authorised 3GPP WLAN UEs will be able to send packets to the (logical) WLAN AN Border Router, so only these devices can send packets to the configured/advertised addresses.

The above two approaches require that the addresses or prefixes configured or advertised are **not** also advertised over the public Internet. This is because although an address/prefix may be configured/advertised, there may be firewall rules or policies in the VPLMN which prevent packets being routed over the inter-operator backbone to that address. In that case, packets to that address would be dropped, meaning that any device re-using that address would not be routable at all from the WLAN UEs.

The solution is summarised in the figure below (assuming the VLAN option for dealing with multiple VPLMNs). Note that this is a logical view – the existence of two Border Routers with links to the Internet does not imply two physical elements/links.

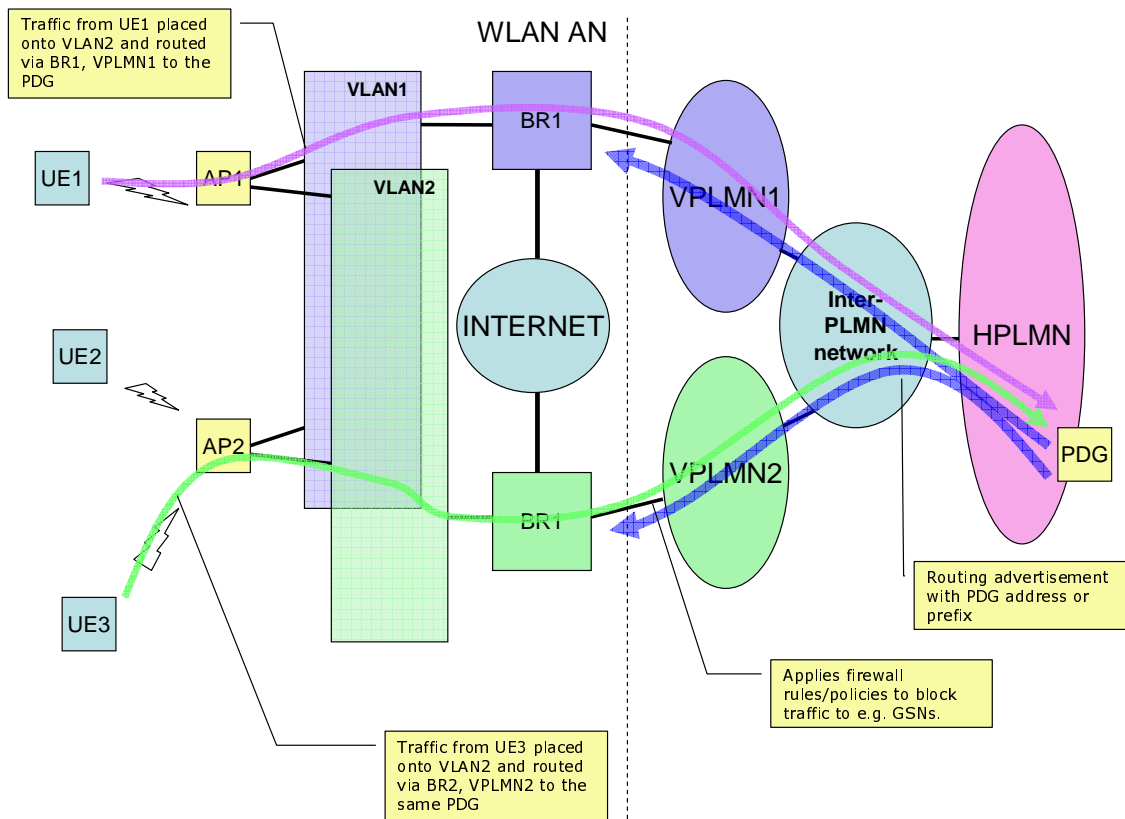


Figure C.2.1: Traffic routing based on the use of VLANs in the WLAN AN

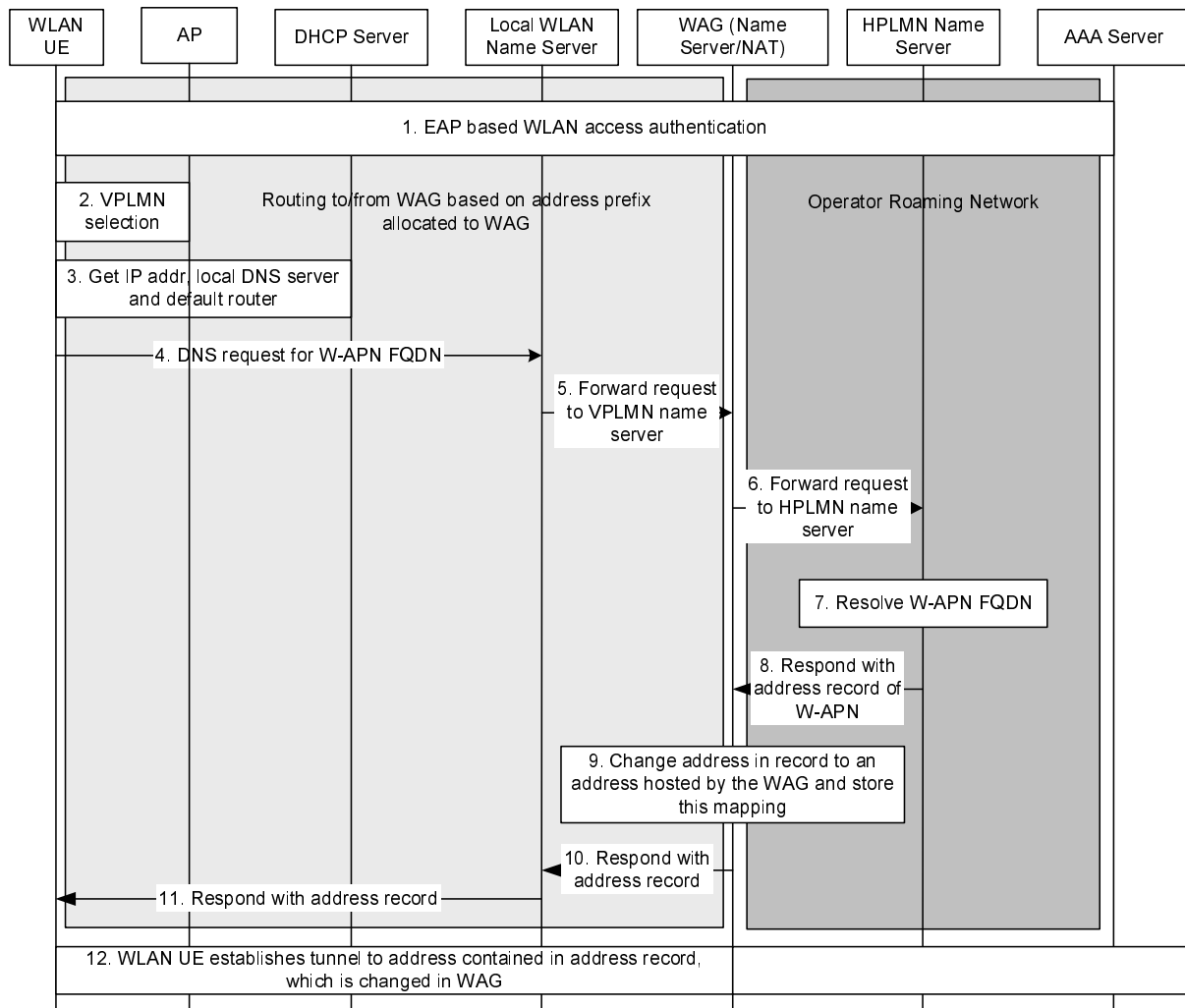
### C.2.3 Separating traffic to different VPLMNs using a combined DNS/NAT approach

If the WLAN UE is associated to the WLAN AN and authenticated through EAP, it can access the Internet directly (for WLAN Direct IP Access) or establish a tunnel to a PDG in the VPLMN/HPLMN to access 3GPP PS based services (for WLAN 3GPP IP Access). Both cases must be enabled in parallel. The WLAN UE performs a DNS query to resolve a W-APN to a PDG address. This IP address is the tunnel endpoint in the PLMN. If the PDG resides in the HPLMN, it must be possible to route traffic to the PDG through the selected VPLMN. The combined DNS/NAT approach as described in this chapter adds no requirements to the WLAN UE and HPLMN and uses only normal IP routing capabilities in the VPLMN.

