

IPWorks 3GPP AAA Server-PDG Wm Interface

INTERWORK DESCRIPTION

Copyright

© Ericsson AB 2011-2014. 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 IPWorksTrademark Information.



Contents

1	Introduction	1
1.1	Prerequisites	1
1.2	Related Information	1
2	Interface Overview	3
2.1	Interface Role	3
2.2	Services	3
2.3	Encapsulation and Addressing	4
3	Procedures	7
3.1	Authentication	7
3.2	Authorization	11
4	Information Model	13
4.1	General	13
4.2	Radius Message in Wm Interface	13
4.3	EAP Message in Wm Interface	15
4.4	EAP-AKA Message in Wm Interface	15
4.5	EAP-SIM Message in Wm Interface	18
5	Error Handling	21
6	Formal Syntax or Schema	23
7	Related Standards	25
	Reference List	27





1 Introduction

This document describes the Wm reference point between IPWorks AAA server and the PDG node.

Scope

It's the IPWorks AAA server that uses this interface.

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

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]





2 Interface Overview

The prime purpose of the protocols crossing the Wm reference point is to transport authentication and authorization information in a secure manner between 3GPP AAA Server and PDG when UE access PS core network.

EAP authentication shall be transported over the Wm reference. Currently, IPWorks AAA server use RADIUS protocol to convey the EAP AKA/SIM authentication message.

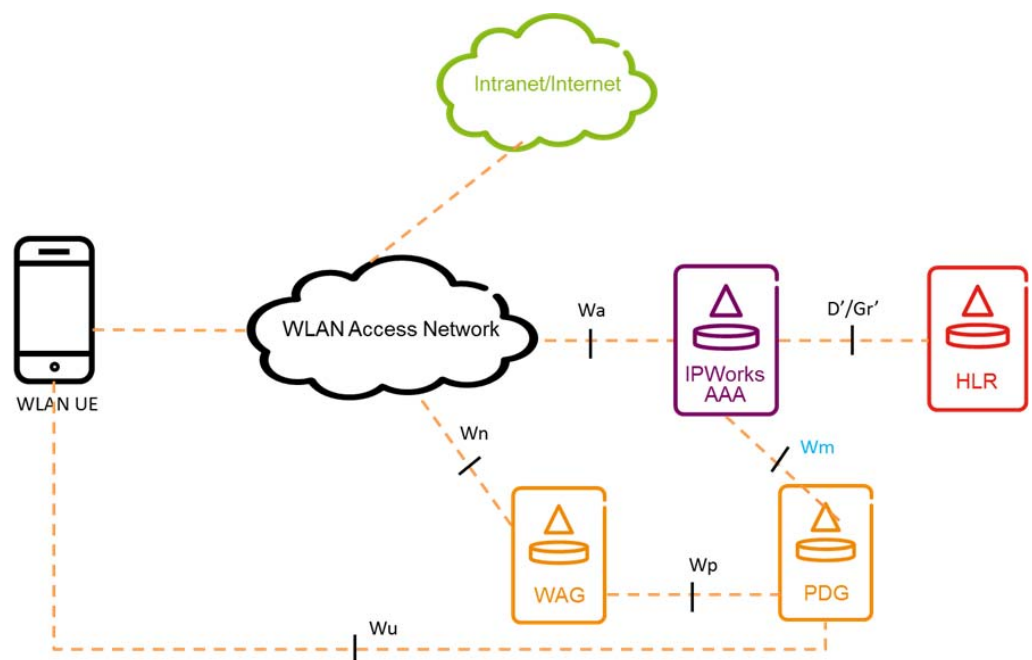


Figure 1 Wm Reference Point in 3GPP WLAN Inter-working Reference Model

2.1 Interface Role

In Wm reference point, IPWorks AAA server will take the role AAA in 3GPP network.

2.2 Services

The services offered by the Wm reference point are shown in Table 1.

Table 1 Offered Services

Offered Service	Description
Authentication, Authorization	IPWorks AAA server offers the Authentication and Authorization service to PDG.

