

Prepared (also subject responsible if other) ECHGCHI		No. 58/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

## IPWorks AAA Overview

### Contents

<b>1</b>	<b>Introduction.....</b>	<b>2</b>
1.1	Document History .....	2
1.2	Purpose .....	2
1.3	Scope .....	2
1.4	Document Structure.....	2
<b>2</b>	<b>Overview of AAA .....</b>	<b>2</b>
2.1	Overview.....	2
2.2	IPWorks AAA Server Functionality Architecture .....	3
2.3	IPWorks AAA Server Component Architecture .....	4
2.4	IPWorks AAA Interworking Reference Model.....	4
2.4.1	Network Element .....	5
2.4.2	Reference Points .....	6
2.4.3	Northbound Interfaces .....	7
2.5	IPWorks AAA Supported Protocols .....	7
2.6	IPWorks AAA Basic Function .....	8
2.6.1	RADIUS AAA Basic Function .....	8
2.6.2	EPC AAA Basic Function .....	9
<b>3</b>	<b>AAA Feature Scenarios.....</b>	<b>10</b>
3.1	Generic RADIUS AAA Functionality .....	10
3.2	IPWorks 3GPP AAA (I-WLAN) .....	10
3.3	IPWorks RADIUS Wi-Fi AAA in ENIW.....	10
3.4	IPWorks AAA for Trusted Non-3GPP IP Access (STa) .....	11
3.5	IPWorks AAA for Untrusted Non-3GPP IP Access (SWm) .....	11
3.6	IPWorks Front End AAA Function .....	11
<b>4</b>	<b>Operational Conditions.....</b>	<b>11</b>
<b>5</b>	<b>Standard Compliance Statement .....</b>	<b>11</b>
<b>6</b>	<b>Miscellaneous .....</b>	<b>11</b>
<b>7</b>	<b>Terminology .....</b>	<b>11</b>
7.1	Abbreviations.....	11
7.2	Definitions.....	12
<b>8</b>	<b>References .....</b>	<b>12</b>
8.1	3GPP Technical Specifications .....	12
8.2	Requests for Comments (RFCs) .....	13
8.3	IPWorks Documents.....	13

Prepared (also subject responsible if other) ECHGCHI		No. 58/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

## 1 Introduction

### 1.1 Document History

Rev	Date	Sign.	Comment
PA1	2017-04-01	ECHGCHI	Initial Draft, based on 20/155 17-AVA 901 16 Uen C.
PB1	2017-08-01	EJIOXUE	Update table 1, impacted by PKI FE feature.

### 1.2 Purpose

The purpose of this document is to describe the AAA server functions supported by IPWorks.

### 1.3 Scope

This document mainly focuses on giving a brief overview of the IPWorks AAA function modules and the relationship between those modules.

**Note:** The TLS/TTLS/PEAP/ EAP-MSCHAPv2 authentication methods are out of the current release scope. They will be implemented in the later release.

### 1.4 Document Structure

## 2 Overview of AAA

This section provides a brief description of the functions included in the IPWorks AAA server.

### 2.1 Overview

The IPWorks AAA Server supports the RADIUS and Diameter protocols. Both protocols are industry standard methods for providing authentication, authorization, and accounting (AAA) services.

- Authentication is the process of verifying a subscriber identity and associating more information to the logon session of subscriber.
- Authorization is the process of determining whether the subscriber is allowed on the network and controlling network access values based on a defined security policy.

Prepared (also subject responsible if other) ECHGCHI		No. 58/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

- Accounting is the process of generating log files that record session statistics used for billing, system diagnosis, and usage planning.

According to the difference of convey protocol, we divide IPWorks AAA into two components, RADIUS AAA server and EPC AAA server. Each of them can work independently to serve for different applications. And in certain special scenario, RADIUS AAA server and EPC AAA server can also work together to provide AAA service.