The main idea is to use some kind of "reverse NAT" in the VPLMN that maps the PDG address received in the answer to the WLAN UE's DNS request to an address out of the address range of the VPLMN. Each PDG address is mapped to one VPLMN address, which may be a private address, depending on the addresses used in the WLAN AN. For simplicity (no new protocol needed) and performance reasons the VPLMN DNS proxy and the desired reverse NAT function are implemented on the WAG. Thus, inside of the NAT is the HPLMN address space, outside is the WLAN AN address space.

As the WLAN is directly connected to the VPLMN it is aware about the VPLMN IP addresses and can easily route WLAN 3GPP IP Access traffic to the correct VPLMN. The VPLMN maps the destination address of the IP packet to the stored PDG address and forwards the packet to the HPLMN. WLAN Direct IP Access traffic goes to the default route configured in the WLAN edge router, i.e. to the Internet.

The following figure shows the process of W-APN resolution and NAT in the VPLMN. The figure shows a local DNS server in the WLAN AN while it is also possible that the WLAN UE receives the address of a DNS server in the VPLMN by DHCP or during EAP authentication. If the WLAN UE wants to access a PDG in the HPLMN, the W-APN indicates the HPLMN and optionally the VPLMN, otherwise the W-APN indicates the VPLMN only.



**Figure C.2.2: DNS controlled reverse NAT procedure**

1. WLAN access authentication procedure between WLAN UE and AAA server based on EAP.
2. WLAN UE retrieves PLMN list from WLAN and selects a preferred VPLMN.
3. WLAN UE gets transport IP address, local name server (optionally) and default router address via DHCP.
4. WLAN UE builds W-APN FQDN indicating VPLMN (optionally) and HPLMN and sends DNS request to local name server or directly to the name server in the VPLMN.
5. Local name server inspects W-APN FQDN and forwards DNS request to VPLMN name server. VPLMN name server is implemented together with a "reverse" NAT and probably a Firewall on the WAG.
6. VPLMN name server inspects W-APN FQDN and forwards DNS request to HPLMN name server through GPRS roaming network.
7. HPLMN name server resolves W-APN.
8. HPLMN name server responds to VPLMN name server with an address record of the W-APN.
9. VPLMN name server (acting as DNS Proxy) optionally changes the PDG address contained in the address record to an address of the WAG address space (this address may be a private address) and stores the mapping between the two addresses. The new address must be routable within the WLAN to the WAG. Changing the addresses may be an option configurable by the operator.
10. VPLMN name server responds the address record to local name server.
11. Local name server responds the address record to WLAN UE.



12. WLAN UE establishes tunnel to the address contained in the address record. This may be an address hosted by the WAG (otherwise it is the PDG address). This address is changed ("NATted") at the WAG to the "real" PDG address.

### C.3 WLAN AN exclusively owned by and connected to a single PLMN

This is when a PLMN operator installs its own WLAN AN without any connections to other ISPs or PLMNs.

In this case, WLAN AN can be regarded as an extension of the PLMN's IP network and no tunnel is required between WLAN AN and PLMN. The local IP address of a WLAN UE in WLAN 3GPP IP Access belongs to the PLMN's IP address space.

### C.4 WLAN AN connected to a single ISP

This is when WLAN AN is solely connected to an ISP's backbone network. WLAN AN is regarded as an extension of the ISP's backbone network. Many legacy WLAN ANs can be categorized to this case

The connectivity between the WLAN AN and the PLMN is in layer 3 through the ISP's backbone network as shown in Figure C.4.1.

This kind of WLAN AN supports WLAN Direct IP Access as defined in the 3GPP TS 23.234, i.e. the authenticated WLAN UE can access the Internet directly via the ISP.

For WLAN 3GPP IP Access, the local IP address of a WLAN UE is generally allocated by the ISP and it belongs to the ISP's IP address space. When PLMN allocates WLAN UE's local IP address, a layer 2 tunnel is required.

When the end to end tunnelling is used between a WLAN UE and a PDG and the IP address of the PDG is non-routable in the Internet, an additional means is required for routing the packets to the PDG and to meet the routing enforcement requirement.

It is FFS for methods to enable WLAN 3GPP IP Access for this kind of WLAN AN.

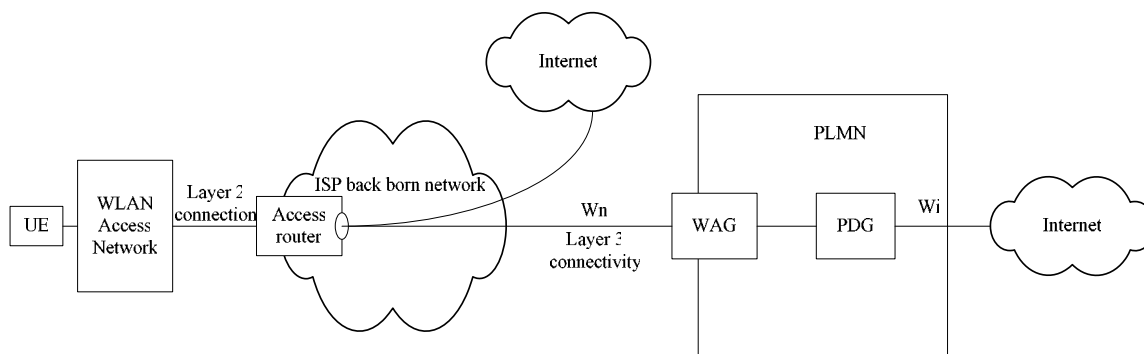


Figure C.4.1: Wn Interface when WLAN is connected to a PLMN through an ISP

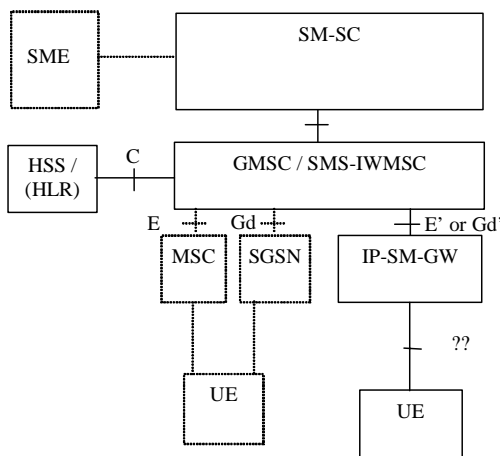
## Annex D (normative): Short Message Service

### D.1 Architecture for support of SMS

The architecture for support of IP delivery and origination of SMS messages is illustrated in figure D.1. The SM-SC and GMSC/SMS-IWMSC are defined in 3GPP TS 23.040 [6]. The IP Short Message Gateway IP-SM-GW communicates between the IP client and the GMSC/SMS-IWMSC.

The intention of this architecture is that it could be realised through re-use of existing messaging protocols supported by the UE e.g. IMS or MMS. The primary purpose of this architecture description is therefore to describe the interaction between the IP SM Gateway and the existing elements supporting the Short Message Service (GMSC/SMS-IWMSC, SM-SC and HLR/HSS).

The IP SM Gateway should be considered as consisting of all the functional entities needed to interwork between the chosen existing messaging protocol(s) and the existing SMS elements. For example, in the case IMS Messaging is chosen, the requirements on the IP SM Gateway specified here could be met by a combination of the CSCFs and an IMS Application Server which interworks to the GMSC/SMS-IWMSC.



**Figure D.1: Architecture for SMS support with an IP attached terminal**

#### D.1.1 IP Short Message Gateway (IP-SM-GW)

The IP-SM-GW shall provide the protocol interworking for delivery of the short message between the IP client and the GSM/UMTS network. The functions of this network element are:

- To connect to the GMSC using established MAP protocols over SS7, appearing to the GMSC as an MSC or SGSN using the E or Gd reference points
- To connect to the SMS-IWMSC using established MAP protocols over SS7, appearing to the SMS-IWMSC as an MSC or SGSN using the E or Gd reference points
- To communicate with the IP client using IP based protocols maintaining the format and functionality of the SMS message. It is intended that existing messaging protocols supported by the UE should be reused for this purpose.
- To maintain the association between the MSISDN and the IP address of the terminal
- Support registration and authentication of the UE for SMS services
- Support of security associations between UE and IP-SM-GW

## D.1.2 HLR/HSS

In the routing of an SMS message, the SMS-GMSC performs a MAP request to the HLR/HSS 'send routing information for short message' as defined in 3GPP TS 29.002 [10] to determine the address of the MSC or SGSN to which to route the short message. When the UE is connected only to a GSM/UMTS network, the 'send routing information for short message' returns the address of the MSC or SGSN for delivery of SMS message. In the event that the UE is registered with an IP Short Message Gateway, the HLR/HSS may return the address of the IP-SM-GW in the 'send routing information for short message'. As such, the HLR/HSS shall support the following functionality:

- An indication that the terminal is registered with an IP Short Message Gateway (e.g. an internal flag) for delivery of SMS
- The SS7 MAP address of the IP-SM-GW
- The logic necessary to act on the fact that the terminal is IP connected and return the IP-SM-GW address

The mechanism for prioritizing whether the short message is delivered via a GSM/UMTS or a WLAN connection when the terminal is simultaneously connected to both access networks is outside the scope of this specification.

