

# IPWorks 3GPP AAA Server-WLAN Access Network Wa Interface

---

## INTERWORK DESCRIPTION

**Copyright**

© Ericsson AB 2011-2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

**Disclaimer**

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

**Trademark List**

All trademarks mentioned herein are the property of their respective owners. These are shown in the document IPWorks Trademark Information.



# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Prerequisites	1
1.2	Related Information	1
<b>2</b>	<b>Interface Overview</b>	<b>3</b>
2.1	Interface Role	3
2.2	Services	3
2.3	Encapsulation and Addressing	4
<b>3</b>	<b>Procedures</b>	<b>7</b>
3.1	Authentication/Authorization	7
3.2	Accounting	11
3.3	Disconnect Message	12
<b>4</b>	<b>Information Model</b>	<b>15</b>
4.1	General	15
4.2	RADIUS Message in Wa Interface	15
4.3	EAP Message in Wa Interface	18
4.4	EAP-AKA Message in Wa Interface	18
4.5	EAP-SIM Message in Wa Interface	21
<b>5</b>	<b>Formal Syntax</b>	<b>23</b>
<b>6</b>	<b>Related Standards</b>	<b>25</b>
	<b>Reference List</b>	<b>27</b>





# 1 Introduction

This document describes the Wa reference point between IPWorks AAA server and the WLAN Access Network.

## Scope

The Wa interface is used by IPWorks AAA server to interact with WLAN Access Network.

This document covers the following topics:

- Interface Overview
- Interface Role
- Services
- Encapsulation and Addressing
- Procedures
- Information Model
- Related Standards

## Target Groups

This document is intended for personnel needing to understand the logical entity, including interfaces and protocols, of the IPWorks.

## 1.1 Prerequisites

N/A

## 1.2 Related Information

Trademark information, typographic conventions, definition, and explanation of acronyms and terminology can be found in the following documents:

- *Trademark Information*, Reference [1]
- *Glossary of Terms and Acronyms*, Reference [2]
- *Typographic Conventions*, Reference [3]



The standard related to the Wa interface can be found in the section References.

2

# Interface Overview

The prime purpose of the protocols crossing the Wa reference point is to transport authentication, authorization, and charging-related information in a secure manner. EAP authentication is transported over the Wa reference point and protocol is Diameter or RADIUS based. Currently, IPWorks AAA server uses RADIUS protocol to convey the EAP-AKA/SIM authentication message.

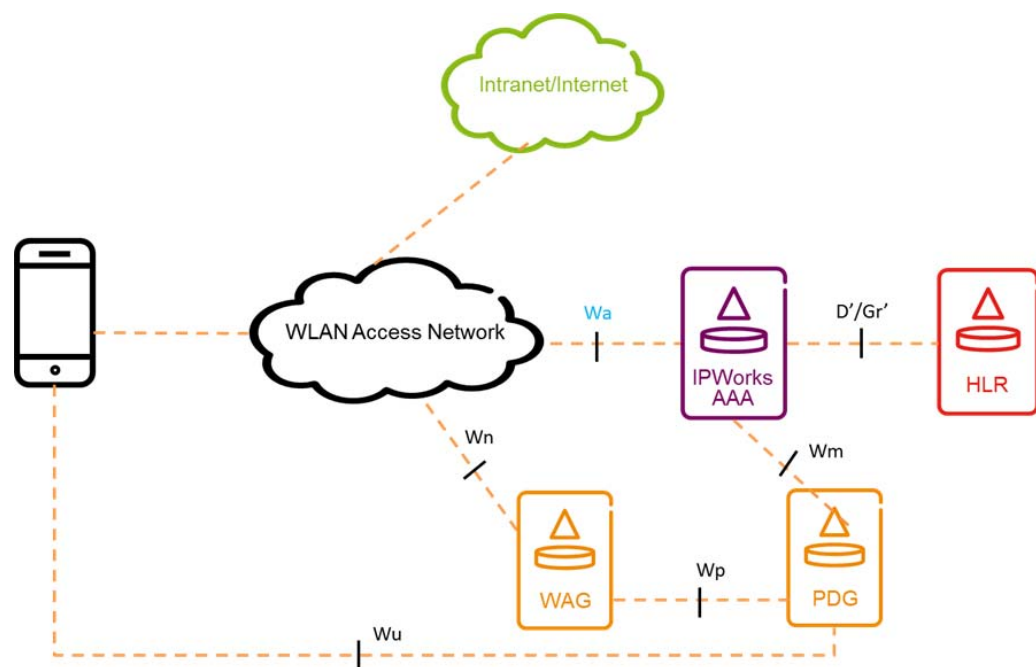


Figure 1 Wa Reference Point in 3GPP WLAN Inter-working Reference Model

2.1

## Interface Role

In Wa reference point, IPWorks AAA server takes the role AAA in 3GPP network.

2.2

## Services

Table 1 Offered Services

Offered Service	Description
Authentication, Authorization, Accounting	IPWorks AAA server offers the AAA service to WLAN Access Network

## 2.3 Encapsulation and Addressing

The following protocol stack is used on this interface for IPWorks AAA Server:

EAP AKA	EAP SIM
RADIUS	
UDP	
IP	

*Figure 2 Protocol Stack Used in 3GPP Network*

The AAA service offered by IPWorks AAA server is addressed by the following RADIUS packets.