## 2.2

### IPWorks AAA Server Functionality Architecture

Figure 1 represents IPWorks AAA functionality architecture that is a layered model divided into different types of layer:

- a transport protocol layer
- an application protocol layer
- a basic function & interface layer
- a feature classification layer
- an authentication method layer

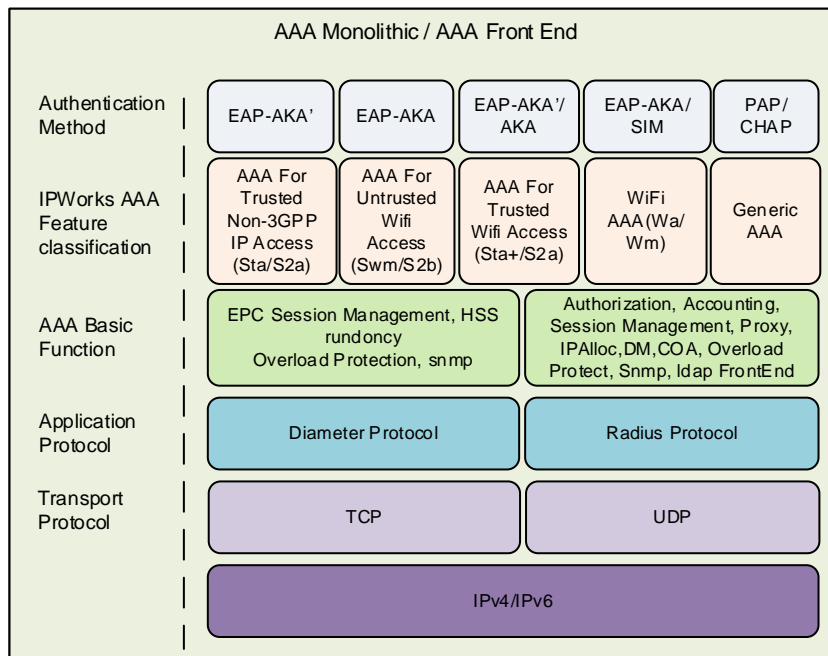


Figure 1 **Error! Reference source not found.** AAA Server Functionality Architecture

Prepared (also subject responsible if other) ECHGCHI		No. 58/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

## 2.3 IPWorks AAA Server Component Architecture

In the default scenario, IPWorks AAA server works on two protocol servers to achieve the traffic and data redundancy. They are two types of AAA server, including Radius AAA and EPC AAA, when deployed on the target machine and shared Server Manager and MySQL NDB Cluster.

The EPC AAA server and the RADIUS AAA server constitute the complete AAA solution for different network scenarios. Figure 2 illustrates the relationship between EPC AAA server and RADIUS AAA server.