### D.1.2.1 Indication that the terminal is registered with an IP Short Message gateway

In order to be able to return the address of the IP-SM-GW in response to a 'SendRoutingInfoForShortMsg' request from the GMSC, the HLR/HSS needs to have an indication that the terminal is registered with an IP Short Message Gateway and that this is the preferred method for delivery of short messages.

The IP Short Message Gateway maintains the UE's registration status. On registration, the IP Short Message Gateway shall send a message to the HLR/HSS indicating that the UE has successfully registered.

### D.1.2.2 The address of the IP-SM-GW

The address of the IP-SM-GW associated with a registered UE may either be pre-defined as a single address in the HLR/HSS or dynamically configured during the registration process, depending on information received from the IP-SM-GW.

NOTE: In the context of WLAN, the IP address of the WLAN UE is the remote IP address.

## D.1.3 Reference points

The need for additional reference points is for further study.

## D.2 Procedures

### D.2.1 Registration with IP Short Message Gateway

#### D.2.1.1 General

Before originating or receiving SMS messages over IP, the UE must register with an appropriate IP Short Message Gateway.

The registration process shall:

- Provide mutual authentication between UE and IP Short Message Server
- Provide for authorisation of the UE for the SMS service
- Establish registration state for the UE within the IP Short Message Server

On completion of registration the IP Short Message Gateway shall inform the HLR/HSS that the user has registered.

NOTE: This registration may be implicitly provided through registration to an existing messaging service which is providing interworking to SMS (assuming SMS interworking is allowed according to the user's subscription).

### D.2.1.2 Information flows for registration

FFS.

## D.2.2 De-registration from the IP Short Message Gateway

### D.2.2.1 General

De-registration of the UE from the IP Short Message Gateway may be triggered by an explicit UE-initiated deregistration procedure with the IP SM GW or automatically by the IP SM GW on SMS delivery failure.

The explicit UE-initiated de-registration procedure may be used when the UE is aware that it is about to loose IP connectivity or when the terminal is shut down.

After de-registration, the IP SM GW shall inform the HLR so that subsequent SMS messages shall be delivered instead over the CS or PS domain.

NOTE: This de-registration may be implicitly provided through de-registration from an existing messaging services which is providing SMS interworking.

### D.2.2.2 Information flows for UE-initiated de-registration

FFS.

### D.2.2.3 Information flows for automatic de-registration

FFS.

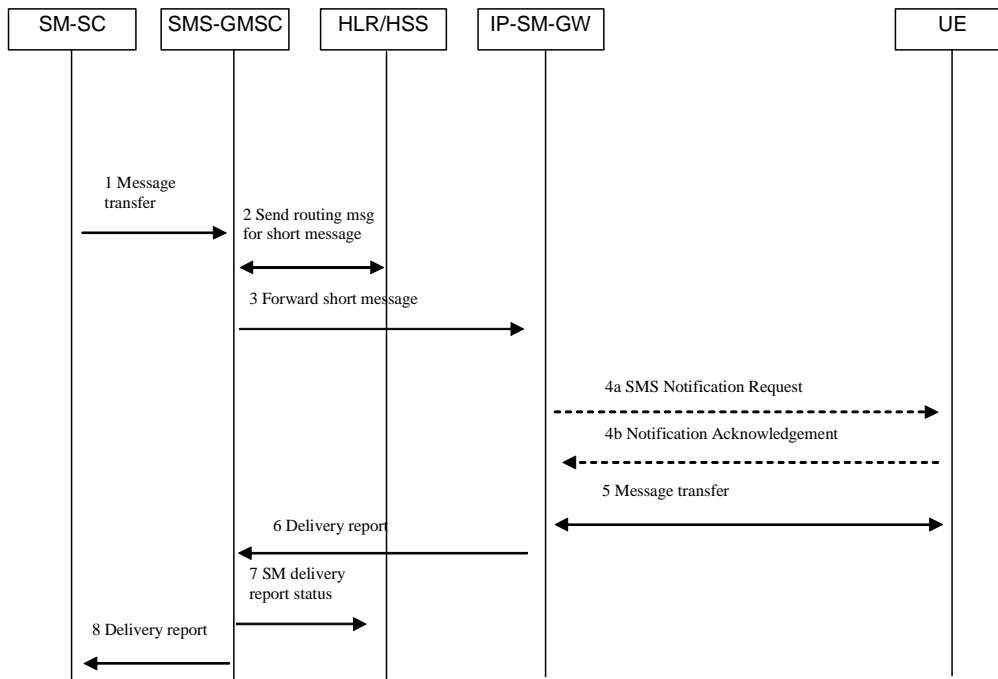
## D.2.3 Delivery of short messages

An SMS message destined for a particular terminal (with a destination address identified by a MSISDN) is originated by an SME and is sent to the SM-SC associated with that SME in accordance with 3GPP TS 23.040 [6]).

### D.2.3.1 Message Information flows for IP terminated short messages

The information flow for transport of the IP terminated short message from the short message service centre (SM-SC) to the IP client on the UE is shown in figure D.2.

The SMS may either be delivered directly to the UE once the IP-SM-GW has received the short message (direct method), or alternatively a notification may be used (notification method). In the notification method, the IP-SM-GW sends a message to the UE that a short message is available and awaits a response from the UE to determine if the user wishes to receive the message.



**Figure D.2: SMS delivery to IP terminal**

- 1) The SM-SC forwards the SMS message to the GMSC
- 2) The GMSC interrogates the HLR/HSS to retrieve routing information `sendRoutingInfoForShortMsg` for the UE. When a user is registered on a WLAN network for delivery of SMS messages, the HLR/HSS returns the address of IP-SM-GW (rather than address of appropriate MSC or SGSN)
- 3) GMSC delivers the SMS to IP-SM-GW using protocols as if it was a message to an MSC or SGSN.
- 4a) When notification method of delivery is used, the IP-SM-GW sends an SMS notification request to the UE to inform it that an SMS message is available for delivery.
- 4b) When notification method of delivery is used, on receipt of the SMS notification message, the UE responds with a notification acknowledgement indicating whether it wishes to receive the SMS message.
- 5) In the event that the direct method of delivery is used, or that a positive acknowledgement is received from the UE in response to the SMS notification request, the IP-SM-GW delivers SMS to IP client using e.g. WAP, SMPP, MMAP, XML, SIP (e.g. IMS client), SMTP, IMAP.
- 6) IP-SM-GW sends delivery report back to SMS-GMSC (see 3GPP TS 23.040 [6])
- 7) SMS-GMSC sends SM delivery report to HLR/HSS (see 3GPP TS 23.040 [6])
- 8) SMS-GMSC sends SM delivery report to SM-SC (see 3GPP TS 23.040 [6])

Error handling is performed using the mechanisms defined in 3GPP TS 23.040 [6].

## D.2.4 Short message origination

An SMS message destined for a particular terminal (with a destination address identified by a MSISDN) may be originated by the UE and sent, to the IP-SM-GW using an IP based protocol.

### D.2.4.1 Message Information flow for IP originated short messages

The information flow for transport of the IP originated short message to the short message service centre (SM-SC) is shown in figure D.3. This is based on the message sequence flow in 3GPP TS 23.040 [6], maintaining where possible the existing message sequences.