2.3 Encapsulation and Addressing

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

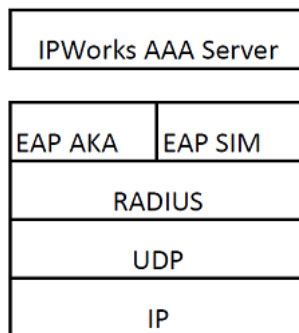


Figure 2 Protocol Stack Used on IPWorks AAA Server

The offered WLAN access authentication and authorization service by IPWorks AAA server is addressed by the following RADIUS packets which defined in RFC2865, RFC3579:

- 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, including 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, including 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





3 Procedures

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

3.1 Authentication

IPWorks AAA server supports EAP-AKA/SIM authentication methods for WLAN access in Wm reference point.

The following figures show the basic EAP-AKA/SIM authentication procedures base on Radius protocol, include full authentication and fast re-authentication.

3.1.1

EAP-AKA full authentication

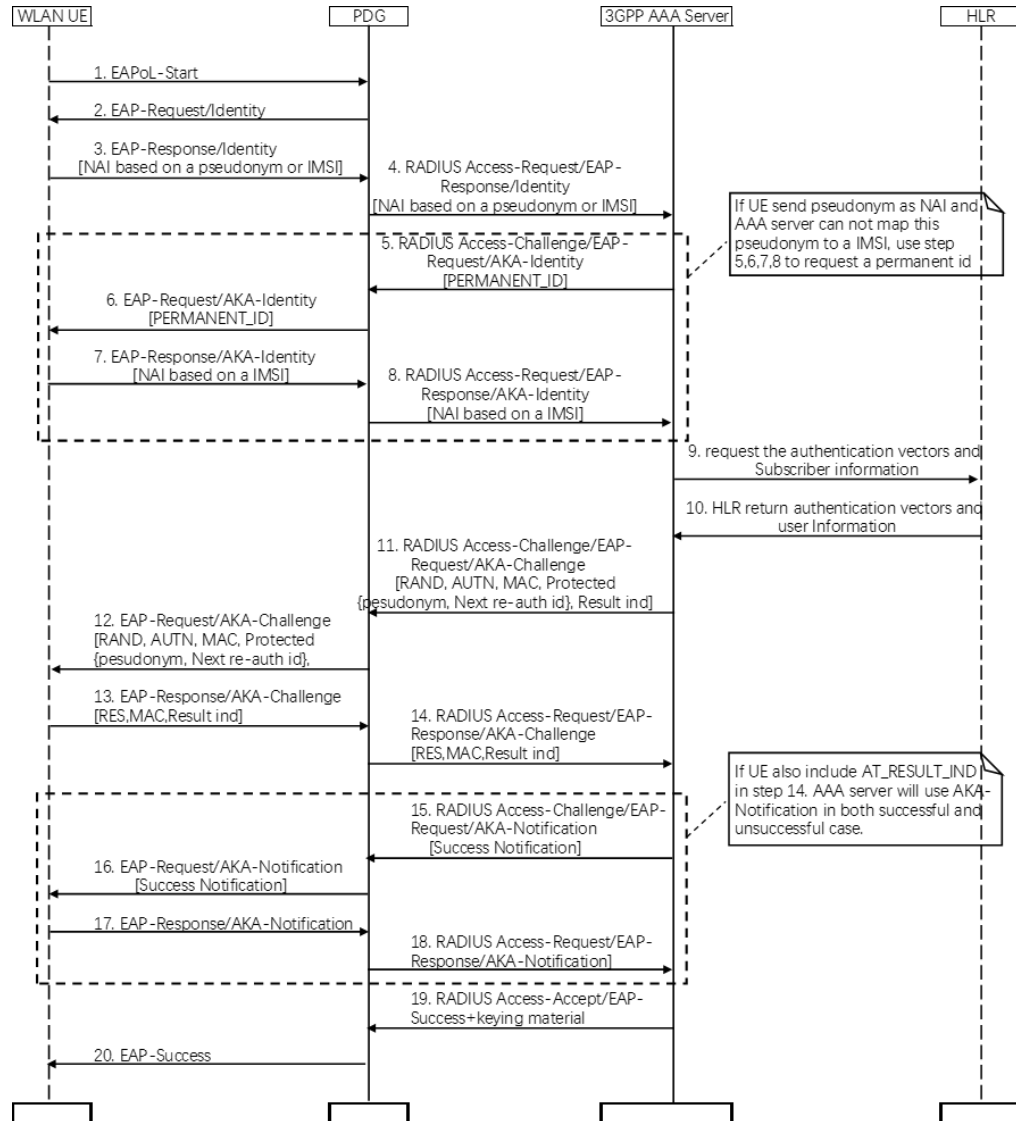


Figure 3 EAP-AKA Full Authentication Flow

3.1.2 EAP-SIM full authentication

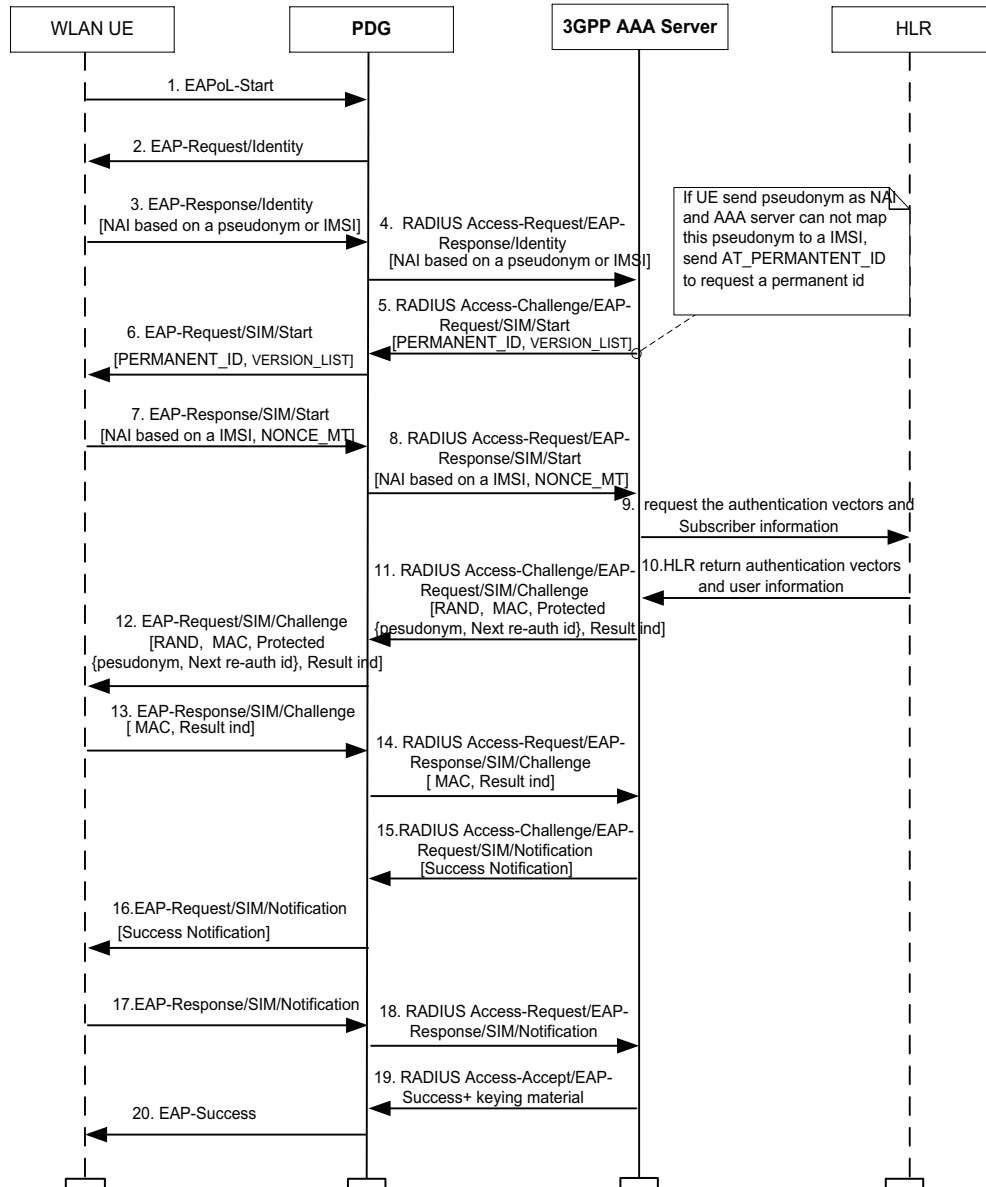


Figure 4 EAP-SIM Full Authentication Flow

3.1.3 EAP-AKA fast re-authentication

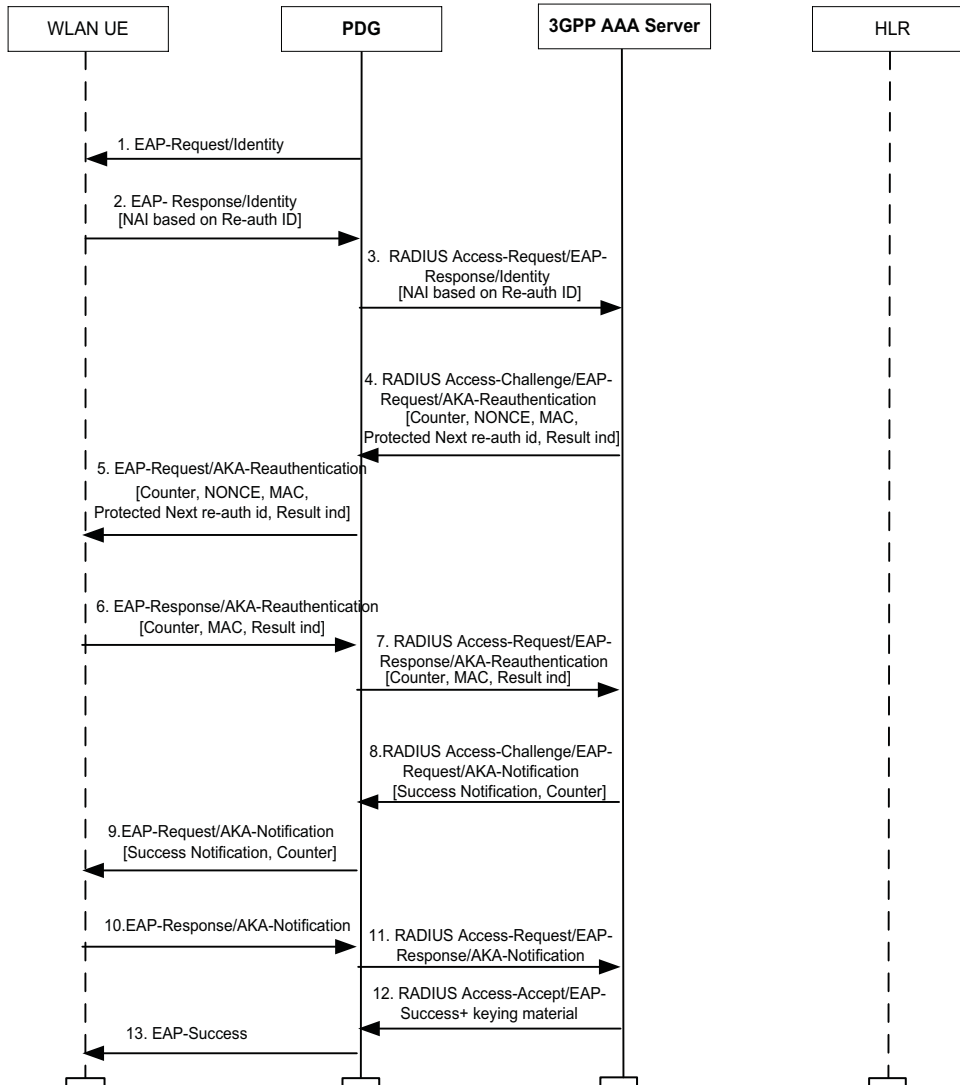


Figure 5 EAP-AKA Fast Re-Authentication Flow



3.1.4 EAP-SIM fast re-authentication

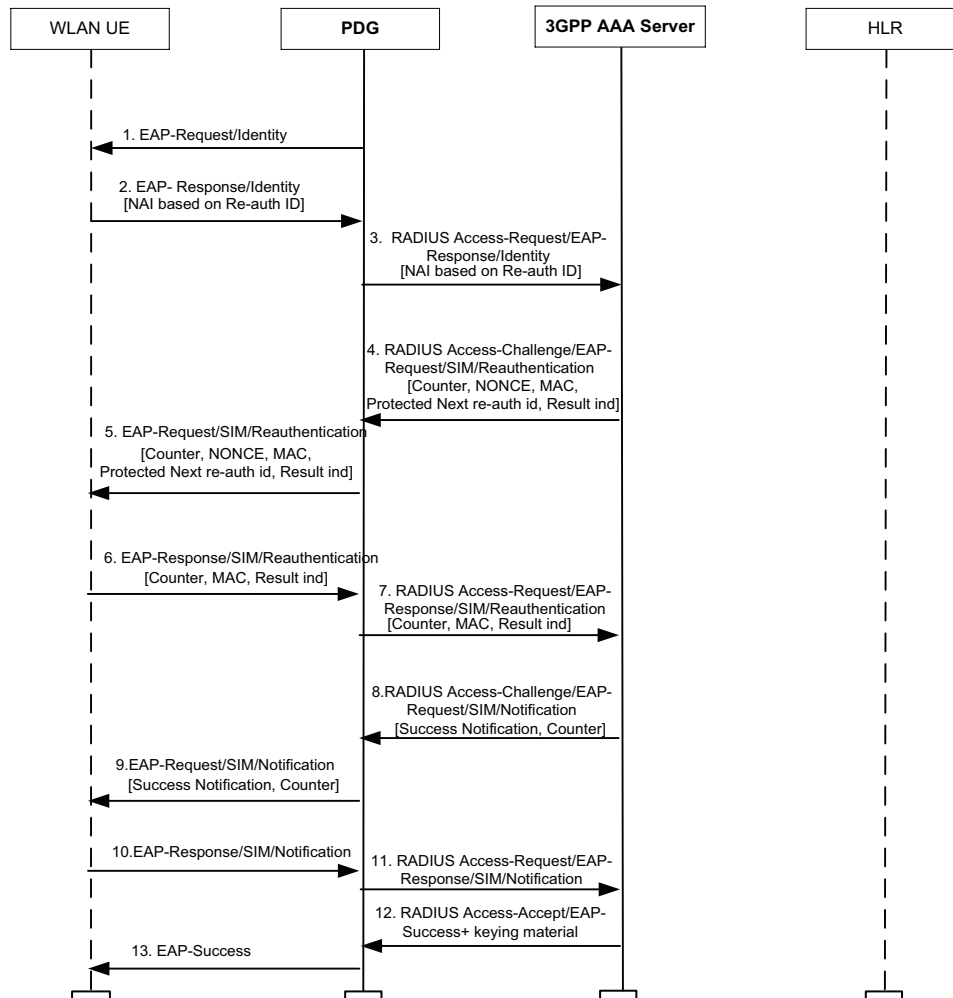


Figure 6 EAP-SIM Fast Re-Authentication Flow

3.2 Authorization