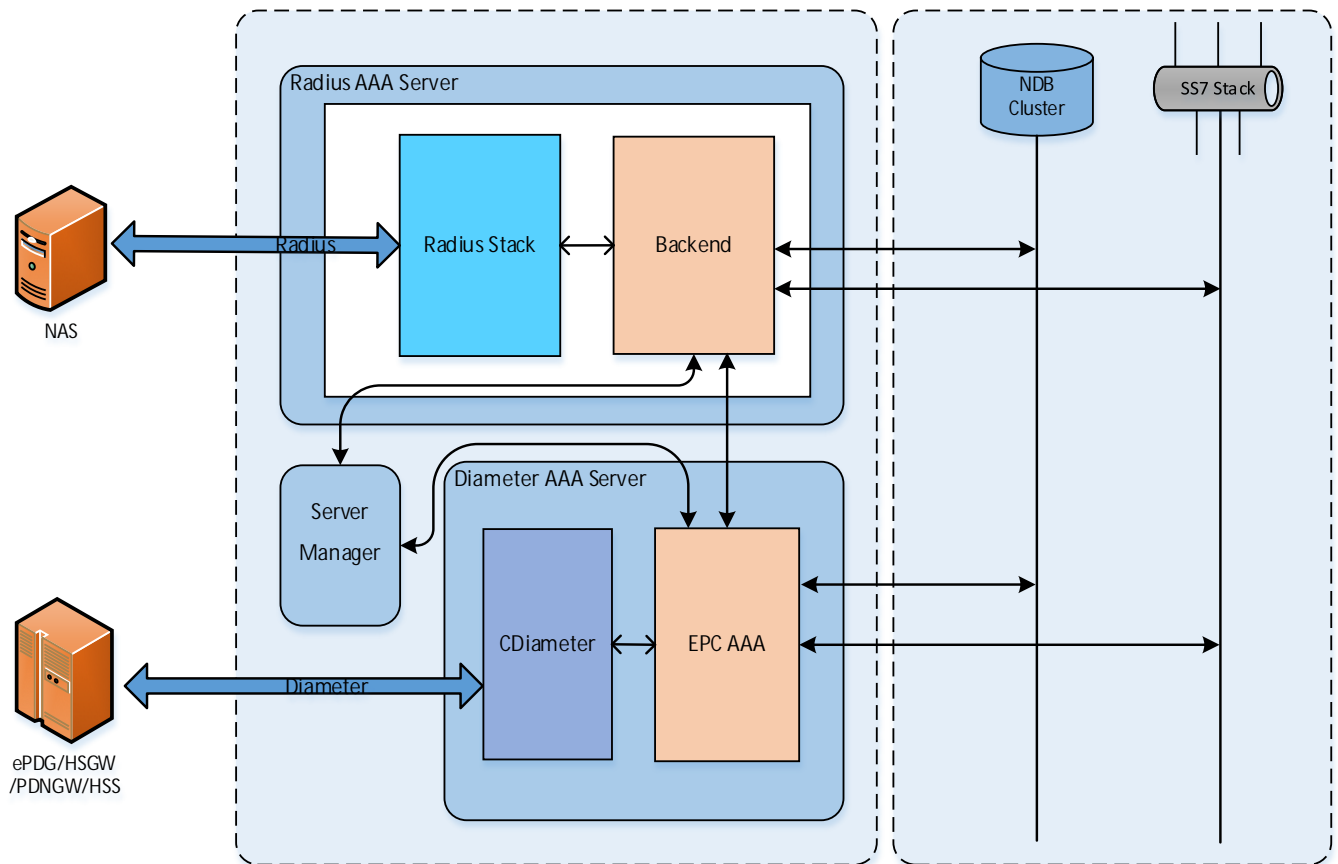


Figure 2 AAA Server Component Architecture

## 2.4 IPWorks AAA Interworking Reference Model

The network devices that make up a 3GPP network are called network elements. Each network element performs a specific function. As shown in Figure 3, network elements communicate with each other over reference points. This section provides a brief overview of the IPWorks AAA reference model and interface. For details, refer to the appropriate 3GPP specification and IPWorks CPI documents.

Prepared (also subject responsible if other) <b>ECHGCHI</b>		No. <b>58/155 17-AVA 901 16 Uen</b>		
Approved	Checked	Date <b>2017-08-24</b>	Rev <b>PB1</b>	Reference