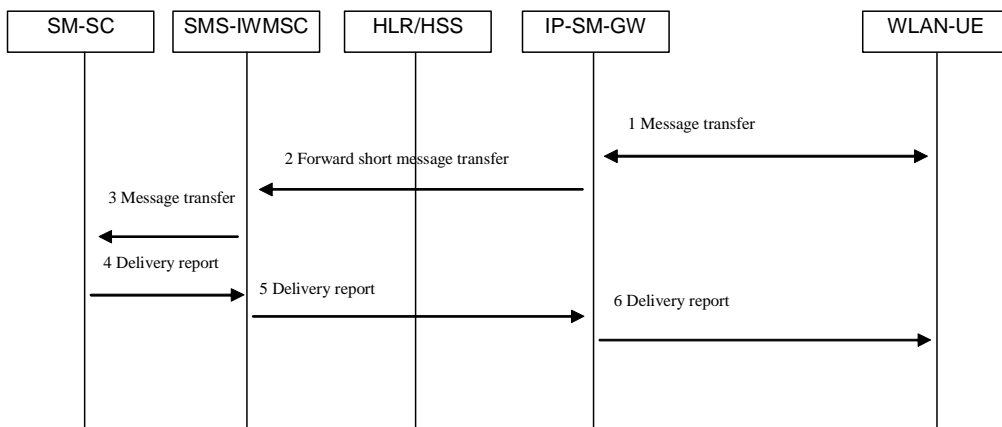


Figure D.3: SMS origination from IP terminal

- 1) IP client delivers SMS message to the IP-SM-GW, using e.g. WAP, SMPP, MMPP, XML, SIP, SMTP.
- 2) IP-SM-GW extracts the SMS message and forwards it to SMS-IWMSC using standard MAP (as 3GPP TS 23.040) exactly as if it was an MSC or SGSN.
- 3) The SMS-IWMSC forwards the SMS message to the SM-SC (see 3GPP TS 23.040 [6])
- 4) SM-SC sends delivery report SMS-IWMSC (see 3GPP TS 23.040 [6])
- 5) SMS-IWMSC sends delivery report to IM-SM-SC (see 3GPP TS 23.040 [6])
- 6) IP-SM-GW sends delivery report to IP-UE.

Error handling is performed using the mechanisms defined in 3GPP TS 23.040 [6].

### D.3 Support of SMS over WLAN interworking

This subclause describes the use of the above mechanism with the WLAN interworking system. For this purpose, the WLAN-UE needs IP connectivity. The WLAN-UE gets IP connectivity by establishing a tunnel to an appropriate home network PDG. The registration of WLAN-UE for SMS services occurs over this tunnel. This tunnel shall be maintained for use with SMS services while the WLAN-UE is registered with IP-SM-GW. It will be used for sending or receiving of any SMS messages to and from the WLAN-UE.

Figure 8.4 below shows a complete call flow, from WLAN tunnel establishment through SMS registration to the sending of an SMS by the UE. Note that Tunnel Establishment and registration with an IP-SM gateway may occur some time before a message needs to be sent since the UE also needs to be registered with the IP-SM-GW in order to receive SMS messages.

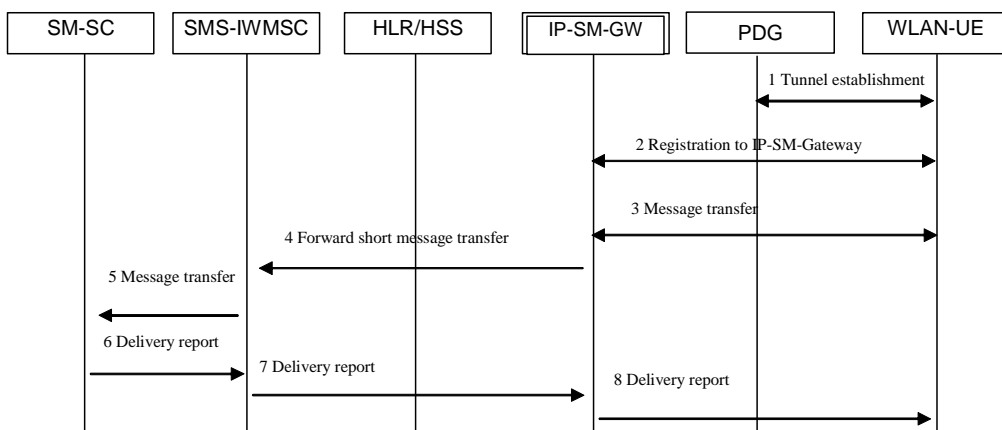


Figure D.4: Complete SMS call flow with WLAN interworking

# Annex E (informative): Information on the discussed tunnel switching alternative

*Editor's Note: The content of this annex does not contain any information relevant to the normative part of this specification and is intended to be removed at a later stage once Stage 3 work is more stable.*

## E.1 Non Roaming WLAN Inter-working Reference Model

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

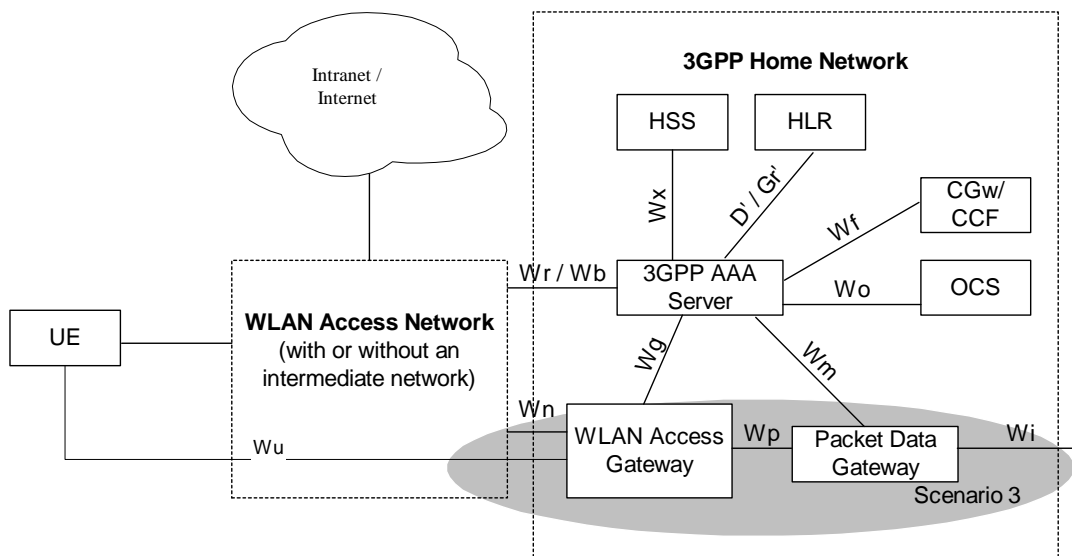


Figure E.1.1: Non Roaming Reference Model

## E.2 Roaming WLAN Inter-working Reference Model

Figure E.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<sub>x</sub> and W<sub>o</sub> reference points are intra-operator. The 3GPP network interfaces to other 3GPP networks, WLANs, and intermediate networks via the W<sub>a</sub> reference point.

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.