### 2.3.1 WLAN Access Authentication and Authorization

The offered WLAN access authentication and authorization service by IPWorks AAA server is addressed by the following RADIUS packets that are defined in RFC2865, Reference [4] and RFC3579 ,Reference [5].

- Access-Request
- Access-Challenge
- Access-Accept
- Access-Reject

The Extensible Authentication Protocol mechanism for authentication and session key distribution that uses the GSM Subscriber Identity Module (SIM) is specified in RFC4186, Reference [8], include following packets:

- EAP-Request/SIM/Start
- EAP-Response/SIM/Start
- EAP-Request/SIM/Challenge
- EAP-Response/SIM/Challenge
- EAP-Request/SIM/Re-authentication
- EAP-Response/SIM/Re-authentication
- EAP-Response/SIM/Client-Error
- EAP-Request/SIM/Notification
- EAP-Response/SIM/Notification





The Extensible Authentication Protocol mechanism for authentication and session key distribution that uses the Authentication and Key Agreement (AKA) mechanism is specified in RFC4187, Reference [9], include following packets:

- EAP-Request/AKA-Identity
- EAP-Response/AKA-Identity
- EAP-Request/AKA-Challenge
- EAP-Response/AKA-Challenge
- EAP-Response/AKA-Authentication-Reject
- EAP-Response/AKA-Synchronization-Failure
- EAP-Request/AKA-Reauthentication
- EAP-Response/AKA-Reauthentication
- EAP-Response/AKA-Client-Error
- EAP-Request/AKA-Notification
- EAP-Response/AKA-Notification

### 2.3.2 Accounting

AAA server uses the following RADIUS for accounting functionality. For more information refer to RFC2866, Reference [7].

- Accounting-Request
- Accounting-Response

### 2.3.3 Disconnect Subscriber

AAA server can disconnect an online subscriber by using the following DM packets that are defined in RFC5176, Reference [6].

- Disconnect-Request
- Disconnect-ACK
- Disconnect-NAK





## 3 Procedures

The following procedures describe the general interaction for authentication, authorization, and accounting.

### 3.1 Authentication/Authorization

IPWorks AAA server supports SIM-based (EAP-AKA/SIM) authentication methods for WLAN access in Wa reference point. The following figures show the basic authentication procedures based on RADIUS protocol.