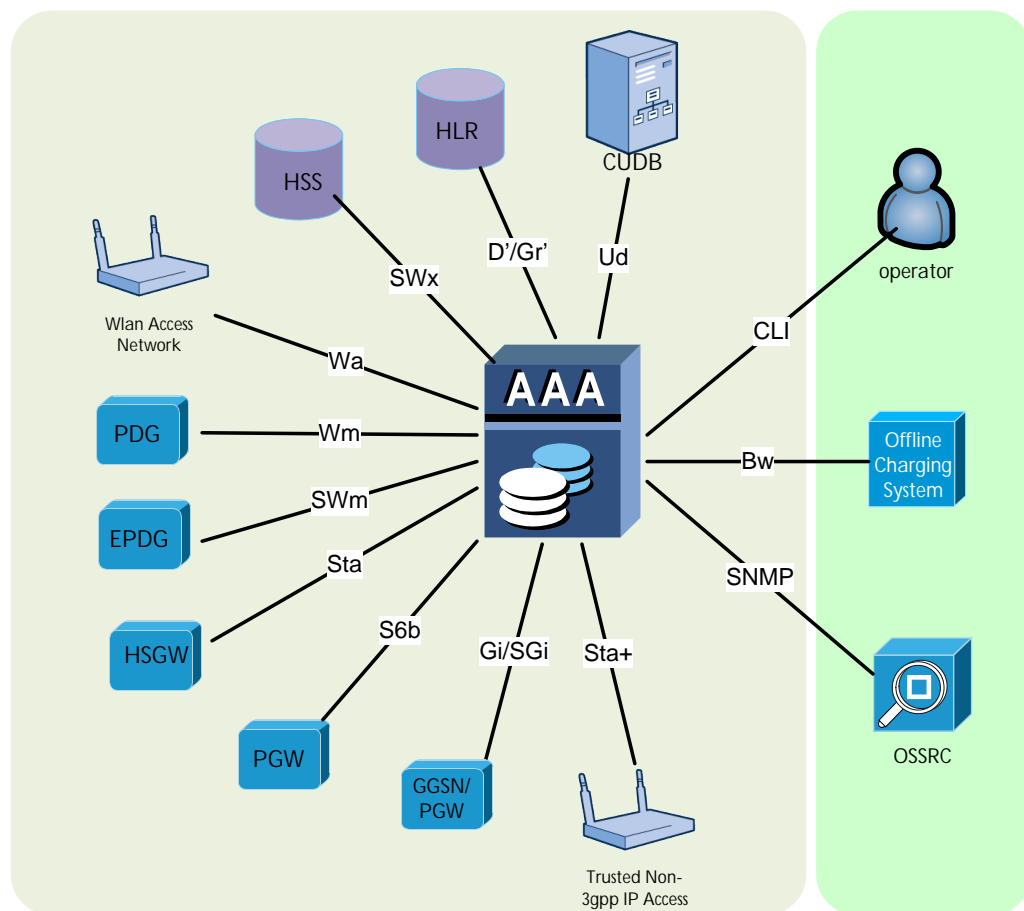


Figure 3 AAA Server Reference Model

#### 2.4.1

#### Network Element

**HSS:** The Home Subscriber Server (HSS) is a central database that contains user-related and subscription-related information. The functions of the HSS include functionalities, such as mobility management, call and session establishment support, user authentication and access authorization.

**HLR:** The Home Location Register (HLR) 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.

**WLAN AN:** The Wireless LAN Access Network (WLAN AN) provides the wireless IP connectivity to the WLAN UE so that requests from the WLAN UE can be authenticated and authorized by the IPWorks AAA server in the 3GPP network.

Prepared (also subject responsible if other) ECHGCHI		No. 58/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

**PDG:** The Packet Data Gateway (PDG) performs authentications and authorizations for tunnel requests, when tunneled IP service (WLAN 3GPP IP Access) is being provided. 3GPP PS (Packet Switched) services are accessed through a PDG in the subscriber's HPLMN (Home Public Land Mobile Network) or a PDG in the selected VPLMN

**ePDG:** The main function of the ePDG (Evolved Packet Data Gateway) is to secure the data transmission with a UE connected to the EPC over an untrusted non-3GPP access. For this purpose, the ePDG acts as a termination node of IPsec tunnels established with the UE. And during such process, the authentication and authorization procedures are used between the ePDG and IPWorks AAA.

**HSGW:** The HRPD Serving Gateway (HSGW) connects the 3GPP2 eHRPD access with the 3GPP EPC (Evolved Packet Core) as a trusted non-3GPP access network.

**PGW:** The PDN Gateway (PGW) provides connectivity from the UE to external packet data network by being the point of exit and entry of traffic for the UE. A UE may have simultaneous connectivity with more than one PGW for accessing multiple PDNs.

**GGSN/PGW:** The Gateway GPRS Support Node (GGSN) is a main component of the GPRS network. The GGSN is responsible for the interworking between the GPRS network and external packet switched networks.

**Offline Charging System:** The WLAN AN periodically forwards collected offline charging information to the 3GPP AAA Server, which in turn forwards this information to the Offline Charging System.