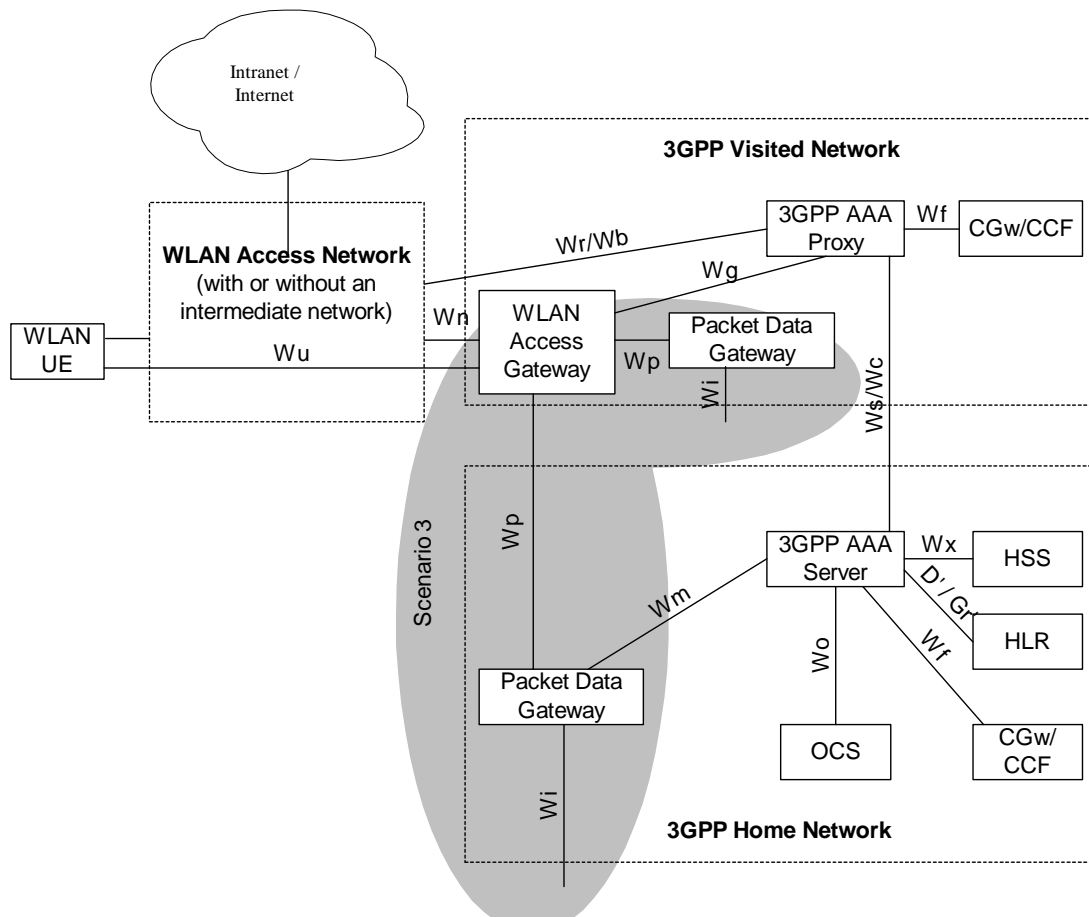


Figure E.2.1: Roaming Reference Model

### E.3 WAG Description

Support of the WAG for WLAN 3GPP IP Access 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.

### E.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 WLAN Direct IP Access.

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.

## E.5 Wn Reference Point

Reference point Wn is located between the WLAN Access Network and the WAG for user data traffic.

## E.6 Wp Reference Point

Reference point Wp is located between the WAG and the PDG. 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 Wp serves a similar purpose as the connecting network entities of the Gn/Gp interface in GPRS; the GTP protocol would be considered as a candidate for the Wp reference point.

## Annex F (normative): Information on re-using the GGSN to implement the PDG function

This annex does not introduce new normative requirements for the PDG.

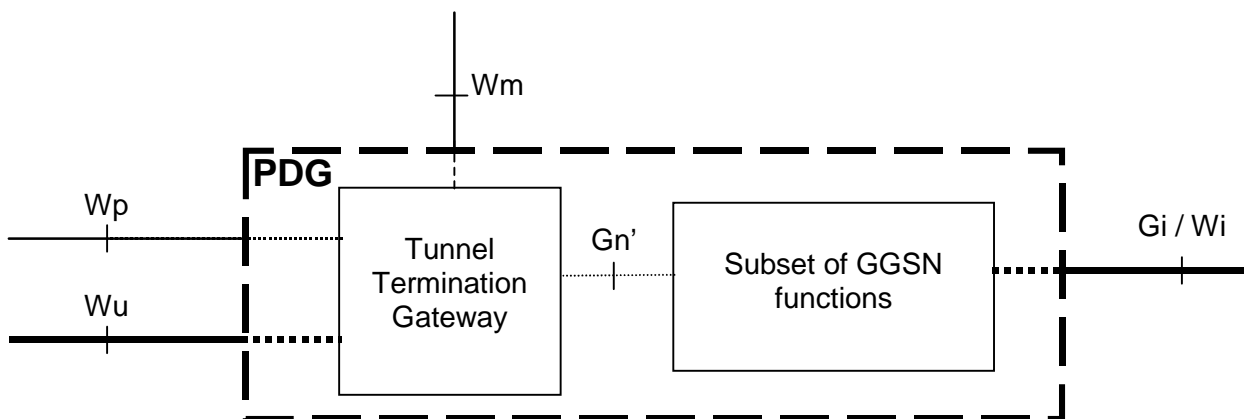
### F.1 Introduction

This section provides information on how to re-use existing GGSN deployments to implement the PDG functionality via using a subset of the Gn reference point (denoted here as Gn'). The Gn' reference point provides means where GPRS mobile operators can reuse existing infrastructure and functionality for a user accessing from a WLAN UE. By using this existing standardized reference point, interoperability towards the Gateway GPRS Support Nodes (GGSN) is assured. Such a PDG implementation allows re-use of existing GGSN functionality without upgrading GGSNs. For example, GGSN functions, which are used in this case are:

- Charging Gateway interfaces;
- IP address allocation;
- Authentication in external networks;
- Single access to 3GPP PS domain services.

Traffic Plane Functionality in the GGSN for online and offline service data flow charging (IP flow level bearer charging), introduced in Release 6 may also be re-used.

The following figure depicts a PDG implementation that re-uses GGSN functionality. It shall be noted that only a subset of the GGSN is reused for this purpose.



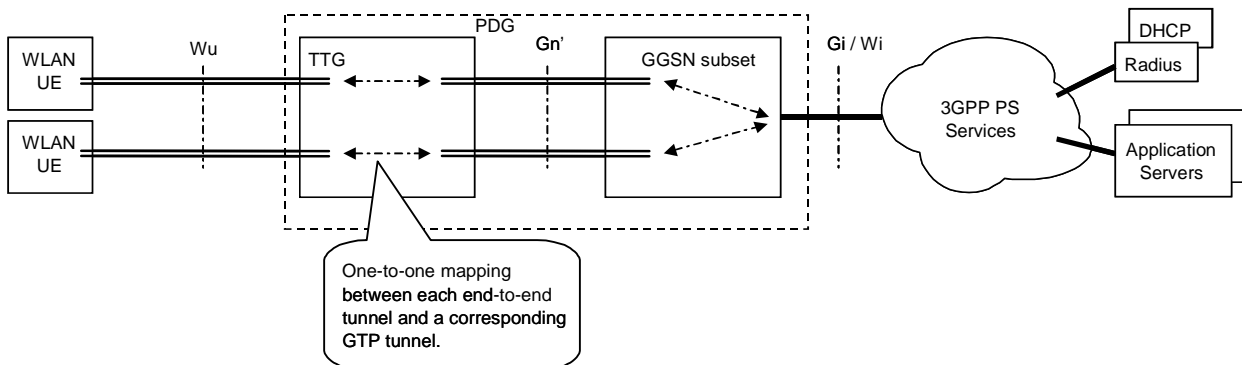
**Figure F.1: PDG implementation re-using GGSN functionality**

The PDG functionality described in this specification may be implemented using the architecture described above in Figure F.1. In case this implementation is applied, the TTG and GGSN parts of the PDG shall be in the same PLMN. This type of PDG implementation shall remain transparent to the other functional elements of the network.

### F.2 Mapping between E2E tunnel and GTP tunnel

The end-to-end tunnel between the WLAN UE and the PDG is setup according to the procedure described in this specification. In a configuration when the Gn' reference point is used, then the end-to-end tunnel setup is terminated by the TTG of the PDG, and the setup of a GTP tunnel is triggered towards the GGSN part of the PDG. Each end-to-end tunnel is mapped one-to-one to a GTP tunnel. The GTP tunnel between the TTG part and the GGSN part of the PDG is

established using the two messages Create PDP Context Request and Create PDP Context Response. A GTP tunnel is identified in each node with a TEID (Tunnel End-point Identifier - an integer), an IP address and a UDP port.



**Figure F.2: Mapping between E2E tunnel and GTP tunnel**

In GPRS different quality-of-service can be assigned to GTP tunnels. WLAN support of layer 2 QoS is being addressed by the IEEE 802.11e study group. Work specifying the interactions with signalling techniques to support the different quality of service techniques needs to be defined. It is unclear at this time how to have a QoS mapping from IEEE 802.11e to IP and hence to the GTP tunnel.

The W-APN provided over the end-to-end tunnel shall be forwarded in the Create PDP Context Request message to GGSN to select external network e.g. PLMN service network, a corporate intranet or the Internet. Internet access can be provided directly from the WLAN Access Network using for WLAN Direct IP Access, but of course nothing prevents a PLMN operator from providing Internet access as well via Gi interface using for WLAN 3GPP IP Access. Some mobile operators might have benefits in using one unified access for all kinds of traffic.

The IMSI of the WLAN UE shall be forwarded to GGSN in the Create PDP Context Request message.

For further details on GTP tunnel management please refer to 3GPP TS 29.060 [28].

## F.3 Gn' considerations

**Editor's note: The Gn' procedures shall comprise a subset of the Gn reference point procedures. There shall be no enhancements to Gn applied.**

### F.3.0 General

A minimum set of interworking procedures over the Gn' reference point would include the following messages from the Gn reference point messages and procedures specified in 3GPP TS 29.060 [28]:

- Create PDP Context Request / Response;
- Update PDP Context Request / Response;
- Delete PDP Context Request / Response;
- Error Indication;
- Version Not Supported;
- GTP Payload Forwarding.