### 3.1.1 EAP-AKA Full Authentication

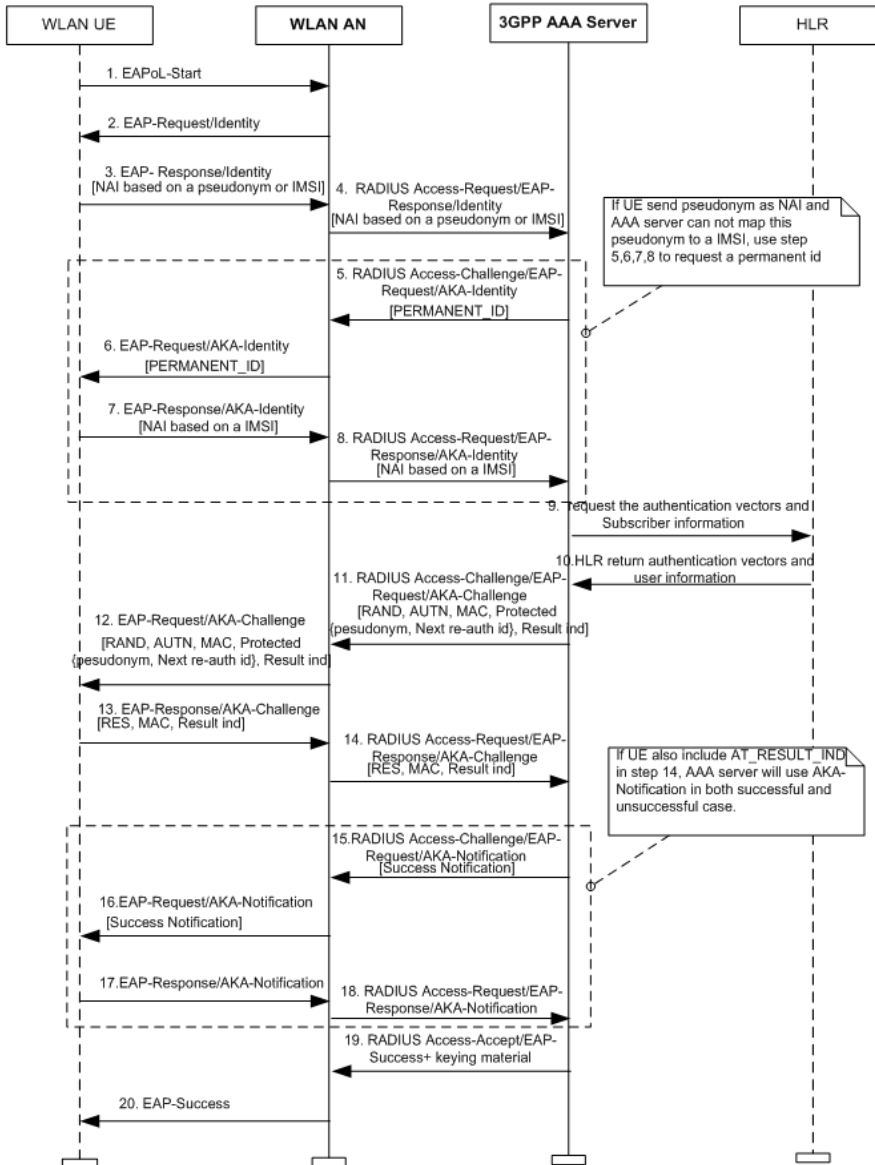


Figure 3 EAP-AKA Full Authentication Flows

### 3.1.2 EAP-SIM Full Authentication

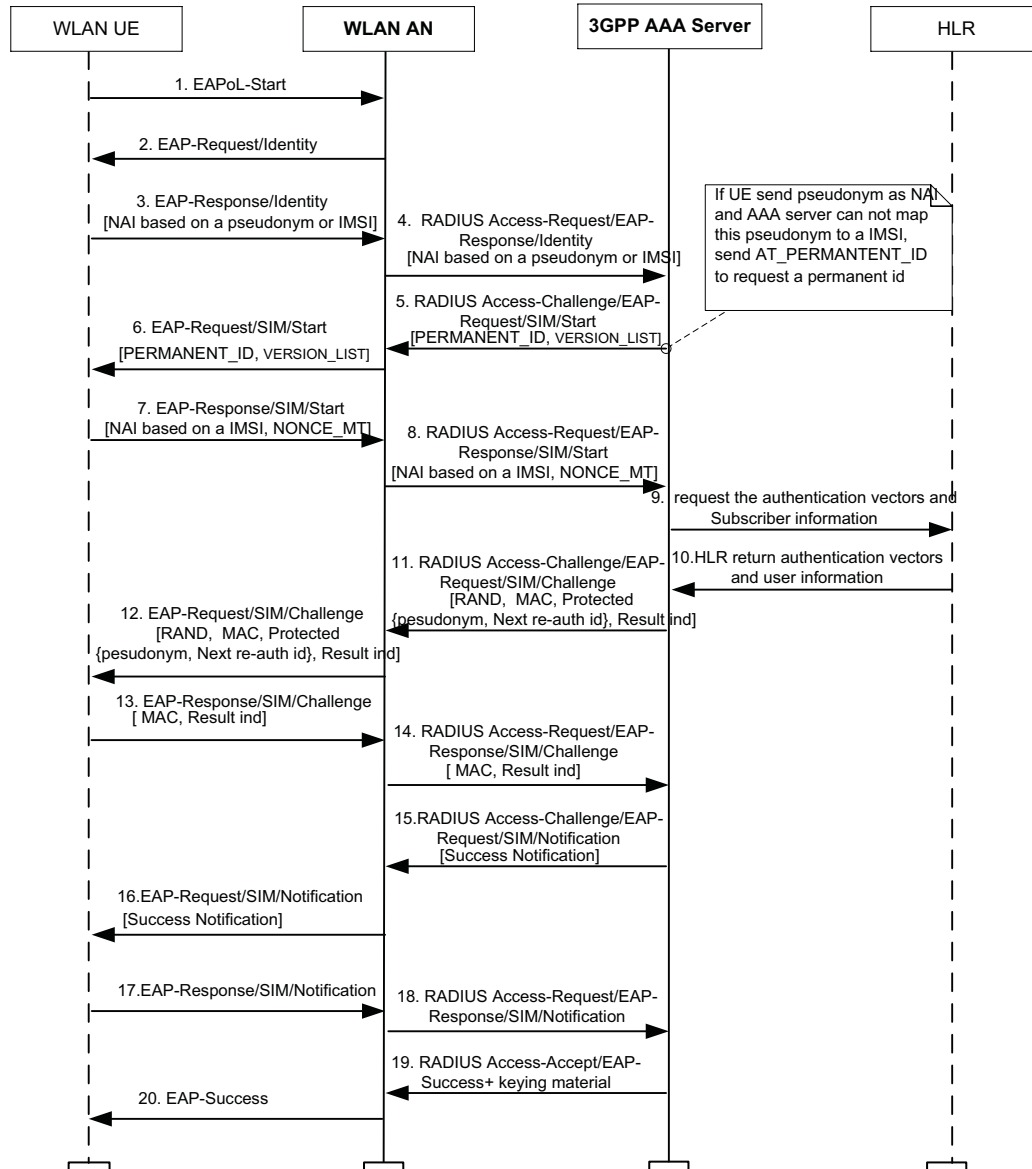


Figure 4 EAP-SIM Full Authentication Flows

### 3.1.3 EAP-AKA Fast Re-authentication

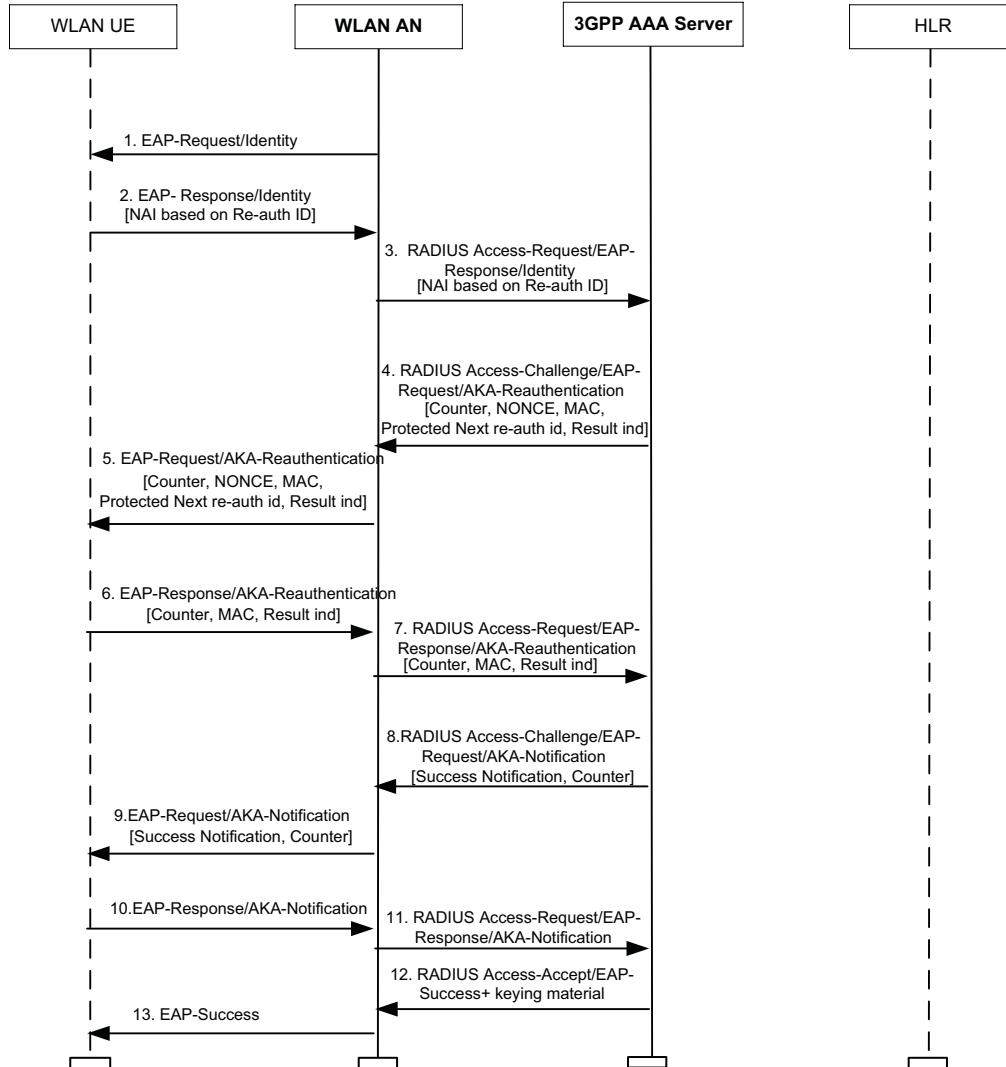


Figure 5 EAP-AKA Fast Re-authentication Flows

### 3.1.4 EAP-SIM Fast Re-authentication

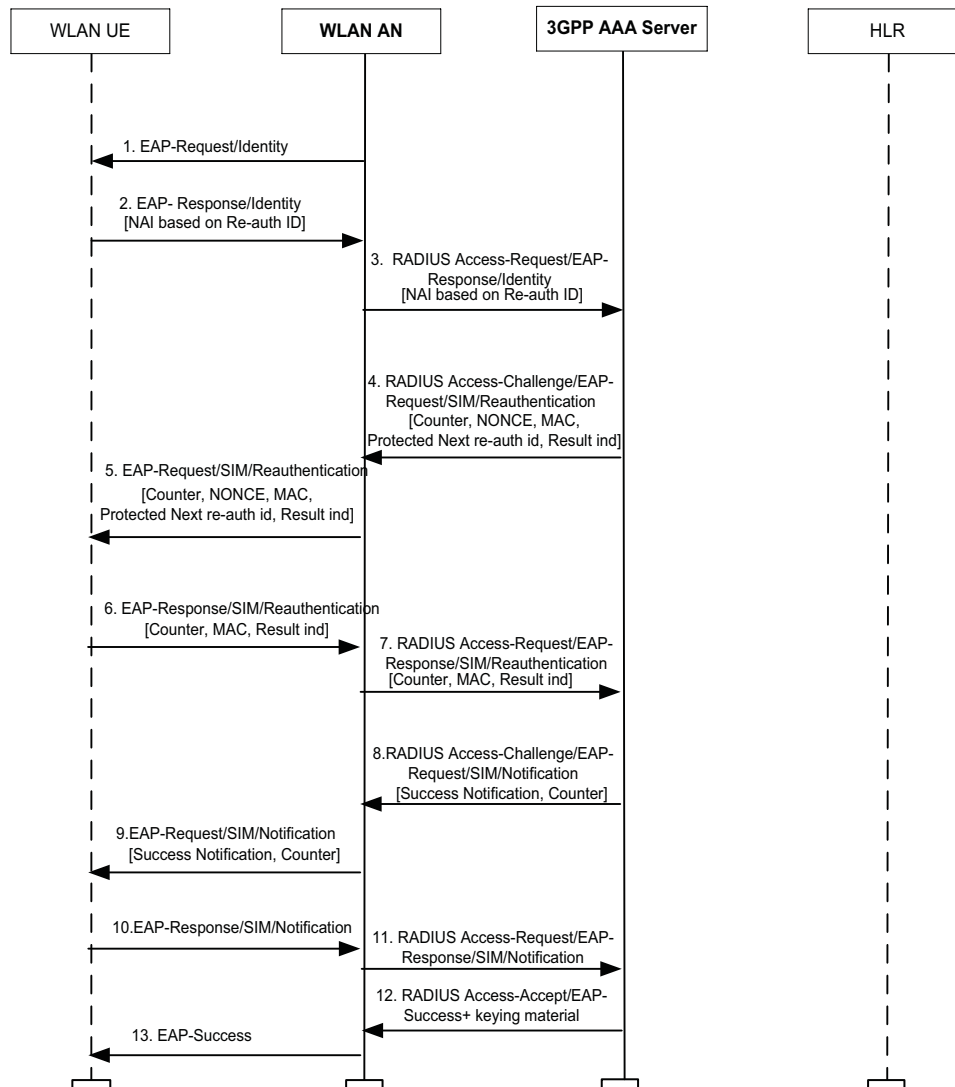


Figure 6 EAP-SIM Fast Re-authentication Flows

## 3.2 Accounting

Accounting is used to collect the resource usage information for analysis or billing purposes. Accounting-Request START message means that a user session has started; Accounting-Request Interim-Update is used to update the user session information; and Accounting-Request STOP means that the user session is terminated.