#### 2.4.2 Reference Points

**Gi/SGi:** The Gi reference point is between the GGSN and the external IP network. A GGSN may, on a per APN basis, use RADIUS authentication to authenticate a user and RADIUS accounting to provide information to IPWorks AAA server.

**Wa:** The Wa reference point connects the WLAN Access Network, possibly via intermediate networks, to the 3GPP Network. The prime purpose of the protocols crossing this reference point is to transport authentication, authorization, and charging-related information in a secure manner. IPWorks AAA supports Radius-based EAP-AKA and EAP-SIM authentication methods.

**Wm:** The Wm reference point between AAA Server and PDG is based on RADIUS. It is used during establishment of the secure tunnel using the EAP-AKA/SIM authentication procedures with the RADIUS operations as described in Wa reference point.

**D'/Gr':** The D'/Gr' reference point is the interface between the AAA Server node and HLR node. D'/Gr' interfaces use the Mobile Application Part (MAP) protocol to obtain the authentication vector and subscriber profile from HLR.

Prepared (also subject responsible if other) ECHGCHI		No. 58/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

**STa:** The STa reference point between Trusted Non-3GPP IP Access (such as CDMA2000 Access Network) and the 3GPP AAA Server/Proxy. And STa is used to transport access authentication, authorization, mobility parameters, and charging-related information in a secure manner.

**SWm:** This reference point is located between IPWorks AAA Server and ePDG and is used for AAA signalling (transport of mobility parameters, tunnel authentication, and authorization data).

**S6b:** It is the reference point between PDN Gateway and 3GPP AAA server/proxy for mobility-related authentication if needed. This reference point may also be used to retrieve and request storage of mobility parameters. This reference point may also be used to retrieve static QoS profile for a UE for non-3GPP access in case dynamic PCC is not supported.

**SWx:** SWx reference point is located between 3GPP AAA Server and HSS and is used for transport of authentication vectors and user profiles from HSS, register, and deregister user into HSS and also update the PDN GW information in HSS.

**STa+:** RADIUS STa+ is the customized reference point between WIC/EWG and IPWorks AAA in ENIW solution. The reference point is RADIUS-based. And it is used for access authentication and authorization when Trusted WLAN user to access to EPC via S2a or to use NSWO.

**Ud:** It is the reference point between a FE and CUDB, it is used for AAA-FE to retrieve user authentication data and profile from CUDB via LDAP protocol.

### 2.4.3 Northbound Interfaces

**Bw:** The Bw reference point is used between AAA Server and Offline Charging System. IPWorks AAA supports to generate the Accounting CDRs locally and provides the FTP/SFTP interface to Offline Charging System for uploading or fetching the CDR data.

**SNMP:** IPWorks AAA uses SNMP protocol as interworking with OSS-RC for Fault Management and Performance Management purpose.

**CLI:** Operator can use IPWorks command line interface (CLI) to manage part of configuration items and provision user profile into the local *MYSQL* database.

## 2.5 IPWorks AAA Supported Protocols

**Diameter:** IPWorks EPC AAA server depends on Diameter Stack for providing the Diameter protocol implementation.

**RADIUS:** A standalone RADIUS stack process is implemented to provide RADIUS message sending and receiving actions.

**TCP:** IPWorks EPC AAA server uses TCP as the transport protocol.

Prepared (also subject responsible if other) ECHGCHI		No. 58/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

**UDP:** IPWorks RADIUS AAA server uses UDP protocol as the transport protocol.

**IPv4/IPv6:** Both the IPWorks RADIUS AAA server and EPC AAA server support working on IPv4 and IPv6 stack.

## 2.6 IPWorks AAA Basic Function

The whole IPWorks AAA server consists of some basic functions. In different networks scenarios, IPWorks AAA server supports difference basic function. Considering the difference on RADIUS AAA and EPC AAA, some basic functions may have different behavior and implementation. Table 1 shows the usage status in different scenarios.