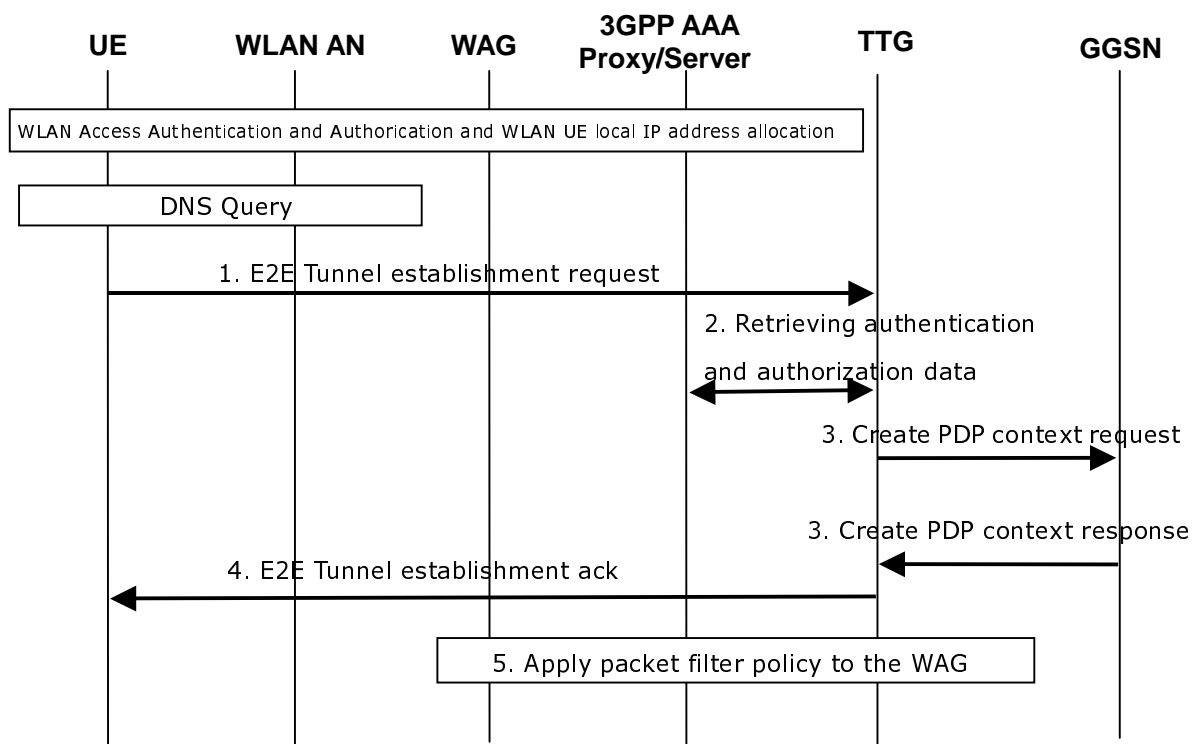
The TTTG must be provided with information, e.g. MCC and MNC of the VPLMN, needed to include the RAI Information Element within the messaging to the GGSN to enable simple position based billing and to enable the HPLMN to restrict certain content to those countries depending on that country's legal requirements.

The assignment of the remote IP address should be done from a pool of IP address belonging to the GGSN/RADIUS server or at least 'address range coordinated' with those to enable correct routing on Gi. The End-user-address IE must be provided in the Create PDP Context Request. If address assignment is done by the GGSN/RADIUS, the IE shall be empty in the request message (indicating dynamic address assignment by GGSN/RADIUS), which makes the GGSN/RADIUS assign and return an IP address in the Response message.

The NSAPI value to be provided over the Gn" reference point is allocated in the TTG, see subclause F.5.

If a certain charging profile should be applied in GGSN the Charging Characteristics IE may be included. In that case this information needs to be available in the TTG. The Charging Characteristics may be used to give special charging for WLAN in the GGSN. The Charging Characteristic is defined per subscriber and is stored in HLR. For GPRS the Charging Characteristic is sent to SGSN at attach and is forwarded to GGSN at PDP context creation. For WLAN interworking, the TTG may for example get this information from HLR via the 3GPP AAA Server.

### F.3.1 Interworking procedure over Gn" - Tunnel establishment procedure

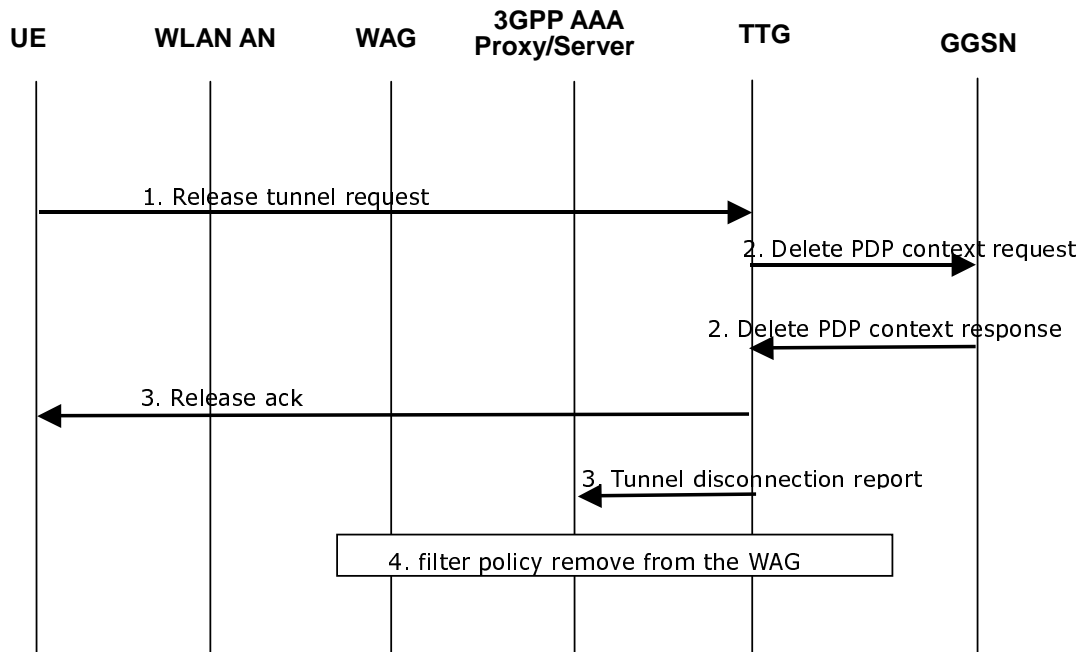


**Figure F.3.1: Tunnel establishment procedure**

- 1) The UE performs a DNS query to resolve the W-APN and sends E2E tunnel establishment request (W-APN, user identity) to the TTG (see subclause 7.9).
- 2) The TTG contacts the 3GPP AAA Server in the HPLMN possibly via the AAA proxy for authorization and authentication of the WLAN UE (see subclause 7.9). Additionally, the TTG retrieves the IMSI, MSISDN, and serving network identity from the AAA server.
- 3) The TTG performs PDP Context Activation procedure towards the GGSN by using Create PDP Context Request message and Create PDP Context Response message (see 3GPP TS 23.060 [7]).
- 4) The TTG returns E2E tunnel establishment acknowledgement (remote IP address) to the WLAN UE.
- 5) The TTG provides filtering information to the WAG (see subclause 7.9).