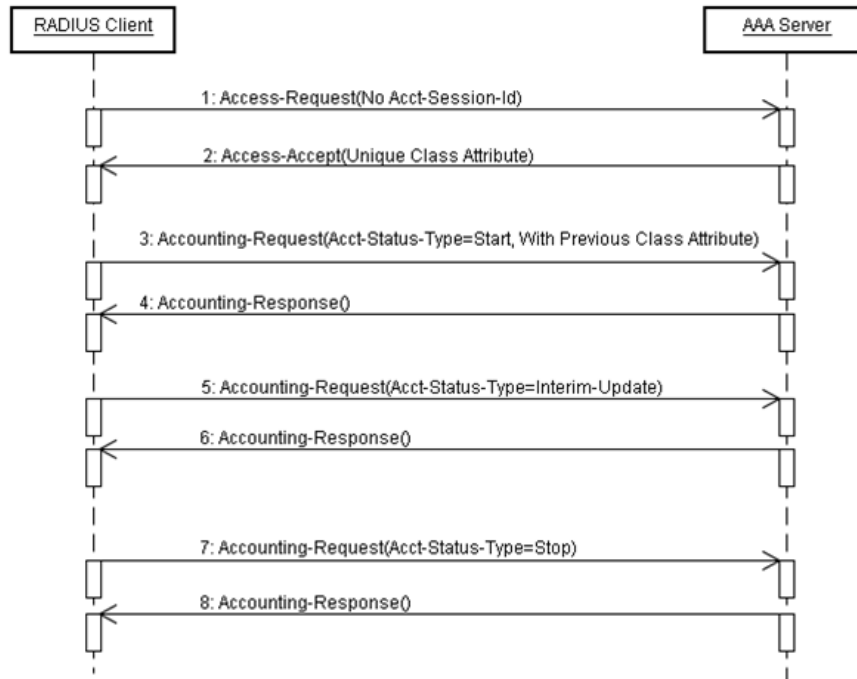


Figure 7 Accounting

### 3.3 Disconnect Message

The AAA server could receive the status change of related subscribers from HLR and decide whether need to terminate the active session. If the user's WLAN accessible flag has changed or the user logged on from the other server, AAA server may issue the Disconnect-Request messages to notify an NAS about the termination of the accounting sessions.



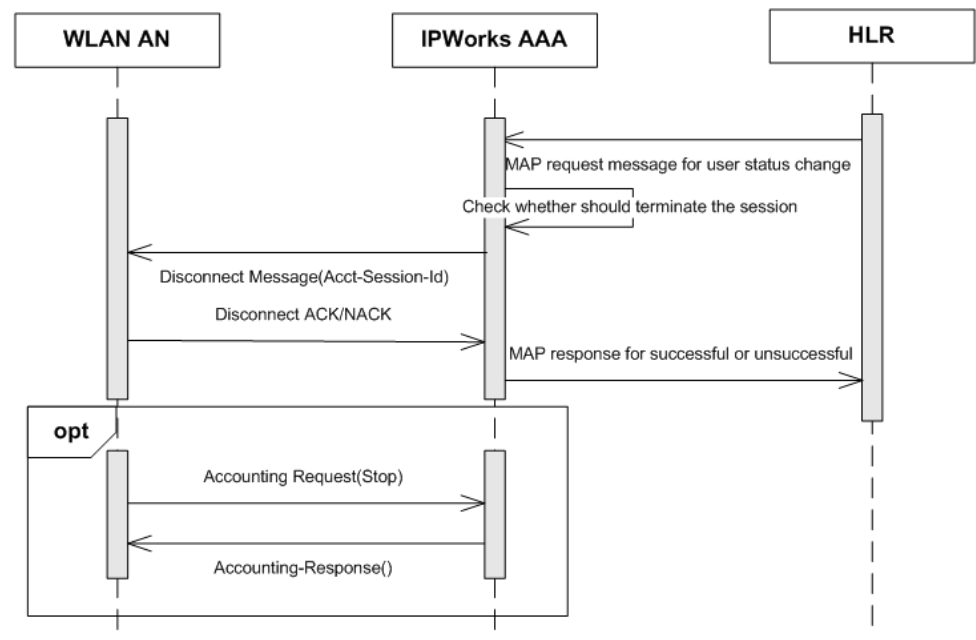


Figure 8 Terminate Session



## 4 Information Model

This section describes the information model including mandatory and optional parameters of each service operation.

### 4.1 General

The following convention is used to indicate how the attribute is present in a message:

*Table 2 Convention*

Attribute	Description
0	This attribute MUST NOT be present in message.
0+	Zero or more instances of this attribute MAY be present in message.
0-1	Zero or one instance of this attribute MAY be present in message.
1	Exactly one instance of this attribute MUST be present in message.
0*	The attribute is not included in the message in cases specified in the related RFC, but MAY be included in the future versions of the protocol.