Table 1 IPWorks AAA Basic Function List

	IPWorks RADIUS AAA			IPWorks EPC AAA	
	Generic AAA (GPRS)	3GPP AAA (I-WLAN)	Wi-Fi AAA (ENIW)	Trusted Non-3GPP IP Access (STa)	Untrusted Non-3GPP IP Access (SWm)
Authentication	PAP/CHAP	EAP-AKA/SIM	EAP-AAA/SIM EAP-AKA' (1)	EAP-AKA'	EAP-AKA
Authorization	support	support	support	support	support
Accounting	support	support	support		
IP Allocation	support		partial support (4)		
Proxy	support	support	support		
DM/COA	support	support(2)	support		
Session Management	support	support	support	support	support
Overload Protection	support	support	support	support	support
FM/PM	support	support	support	support	support
CUDB FrontEnd	support		partial support(3)		support
SLF/HSS Redundancy				support	support
<p>Note1: In ENIW Trusted Wi-Fi Access, RADIUS AAA might mediate EAP-AKA/EAP-AKA' authentication to EPC AAA and only EPC AAA can handling EAP-AKA' authentication request.</p> <p>Note2: Besides CLI initiated DM/COA message, RADIUS AAA also support HLR initiated DM procedure</p> <p>Note3: If non-SIM based authentication use local user profile, the CUDB front end is supported</p> <p>Note4: If non-SIM based authentication use local user profile, the IP Allocation is supported</p>					

### 2.6.1 RADIUS AAA Basic Function

This section gives a simple list for some basic function that can be shared in different RADIUS AAA feature scenarios. Those basic functions might have different behaviors in different scenarios. For more details, please refer to IPWorks Generic AAA Function Overview.



Prepared (also subject responsible if other) ECHGCHI		No. 58/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

**Authentication:** RADIUS AAA supports the authentication procedure base on the user policy which been save in local MYSQL database or the subscriber profile which been retrieved from HLR.

**Authorization:** This function determines whether a requesting entity is allowed to access a resource. The RADIUS AAA server might authorize the request by checking whether the preconfigured policy matches the corresponding attributes in the *Access-Accept* message or subscriber information received from HLR.

**Accounting:** RADIUS AAA collects the resource usage for analysis or billing purposes according to the RADIUS Accounting Request message.

**IP Allocation:** RADIUS AAA supports allocating an IPv4 address or IPv6 prefix for an authenticated user.

**Proxy:** RADIUS AAA server can work as Proxy mode for transmitting RADIUS messages to other RADIUS AAA server. In proxy scenarios, the RADIUS AAA Server acts as a RADIUS client.

**DM/COA:** Change of Authorization and Disconnect Messages are for RADIUS dynamic authorization requests.

**Session Management:** RADIUS AAA allows operator to use CLI interface to search and clean related RADIUS accounting session.

**Overload Protection:** RADIUS AAA can buffer received RADIUS message in RADIUS stack and discard some message in overload situation for ensuring some degree of success rate.

**FM/PM:** RADIUS AAA can collect statistics and report alarms through a standalone RADIUS AAA SNMP subagent.

## 2.6.2 EPC AAA Basic Function

Different EPC AAA feature scenarios are implemented in similar architecture and share some basic functions. For more details, refer to Section 3 in *IPWorks EPC AAA Function Overview* [23].

- Authentication: EPC AAA supports the authentication procedure base on the subscriber profile which been retrieved from HSS.
- Authorization: This function determines whether a requesting entity is allowed to access a resource. The RADIUS AAA server might authorize the request by checking whether the preconfigured policy matches the corresponding attributes in the *Access-Accept* message or subscriber information received from HLR.
- SLF/HSS Redundancy: EPC AAA supports to connect to several SLF/HSS to achieve HSS redundancy, with either failover mode or round-robin mode.

Prepared (also subject responsible if other) ECHGCHI		No. 58/155 17-AVA 901 16 Uen	
Approved	Checked	Date 2017-08-24	Rev PB1
		Reference	

- Session Management: EPC AAA allows operator to use CLI interface to search and clean related diameter session.
- Overload Protection: When an incoming traffic load on IPWorks EPC AAA server exceeds the engineered capacity, it triggers the Overload Protection mechanism, and then EPC AAA server handles the traffic with reduced capacity through sending back DIAMETER\_TOO\_BUSY code.
- FM/PM: EPC AAA can collect statistics and report alarms through a standalone EPC AAA SNMP subagent.