IPWorks AAA server tries to get the subscriber information from HLR to decide whether allow the user access WLAN network and send related information to PDG, including:

- **3GPP-Charging-Characteristics:** this attribute is from the MAP message MAP-INSERT-SUBSCRIBER-DATA, AAA tries to get the ChargingCharacteristics attribute of PDP-Context for setting the value.
- **3GPP-PDP-Type:** this attribute is from the MAP message MAP-INSERT-SUBSCRIBER-DATA, AAA tries to get the PDP-Type attribute of PDP-Context for setting the value, for example, IPv4, IPv6, IPv4v6.



- 3GPP-GPRS-Negotiated-QoS-Profile: this attribute is from the MAP message MAP-INSERT-SUBSCRIBER-DATA, AAA tries to get the Ext-Qos-Subscribed attribute of PDP-Context for setting the value.



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 Attribute description

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 sub-attributes. For example, `26/311-28` is the code of Microsoft vendor-specific RADIUS attribute MS-Primary-DNS-Server.

4.2 Radius Message in Wm Interface

The messages supported by Wm interface comply with the RADIUS data format which is defined in section 3 in RFC 2865 including:

- Authentication/Authorization: Access-Request, Access-Accept, Access-Reject, Access-Challenge

Following table lists the attributes which be used in the messages of Wm interface. If the messages also include other attributes according related protocols, AAA server will bypass them.