## F.3.2 Interworking procedure over Gn" - Tunnel disconnection procedure

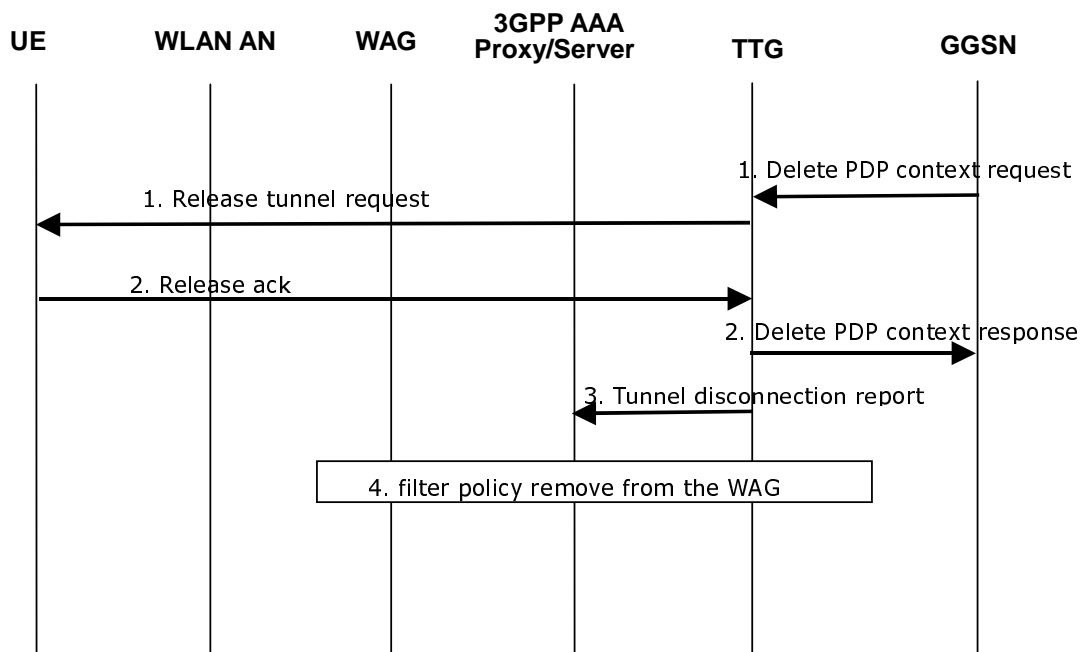
### F.3.2.1 UE initiated tunnel disconnection



**Figure F.3.2.1: UE initiated tunnel disconnection procedure**

- 1) The WLAN UE determines to release the tunnel and sends a Release tunnel request to the TTG (see subclause 7.10.1).
- 2) Upon receiving the Release tunnel request, the TTG performs PDP Context Deactivation procedure towards the GGSN by using Delete PDP Context Request message and Delete PDP Context Response message (see TS 23.060 [7]).
- 3) The TTG sends a Release acknowledgement to the WLAN UE and Tunnel disconnection report to the 3GPP AAA server (see subclause 7.10.1).
- 4) Upon receiving the Tunnel disconnection report, the 3GPP AAA server removes the filtering policy from the WAG (see subclause 7.10.1).

## F.3.2.2 Network initiated tunnel disconnection



**Figure F.3.2.2: Network initiated tunnel disconnection procedure**

- 1) The GGSN determines to release the tunnel and sends Delete PDP Context Request message towards the TTG (see TS 23.060 [7]). The TTG then sends a Release tunnel request to the WLAN UE (see subclause 7.10.2).
- 2) Upon receiving the Release tunnel request, the WLAN UE sends a Release acknowledgement to the TTG (see subclause 7.10.2). The TTG sends a Delete PDP Context Response message to the GGSN (see 3GPP TS 23.060 [7]).
- 3) The TTG sends a Tunnel disconnection report to the 3GPP AAA server (see subclause 7.10.2).
- 4) Upon receiving the Tunnel disconnection report, the 3GPP AAA server removes the filtering policy from the WAG (see subclause 7.10.2).

NOTE: Network initiated tunnel disconnection procedure may also be triggered by the TTG (e.g. request from AAA server).

## F.4 Void

## F.5 Tunnel Terminating Gateway (TTG) functionality

The functionality of the TTG shall cover all aspects of the PDG that are not covered by the GGSN.

The TTG shall be responsible for allocating NSAPI values before sending the Create PDP Context Request message to the GGSN. Although the TTG acts like the SGSN in terms of GTP tunnel establishment, it also manages NSAPI allocation as WLAN UE's proxy for the purpose of leaving the G<sub>n</sub> based PDG transparent to the WLAN UE.

If the network supports simultaneous GPRS and WLAN connections, the TTG shall ensure that the NSAPI values allocated do not overlap with those used by the UE for GPRS PDP Contexts.

NOTE: This can be achieved by restricting TTG allocated NSAPI values to those which are reserved on the mobile radio layer 3 interface in this case.

The TTG shall reject a tunnel establishment request if all available NSAPI values for this user in this GGSN have already been allocated. However, the TTG should not explicitly indicate the exhaustion of the NSAPI values to the UE in such a case.

NOTE: The mechanism above implies that it may not be possible to deploy distinct TTGs providing service for a single user for W-APNs which are then served from the same GGSNs. For a given user, all tunnels towards W-APNs served from the same GGSNs should be directed to the same TTG; the method by which this will be done is FFS.

---

## Annex G (informative): Consideration on supporting IMS over I-WLAN

In GPRS, interaction between bearer service (i.e. GPRS) and IMS is done by a service-based local policy (SBLP) for bearer QoS authorization, gating and charging correlation.

The followings are a brief analysis of possible methods to provide interactions between I-WLAN and IMS.

1. Applying SBLP with full functionality including QoS authorization
  - Pros: It provides full solution for IMS over I-WLAN as the same level as GPRS.
  - Cons: It requires a big amount of new work including E2E QoS and enhancement of SBLP.
  - It is not standardized in this version of the TS.
2. Applying SBLP partially, e.g. without QoS authorization
  - Pros: It provides necessary functions of SBLP for IMS over I-WLAN. Note that current assumption is there is no mechanism of QoS provisioning for I-WLAN in this release.
  - Cons: It also requires modification of SBLP.
  - It is not standardized in this version of the TS.
3. Applying IP-Flow Based Charging (FBC) instead of SBLP
  - Pros: As stated in 3GPP TS 23.125 [15] Annex D, FBC can provide policing functions, which can be used for IMS over I-WLAN. When QoS is not in the picture, FBC can provide enough functionalities required for IMS over I-WLAN such as gating and charging related features.
  - Cons: In the current version of 3GPP TS 23.234, FBC is stated of optional feature of a PDG (not mandatory one). It also requires additional functionality and interface in PDG.
  - It is an optional feature in this version of the TS.
4. Using GGSN's SBLP/FBC functions
  - Pros: When GN" interface is used, the SBLP/FBC functions and related interfaces can be used.
  - Cons: It can be used only in the tunnel extension architecture.
  - It is an optional feature in this version of the TS.
5. Not using any policing mechanism
  - Pros: No more work is required.
  - Cons: IMS over I-WLAN is not able to support policy control and bearer level charging.
  - It is a main working assumption in this version of TS.