The format `<Attr#>/<Vendor-ID>-<Sub-attr#>` is used for the vendor-specific subattributes. For example, `26/311-28` is the code of Microsoft vendor-specific RADIUS attribute MS-Primary-DNS-Server.

### 4.2 RADIUS Message in Wa Interface

The messages supported by the Wa interface comply with the RADIUS data format that is defined in RFC 2865, Reference [4], RFC5176, Reference [6], and RFC 2866, Reference [7]. They can be divided into the following groups:

- Authentication/Authorization: Access-Request, Access-Accept, Access-Reject, Access-Challenge
- DM: Disconnect-Request, Disconnect-ACK/NAK
- Accounting: Accounting-Request, Accounting-Response

The following sections list the attributes which be used in the messages of Wa interface. If the messages also include other attributes according to related protocols, AAA server bypasses them.



## 4.2.1 Authentication/Authorization Message Attributes

The following table contains the authentication or authorization message attributes:

**Table 3** Attributes Supported by Authentication/Authorization Message for Wa Interface

Attr #	Attribute Name	Access-Request	Access-Accept	Access-Reject	Access-Challenge	Description
1	User-Name <sup>(1)</sup>	1	1	1	1	Section 5.1, RFC 2865
4	NAS-IP-Address	1	0	0	0	Section 5.4, RFC 2865
31	Calling-Station-ID	1	0	0	0	Section 5.31, RFC 2865
30	Called-Station-ID	1	0	0	0	Section 5.30, RFC 2865
32	NAS-Identifier	1	0	0	0	Section 5.32, RFC 2865
87	NAS-Port-Id	1	0	0	0	Section 5.32, RFC 2865
24	State	0-1	0-1	0	1	Section 5.7, RFC 2865 Section 2.1.1, RFC 5080
27	Session-Timeout	0	1	0-1	0	Section 5.27, RFC 2865 Section 3.17, RFC 3580
29	Termination-Action	0	1	0-1	0	Section 5.29, RFC 2865 Section 3.17, RFC 3580
79	EAP-Message	1+	1+	1+	1+	Section 3.1, RFC 3579
80	Message-Authenticator	1	1	1	1	Section 3.2, RFC 3579
89	Chargeable-User-Identity	0-1	1	0	0	Section 2.2, RFC 4372
85	Acct_Interim_Interval	0	1	0	0	Section 5.16, RFC 2869
26-31 1-17	MS-MPPE-Recv-Key	0	1	0	0	Section 2.4.3, RFC 2548
26-31 1-16	MS-MPPE-Send-Key	0	1	0	0	Section 2.4.2, RFC 2548
25	class	0	0+	0	0	Section 5.25, RFC 2865
26-1 0415 -13	3GPP-Charging-Characteristics	0	0-1	0	0	3GPP TS 29.061 v9.0.0, Section 16.4.7.2

(1) When the Trusted WiFi Support feature is enabled, the value of User-Name is only set as IMSI; otherwise set as NAI.



## 4.2.2 DM Message Attributes

*Table 4 Attributes Supported by DM Message for Wa Interface*

Attr #	Attribute Name	Disconnect-Request	Disconnect-ACK	Disconnect-NAK	Description
1	User-Name(1)	1	0	0	Section 5.1, RFC 2865
4	NAS-IP-Address	1	0	0	Section 5.4, RFC 2865
32	NAS-Identifier	1	0	0	Section 5.32, RFC 2865
44	Acct-Session-Id	1	0	0	Section 5.5, RFC 2866
80	Message-Authenticator	1	1	1	Section 3.2, RFC 3579

**Note:** The value of User-Name attribute will be the NAI in the Access-Accept which be sent in the last successful authentication.

## 4.2.3 Accounting Message Attributes

*Table 5 Accounting Message Attributes*

Attr #	Attribute Name	Accounting-Request START	Accounting-Request STOP	Accounting-Request Interim-Update	Description
1	User-Name	1	1	1	Section 5.1, RFC 2865
4	NAS-IP-Address	1	1	1	Section 5.4, RFC 2865
31	Calling-Station-ID	1	1	1	Section 5.31, RFC 2865
30	Called-Station-ID	0-1	0-1	0-1	Section 5.30, RFC 2865
32	NAS-Identifier	1	1	1	Section 5.32, RFC 2865
87	NAS-Port-Id	1	1	1	Section 5.17, RFC 2869
40	Acct-Status-Type	1	1	1	Section 5.1, RFC 2866
42	Acct-Input-Octets	0	1	1	Section 5.3, RFC 2866
43	Acct-Output-Octets	0	1	1	Section 5.4, RFC 2866
44	Acct-Session-Id	1	1	1	Section 5.5, RFC 2866
89	Chargeable-User-Identity	0-1	0-1	0-1	Section 2.2, RFC 4372
46	Acct-Session-Time	0	1	1	Section 5.7, RFC 2866
47	Acct-Input-Packets	0	1	1	Section 5.8, RFC 2866

**Table 5 Accounting Message Attributes**

Attr #	Attribute Name	Accounting-Request START	Accounting-Request STOP	Accounting-Request Interim-Update	Description
48	Acct-Output-Packets	0	1	1	Section 5.9, RFC 2866
52	Acct-Input-Gigawords	0	1	1	Section 5.1, RFC 2869
53	Acct-Output-Gigawords	0	1	1	Section 5.2, RFC 2869
27	Session-TimeOut	1	0	0	Section 5.27, RFC 2865
25	class	0+	0+	0+	Section 5.25, RFC 2865
49	Acct-Terminate-Cause	0	1	0	Section 5.10, RFC 2866

## 4.3 EAP Message in Wa Interface

In Wa interface, the following EAP packets will be used for authentication:

- Request(1)
- Response(2)
- Success(3)
- Failure(4)

The following EAP types will be used in EAP Request/Response exchanges for the Wa interface.