Table 3 Radius Message

Attr #	Attribute Name	Access-Request	Access-Accept	Access-Reject	Access-Challenge	Description
1	User-Name	1	1	1	1	Section 5.1, RFC 2865
4	NAS-IP-Address	1	0	0	0	Section 5.4, RFC 2865
27	Session-Timeout	0	0-1	0	0-1	Section 5.27, RFC 2865 Section 3.17, RFC 3580
30	Called-Station-Id	1	0	0	0	Section 5.30, RFC 2865
31	Calling-Station-Id	0-1	0	0	0	Section 5.31, RFC 2865
64	NAS-Port-Type	1	0	0	0	Section 5.17, RFC 2869
79	EAP-Message	1+	1+	1+	1+	Section 3.1, RFC 3579
80	Message-Authenticator	1	1	1	1	Section 3.2, RFC 3579
85	Acct-Interim-Interval	0	1	0	0	Section 5.16, RFC 2869
89	Chargeable-User-Id	1	1	0	0	Section 2.2, RFC 4372
26/311-17	MS-MPPE-Recv-Key	0	1	0	0	Section 2.4.2, RFC 2548
26/311-16	MS-MPPE-Send-Key	0	1	0	0	Section 2.4.3, RFC 2548



Attr #	Attribute Name	Access-Request	Access-Accept	Access-Reject	Access-Challenge	Description
26/10415-2	3GPP-Charging-ID	1	0	0	0	Section 5.25, RFC 2865
26/10415-13	3GPP-Charging-Characteristics	0	1	0	0	3GPP TS29.061
26/10415-3	3GPP-PDP type	0	0-1	0	0	3GPP TS29.061
26/10415-5	3GPP-GPRS-Negotiated-QoS-Profile	0	1	0	0	3GPP TS29.061

4.3 EAP Message in Wm Interface

In Wm interface, following EAP packets are used for authentication:

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

Following EAP types are used in EAP Request/Response exchanges for the Wm interface:

- Identity (1)
- EAP-AKA(23)
- EAP-SIM(18)

4.4 EAP-AKA Message in Wm Interface

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

- 1 EAP-Request/AKA-Identity
- 2 EAP-Response/AKA-Identity



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

The column denoted with "E" indicates whether the attribute is a nested attribute that MUST be included within AT_ENCR_DATA.

Table 4 Attributes Supported by EAP-AKA Message for Wm 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_AUTH_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_REQUIRE	0	0	1	0	0	0	0	0	0	0	0	No	Section 10.6, RFC 4187
AT_AUTHN	0	0	1	0	0	0	0	0	0	0	0	No	Section 10.7, RFC 4187
AT_REQUIRE	0	0	0	1	0	0	0	0	0	0	0	No	Section 10.8, RFC 4187



Attribute Name	1	2	3	4	5	6	7	8	9	10	11	E	Description
AT_A UTS	0	0	0	0	0	0	0	0	0	0	1	No	Section 10.9, RFC 4187
AT_N EXT_ PSEU DONY M	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 ADDIN G	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_IND	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 ONCE _S	0	0	0	0	0	0	0	1	0	0	0	Yes	Section 10.18, RFC 4187



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 Wm 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:

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

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 5 EAP-SIM Message in Wm 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



Attribute Name	1	2	3	4	5	6	7	8	9	Encr	Skip	Description
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
AT_PERMISSION_DENIED_REQ	0-1	0	0	0	0	0	0	0	0	No	No	Section 10.5, RFC 4186
AT_AUTH_DENIED_REQ	0	0	0	0	0	0	0	0	0	No	No	Section 10.6, RFC 4186
AT_FULL_AUTH_REQUIRED	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_REQUIRE	0	0	1	0	0	0	0	0	0	No	No	Section 10.9, RFC 4186
AT_NEXT_PS_EUD_ONLY_M	0	0	0-1	0	0	0	0	0	0	Yes	Yes	Section 10.10, RFC 4186
AT_NEXT_REQUIRED_AUTH_ID	0	0	1	0	0	0	0	0-1	0	Yes	Yes	Section 10.11, RFC 4186