## Annex H (informative): Change history

| Change history |        |           |     |     |   |        |        |
|----------------|--------|-----------|-----|-----|---|--------|--------|
| Date           | TSG #  | TSG Doc.  | CR  | Rev | Subject/Comment   | Old    | New    |
| 2002-08        |        |           |     |     | Converted TR23.934v0.5.0 into this TS   | 0.0.0  | 0.1.0  |
| 2002-09        |        |           |     |     | Raised to v.1.0.0 for presentation at SA#17 (same content as v.0.1.0)   | 0.1.0  | 1.0.0  |
| 2002-10        | SA2#27 | S2-022989 |     |     | Modifications/enhancements for scenarios 2 and 3  | 1.0.0  | 1.1.0  |
| 2002-11        | SA2#28 | S2-023517 |     |     | Modifications/enhancements for scenarios 2 and 3  | 1.1.0  | 1.2.1  |
| 2003-01        | SA2#29 | S2-030295 |     |     | Modifications/enhancements for scenarios 2 and 3  | 1.2.1  | 1.4.0  |
| 2003-02        | SA2#30 | S2-030727 |     |     | Split between scenarios 2 and 3   | 1.4.0  | 1.6.0  |
| 2003-04        | SA2#31 | S2-031514 |     |     | Modifications for scenarios 2 and 3   | 1.6.0  | 1.7.0  |
| 2003-04        |        |           |     |     | Modifications/enhancements for scenarios 2 and 3  | 1.7.0  | 1.8.0  |
| 2003-05        | SA2#32 |           |     |     | Modifications/enhancements for scenarios 2 and 3; sent for information to SA#20; scenario 2 now considered as stable; authentication definitely moved to SA3. | 1.8.0  | 1.10.0 |
| 2003-08        | SA2#34 | S2-033183 |     |     | Editorial clarifications; inclusion of tunnelling solution. Sent to SA for approval   | 1.10.0 | 1.14.0 |
| 2003-10        | SA2#35 | S2-033797 |     |     | Enhancements for scenario 3   | 2.0.0  | 2.2.0  |
| 2003-11        | SA2#36 | S2-034357 |     |     | Enhancements for scenarios 2 and 3  | 2.2.0  | 2.3.0  |
| 2004-01        | SA2#37 | S2-040609 |     |     | Enhancements for scenarios 2 and 3  | 2.3.0  | 2.4.0  |
| 2004-02        | SA2#38 |           |     |     | Modifications/enhancements for scenarios 2 and 3; sent for approval to SA#23.   | 2.4.0  | 2.5.0  |
| 2004-03        | SA #23 | SP-040049 |     |     | Raised to v.6.0.0 after approval at SA#23 (same content as previous version)  | 2.5.0  | 6.0.0  |
| 2004-06        | SA #24 | SP-040320 | 001 | 2   | Update of disconnection procedures  | 6.0.0  | 6.1.0  |
| 2004-06        | SA #24 | SP-040320 | 012 |     | Clarifications on the Wa reference point  | 6.0.0  | 6.1.0  |
| 2004-06        | SA #24 | SP-040320 | 013 | 1   | Corrections in the network selection clause   | 6.0.0  | 6.1.0  |
| 2004-06        | SA #24 | SP-040320 | 022 | 2   | Routing Enforcement in WLAN AN  | 6.0.0  | 6.1.0  |
| 2004-06        | SA #24 | SP-040320 | 027 |     | Corrections of Wg definition and some obsolete texts  | 6.0.0  | 6.1.0  |
| 2004-06        | SA #24 | SP-040320 | 029 | 2   | Update on definition on WLAN UE   | 6.0.0  | 6.1.0  |
| 2004-06        | SA #24 | SP-040320 | 030 | 6   | Suggested changes to the new WLAN access terms  | 6.0.0  | 6.1.0  |
| 2004-06        | SA #24 | SP-040320 | 033 | 3   | WLAN UE initiated disconnection procedures  | 6.0.0  | 6.1.0  |
| 2004-06        | SA #24 | SP-040320 | 035 | 2   | Clarification on WLAN access authentication and authorisation   | 6.0.0  | 6.1.0  |
| 2004-06        | SA #24 | SP-040320 | 036 |     | Reference to 23.825   | 6.0.0  | 6.1.0  |
| 2004-06        | SA #24 | SP-040320 | 038 | 2   | Considerations on the format of the IP address used for tunnel establishment  | 6.0.0  | 6.1.0  |
| 2004-06        | SA #24 | SP-040320 | 041 | 2   | Per-user charging in the VPLMN  | 6.0.0  | 6.1.0  |
| 2004-06        | SA #24 | SP-040320 | 044 | 1   | Correction of Wd reference point requirements   | 6.0.0  | 6.1.0  |
| 2004-06        | SA #24 | SP-040320 | 045 | 1   | Clarification of Wm reference point requirements  | 6.0.0  | 6.1.0  |
| 2004-06        | SA #24 | SP-040320 | 047 | 2   | Re-authentication   | 6.0.0  | 6.1.0  |
| 2004-06        | SA #24 | SP-040320 | 048 | 3   | Alignment with 3GPP IMS architecture: SLF usage in Wx to locate the HSS   | 6.0.0  | 6.1.0  |
| 2004-06        | SA #24 | SP-040320 | 052 | 2   | Removal of WLAN UE classes  | 6.0.0  | 6.1.0  |
| 2004-06        | SA #24 | SP-040320 | 054 | 1   | Combined CR to 23.234 Annex D (SMS over IP)   | 6.0.0  | 6.1.0  |
| 2004-06        | SA #24 | SP-040454 | 053 | 2   | Merge of approved CR"s in TS 23.234, Annex F  | 6.0.0  | 6.1.0  |
| 2004-09        | SA #25 | SP-040524 | 033 | 3   | WLAN Manual PLMN Network selection - CR   | 6.1.0  | 6.2.0  |
| 2004-09        | SA #25 | SP-040524 | 055 | 1   | Cleanup of figure 7.4 in TS 23.234  | 6.1.0  | 6.2.0  |
| 2004-09        | SA #25 | SP-040524 | 058 | 1   | Correction of mistakes and inaccurate descriptions in 23.234  | 6.1.0  | 6.2.0  |
| 2004-09        | SA #25 | SP-040524 | 061 | 1   | Clarification on usage of 3GPP AAA server   | 6.1.0  | 6.2.0  |
| 2004-09        | SA #25 | SP-040524 | 063 | 4   | Alignment of PLMN selection   | 6.1.0  | 6.2.0  |
| 2004-09        | SA #25 | SP-040524 | 064 | 1   | Correction of Wa reference point functionality  | 6.1.0  | 6.2.0  |
| 2004-09        | SA #25 | SP-040524 | 065 | 1   | Multiple WLAN connections   | 6.1.0  | 6.2.0  |
| 2004-09        | SA #25 | SP-040524 | 066 | 1   | Introduction of the WLAN registration within tunnel establishment procedure   | 6.1.0  | 6.2.0  |
| 2004-09        | SA #25 | SP-040524 | 068 |     | Editorial update of already agreed change in figure 6.2b  | 6.1.0  | 6.2.0  |
| 2004-09        | SA #25 | SP-040524 | 069 |     | Removal of issue chapter in Annex F.  | 6.1.0  | 6.2.0  |
| 2004-09        | SA #25 | SP-040524 | 070 | 1   | Clarification of NSAPI in Annex F.  | 6.1.0  | 6.2.0  |
| 2004-09        | SA #25 | SP-040524 | 071 | 1   | CR on IMS over WLAN   | 6.1.0  | 6.2.0  |
| 2004-09        | SA #25 | SP-040524 | 072 | 3   | Correction to temporary identity usage and reference  | 6.1.0  | 6.2.0  |
| 2004-09        | SA #25 | SP-040524 | 073 | 2   | Correction to PDG Selection Mechanism   | 6.1.0  | 6.2.0  |

|         |        |           |     |   |  |       |       |
|---------|--------|-----------|-----|---|--|-------|-------|
| 2004-09 | SA #25 | SP-040524 | 075 | 3 | Correction to W-APN authorisation and PDG redirection Mechanism              | 6.1.0 | 6.2.0 |
| 2004-09 | SA #25 | SP-040524 | 076 | 3 | WLAN User Profile revision   | 6.1.0 | 6.2.0 |
| 2004-09 | SA #25 | SP-040524 | 077 | 3 | Charging related data for 3GPP PS based services (WLAN 3GPP IP Access)       | 6.1.0 | 6.2.0 |
| 2004-09 | SA #25 | SP-040524 | 078 | 3 | Static Remote IP address allocation  | 6.1.0 | 6.2.0 |
| 2004-09 | SA #25 | SP-040524 | 081 | 2 | Storage of the AAA server IP address in HSS/HLR                              | 6.1.0 | 6.2.0 |
| 2004-12 | SA #26 | SP-040755 | 062 | 2 | Enhancements of Wd Interface   | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 083 | 2 | Charging in WLAN interworking architecture                                   | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 086 | 6 | Correction of online charging disconnect procedure.                          | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 087 | 1 | Clarification on network selection   | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 088 |   | Clarification on Wm reference point  | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 089 | 1 | Correction of multiple service authorization requirement                     | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 090 | 2 | Removal of WLAN UE registration at tunnel establishment                      | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 091 | 1 | Providing configuration parameter to the WLAN UE during tunnel establishment | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 092 |   | Correction of references   | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 093 | 1 | Removing tunnel redirection option   | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 094 | 1 | Revision for PLMN selection procedure  | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 095 | 2 | Revision for Ww reference point definition                                   | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 097 | 3 | Suppliment to the subscriber profile procedure                               | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 099 | 1 | Addition of reference  | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 100 | 1 | Clarification of the procedure to disconnect the last tunnel                 | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 101 |   | Remove duplicated charging requirement for the PDG                           | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 102 | 3 | Consistant Wording, Spacing, and Grammar Readability Changes                 | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 104 | 3 | Rewording Readability Changes Section 1                                      | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 105 | 3 | Rewording Readability Changes Section 3                                      | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 107 | 3 | Section 5 Reordering   | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 109 | 2 | 3GPP WLAN User profile Update  | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 110 | 1 | Removal of unused references   | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 111 | 1 | Redraw of diagrams in section 7  | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 112 | 2 | Editorial corrections  | 6.2.0 | 6.3.0 |
| 2004-12 | SA #26 | SP-040755 | 113 | 1 | Correction on Annex E  | 6.2.0 | 6.3.0 |

---

# History

| <b>Document history</b> |               |             |
|-------------------------|---------------|-------------|
| V6.3.0                  | December 2004 | Publication |
|                         |               |             |
|                         |               |             |
|                         |               |             |
|                         |               |             |