- EAP-AKA(23)
- EAP-SIM(18)

## 4.4 EAP-AKA Message in Wa Interface

The following table provides a guide to which attributes may be found in which kinds of messages, and in what quantity. Messages are denoted with numbers in parentheses as follows:

- EAP-Request/AKA-Identity(1)
- EAP-Response/AKA-Identity(2)
- EAP-Request/AKA-Challenge(3)
- EAP-Response/AKA-Challenge(4)



- EAP-Request/AKA-Notification(5)
- EAP-Response/AKA-Notification(6)
- EAP-Response/AKA-Client-Error(7)
- EAP-Request/AKA-Reauthentication(8)
- EAP-Response/AKA-Reauthentication(9)
- EAP-Response/AKA-Authentication-Reject(10)
- EAP-Response/AKA-Synchronization-Failure(11)

The column denoted with “E” indicates whether the attribute is a nested attribute that MUST be included within AT\_ENCR\_DATA.

*Table 6 EAP-AKA Message in Wa Interface*

Attribute Name	1	2	3	4	5	6	7	8	9	10	11	E	Description
AT_PERMANENT_ID_REQ	0-1	0	0	0	0	0	0	0	0	0	0	No	Section 10.2, RFC 4187
AT_ANY_ID_REQ	0	0	0	0	0	0	0	0	0	0	0	No	Section 10.3, RFC 4187
AT_FULLAUTH_ID_REQ	0	0	0	0	0	0	0	0	0	0	0	No	Section 10.4, RFC 4187
AT_IDENTITY	0	0-1	0	0	0	0	0	0	0	0	0	No	Section 10.5, RFC 4187
AT RAND	0	0	1	0	0	0	0	0	0	0	0	No	Section 10.6, RFC 4187
AT_AUTN	0	0	1	0	0	0	0	0	0	0	0	No	Section 10.7, RFC 4187
AT_RES	0	0	0	1	0	0	0	0	0	0	0	No	Section 10.8, RFC 4187
AT_AUS	0	0	0	0	0	0	0	0	0	0	1	No	Section 10.9, RFC 4187

**Table 6 EAP-AKA Message in Wa Interface**

Attribute Name	1	2	3	4	5	6	7	8	9	10	11	E	Description
AT_N EXT_PSEU DON YM	0	0	0-1	0	0	0	0	0	0	0	0	Yes	Section 10.10, RFC 4187
AT_N EXT_REAU TH_ID	0	0	1	0	0	0	0	0-1	0	0	0	Yes	Section 10.11, RFC 4187
AT_IV	0	0	0-1	0*	0-1	0-1	0	1	1	0	0	No	Section 10.12, RFC 4187
AT_E NCR_DATA	0	0	0-1	0*	0-1	0-1	0	1	1	0	0	No	Section 10.12, RFC 4187
AT_P ADDI NG	0	0	0-1	0*	0-1	0-1	0	0-1	0-1	0	0	Yes	Section 10.12, RFC 4187
AT_C HECK CODE	0	0	0	0	0	0	0	0	0	0	0	No	Section 10.13, RFC 4187
AT_R ESUL T_IN D	0	0	0-1	0-1	0	0	0	0-1	0-1	0	0	No	Section 10.14, RFC 4187
AT_M AC	0	0	1	1	0-1	0-1	0	1	1	0	0	No	Section 10.15, RFC 4187
AT_C OUNT ER	0	0	0	0	0-1	0-1	0	1	1	0	0	Yes	Section 10.16, RFC 4187
AT_C OUNT ER_T OO_S MALL	0	0	0	0	0	0	0	0	0-1	0	0	Yes	Section 10.17, RFC 4187
AT_N ONC E_S	0	0	0	0	0	0	0	1	0	0	0	Yes	Section 10.18, RFC 4187





**Table 6** EAP-AKA Message in Wa Interface

Attribute Name	1	2	3	4	5	6	7	8	9	10	11	E	Description
AT_NOTIFICATION	0	0	0	0	1	0	0	0	0	0	0	No	Section 10.19, RFC 4187
AT_CLIENT_ERROR_CODE	0	0	0	0	0	0	1	0	0	0	0	No	Section 10.20, RFC 4187

## 4.5 EAP-SIM Message in Wa Interface

The following table provides a guide to which attributes may be found in which kinds of messages, and in what quantity. Messages are denoted with numbers in parentheses as follows:

- EAP-Request/SIM/Start(1)
- EAP-Response/SIM/Start(2)
- EAP-Request/SIM/Challenge(3)
- EAP-Response/SIM/Challenge(4)
- EAP-Request/SIM/Notification(5)
- EAP-Response/SIM/Notification(6)
- EAP-Response/SIM/Client-Error(7)
- EAP-Request/SIM/Re-authentication(8)
- EAP-Response/SIM/Re-authentication(9)

The column denoted with “Encr” indicates whether the attribute is a nested attribute that **MUST** be included within AT\_ENCR\_DATA, and the column denoted with “Skip” indicates whether the attribute is a skippable attribute.