Attribute Name	1	2	3	4	5	6	7	8	9	Encr	Skip	Description
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_TO_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 Error Handling

Table 6 describes the behaviors of different error scenarios:

Table 6 Error Handling

Scenario	Return Code
ACCOUNTING_REQUEST and ACCOUNTING_REQUEST Duplicated	discard
ACCOUNTING_REQUEST failed to check the accounting request authenticator	discard
PROXY_RESPONSE failed to check the reply authenticator	discard
PROXY_RESPONSE failed to get the proxy message record	discard
DA_RESPONSE failed to get the DA message record	discard
DA_RESPONSE failed to check the reply authenticator for DA message	discard
Failed to validate Message-Authenticator	discard
ACCESS_REQUEST The number of attributes is wrong	ACCESS_REJECT
DM_REQUEST and COA_REQUEST The number of attributes is wrong	ACCESS_REJECT
The number of attributes is wrong for other messages	discard
Access-Request message does not contain a User-Name or a Calling-Station-ID or a Called-station-ID	discard
Access-Request a NAS-IP-Address or a NAS-Identifier or a NAS-IPv6-Address (or all) is not contained in the message	discard
Access-Request EAP-Message existed with no Message-Authenticator contained in the message	discard



Scenario	Return Code
Accounting-Request a NAS-IP-Address or a NAS-Identifier (or both) is not contained in the message	discard
an Acct-Status-Type is not contained in the Accounting-Request message	discard
Accounting-Request message does not include Acct-Session-Id	discard
Acct-Status-Type is not set to stop in the Accounting -Request message	discard
Acct-Status-Type is not set to start in the Accounting -Request message	discard
Attribute with wrong length ⁽¹⁾	ACCESS_REJECT/discard
unsupported attribute ⁽¹⁾	ACCESS_REJECT/discard
Attribute of string type value error ⁽¹⁾	ACCESS_REJECT/discard
Attribute of integer value error ⁽¹⁾	ACCESS_REJECT/discard
Attribute of IPv4 type value error ⁽¹⁾	ACCESS_REJECT/discard

(1) This ACCESS_REJECT scenario is only for the ACCESS_REQUEST, COA_REQUEST and DM_REQUEST messages. The AAA server discards the other types of messages.



6 Formal Syntax or Schema

N/A





7 Related Standards

Following protocols and standards specified the behavior of Wm interface.

- 3GPP TS 23.234 specified the basic function of Wm interface.
- The Radius packets exchange process is specified in RFC2865
- The Radius attributes which used in authentication are explained and defined by RFC3579, RFC2869, RFC5080, and 3GPP TS29.061
- The EAP message usage is specified in RFC3579
- The EAP-AKA authentication message exchange is follow RFC4187
- The EAP-SIM authentication message exchange is follow RFC4186





Reference List

IPWorks Library Documents

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

Other Documents

- [4] [Remote Authentication Dial In User Service \(RADIUS\)](#)
- [5] [RADIUS \(Remote Authentication Dial In User Service\) Support For Extensible Authentication Protocol \(EAP\)](#)
- [6] [Dynamic Authorization Extensions to Remote Authentication Dial In User Service \(RADIUS\)](#)
- [7] [Extensible Authentication Protocol Method for Global System for Mobile Communications\(GSM\) Subscriber Identity Modules \(EAP-SIM\)](#)
- [8] [Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement \(EAP-AKA\)](#)
- [9] [Extensible Authentication Protocol \(EAP\)](#)
- [10] [RADIUS Extensions](#)
- [11] [Common Remote Authentication Dial In User Service \(RADIUS\) Implementation Issues and Suggested Fixes](#)
- [12] [IEEE 802.1X Remote Authentication Dial In User Service \(RADIUS\) Usage Guidelines](#)
- [13] [Chargeable User Identity](#)
- [14] [3GPP system to Wireless Local Area Network \(WLAN\) interworking, TS 23.234 V9.0.0](#)
- [15] [Interworking between the Public Land Mobile Network \(PLMN\) supporting packet based services and Packet Data Networks \(PDN\) 3GPP TS29.061 R8](#)
- [16] [Microsoft Vendor-specific RADIUS Attributes](#)