**Table 7** EAP-SIM Message in Wa Interface

Attribute Name	1	2	3	4	5	6	7	8	9	Encr	Skip	Description
AT_VERSION_LIST	1	0	0	0	0	0	0	0	0	No	No	Section 10.2, RFC 4186
AT_SELECTED_VERSION	0	0-1	0	0	0	0	0	0	0	No	No	Section 10.3, RFC 4186
AT_NONCE_MT	0	0-1	0	0	0	0	0	0	0	No	No	Section 10.4, RFC 4186

**Table 7 EAP-SIM Message in Wa Interface**

Attribute Name	1	2	3	4	5	6	7	8	9	Encr	Skip	Description
AT_PERM ANENT_ID_REQ	0-1	0	0	0	0	0	0	0	0	No	No	Section 10.5, RFC 4186
AT_ANY_ID_REQ	0	0	0	0	0	0	0	0	0	No	No	Section 10.6, RFC 4186
AT_FULLAUTH_ID_REQ	0	0	0	0	0	0	0	0	0	No	No	Section 10.7, RFC 4186
AT_IDENTITY	0	0-1	0	0	0	0	0	0	0	No	No	Section 10.8, RFC 4186
AT_RAND	0	0	1	0	0	0	0	0	0	No	No	Section 10.9, RFC 4186
AT_NEXT_PSEUDONYM	0	0	0-1	0	0	0	0	0	0	Yes	Yes	Section 10.10, RFC 4186
AT_NEXT_REAUTH_ID	0	0	1	0	0	0	0	0-1	0	Yes	Yes	Section 10.11, RFC 4186
AT_IV	0	0	0-1	0*	0-1	0-1	0	1	1	No	Yes	Section 10.12, RFC 4186
AT_ENCR_DATA	0	0	0-1	0*	0-1	0-1	0	1	1	No	Yes	Section 10.12, RFC 4186
AT_PADDING	0	0	0-1	0*	0-1	0-1	0	0-1	0-1	Yes	No	Section 10.12, RFC 4186
AT_RESULT_IND	0	0	1	0-1	0	0	0	0-1	0-1	No	Yes	Section 10.13, RFC 4186
AT_MAC	0	0	1	1	0-1	0-1	0	1	1	No	No	Section 10.14, RFC 4186
AT_COUNTER	0	0	0	0	0-1	0-1	0	1	1	Yes	No	Section 10.15, RFC 4186
AT_COUNTER_TOO_SMALL	0	0	0	0	0	0	0	0	0-1	Yes	No	Section 10.16, RFC 4186
AT_NONCES	0	0	0	0	0	0	0	1	0	Yes	No	Section 10.17, RFC 4186
AT_NOTIFICATION	0	0	0	0	1	0	0	0	0	No	No	Section 10.18, RFC 4186
AT_CLIENT_ERROR_CODE	0	0	0	0	0	0	1	0	0	No	No	Section 10.19, RFC 4186



# 5 Formal Syntax

N/A





## 6 Related Standards

The following protocols and standards specified the behavior of Wa interface.

*Table 8 Related Standards*

Reference Interface	Standard Version
The basic function of Wa interface	3GPP system to WLAN interworking, TS 23.234 V9.0.0
The RADIUS packets exchange process	RFC2865
The RADIUS attributes used in authentication	RFC3579,RFC2869,RFC5080
The RADIUS disconnect message usage	RFC5176
The Accounting message usage	RFC2866
The EAP message usage	RFC3579
The EAP-AKA authentication message exchange	RFC4187
The EAP-SIM authentication message exchange	RFC4186
Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)	RFC5281





## Reference List

### IPWorks Library Documents

- [1] *Trademark Information*
- [2] *Glossary of Terms and Acronyms*
- [3] *Typographic Conventions*

### Standards

- [4] [Remote Authentication Dial In User Service \(RADIUS\)](#)
- [5] [Remote Authentication Dial In User Service \(RADIUS\) Support For Extensible Authentication Protocol \(EAP\)](#)
- [6] [Dynamic Authorization Extensions to Remote Authentication Dial In User Service \(RADIUS\)](#)
- [7] [RADIUS Accounting](#)
- [8] [Extensible Authentication Protocol Method for Global System for Mobile Communications\(GSM\) Subscriber Identity Modules \(EAP-SIM\)](#)
- [9] [Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement \(EAP-AKA\)](#)
- [10] [Extensible Authentication Protocol \(EAP\)](#)
- [11] [RADIUS Extensions](#)
- [12] [Common RADIUS Implementation Issues and Suggested Fixes](#)
- [13] [IEEE 802.1X RADIUS Usage Guidelines](#)
- [14] [Chargeable User Identity](#)
- [15] [3GPP system to Wireless Local Area Network \(WLAN\) interworking, TS 23.234 V9.0.0](#)
- [16] [3GPP Interworking between the Public Land Mobile Network \(PLMN\) supporting packet based services and Packet Data Networks \(PDN\), TS 29.061 V9.0.0](#)
- [17] [3GPP Evolved Packet System \(EPS\); Evolved General Packet Radio Service \(GPRS\) Tunnelling Protocol for Control plane \(GTPv2-C\) Stage 3, TS 29.274 v11.3.0](#)
- [18] [3GPP Numbering, addressing and identification, TS 23.003 v10.0.0](#)