### 3 AAA Feature Scenarios

This section provides some short descriptions for different AAA feature scenarios.

#### 3.1 Generic RADIUS AAA Functionality

A GGSN might, on a per APN basis, use RADIUS authentication to authenticate a user and RADIUS accounting to provide information to an AAA server. IPWorks Radius Generic AAA supports PAP and CHAP as the authentication method when AAA interworks with GGSN.

In addition, as the first RADIUS AAA feature scenario, generic RADIUS AAA also implements most of basic RADIUS AAA function which can be used by other RADIUS AAA feature scenarios.

For more details, refer to *IPWorks Generic AAA Function Overview* [24] .

#### 3.2 IPWorks 3GPP AAA (I-WLAN)

The IPWorks RADIUS AAA Server can perform SIM-based authentication, subscription authorization (EAP-AKA/SIM), and accounting (AAA) in 3GPP WLAN Interworking environments where the subscriber database is a HLR as referenced in 3GPP TS 23.234.

The 3GPP Wa interface is used for EAP client authentication with HLR and the Wm interface (limited support) is used for tunnel mapping in the PDG.

For more details, refer to Section 4 in *IPWorks RADIUS Wi-Fi AAA Function Overview* [25].

#### 3.3 IPWorks RADIUS Wi-Fi AAA in ENIW

Ericsson's Network Integrated Wi-Fi (ENIW) solution is one part of the Ericsson HetNet concept. IPWorks AAA can be used in this solution to authenticate SIM-based devices in the Home Location Register (HLR) and connects traffic from the Wi-Fi access network through the mobile packet network and up to the service environment of mobile similar as in I-WLAN solution.

Prepared (also subject responsible if other) ECHGCHI		No. 58/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

And as an extension, IPWorks RADIUS AAA also supports some other function in ENIW, such as:

- RADIUS AAA works in Trusted WLAN and 3GPP Interworking.
- Authorization for APN-based Wi-Fi subscription
- Accounting Forward/Mediation.

For more details, refer to Section 5 in *IPWorks Radius WiFi AAA Function Overview*.

### 3.4 IPWorks AAA for Trusted Non-3GPP IP Access (STa)

This AAA feature scenario is used in EPC network to do the work of authentication, authorization, and accounting for the user accessing EPC through trusted Non-3GPP IP Access Network, such as CDMA2000 HSGW.

For more details, refer to Section 4 in *IPWorks EPC AAA Function Overview* [23].

### 3.5 IPWorks AAA for Untrusted Non-3GPP IP Access (SWm)

In the case of if there are untrusted IP access network, IPWorks AAA supports the SWm interface, which provides the mandatory authentication and authorization with IPsec tunnel setup between UE and ePDG.

For more details, refer to Section 5 in *IPWorks EPC AAA Function Overview* [23].

### 3.6 IPWorks Front End AAA Function

For more details, refer to *IPWorks AAA Front End Function Overview* [22].

## 4 Operational Conditions

## 5 Standard Compliance Statement

See *Statement of Compliance for IPWorks* Error! Reference source not found..

## 6 Miscellaneous

## 7 Terminology

### 7.1 Abbreviations

AAA	Authentication, Authorization, Accounting
AKA	Authentication and Key Agreement

Prepared (also subject responsible if other) <b>ECHGCHI</b>		No. <b>58/155 17-AVA 901 16 Uen</b>		
Approved	Checked	Date <b>2017-08-24</b>	Rev <b>PB1</b>	Reference

APN	Access Point Name
CHAP	Challenge-Handshake Authentication Protocol
CoA	Change of Authorization
DM	Disconnect Message
EAP	Extensible Authentication Protocol
GGSN	Gateway GPRS Support Node
GTP	GPRS Tunneling Protocol
HLR	Home Location Register
HSS	Home Subscriber Server
NAS	Network Access Server
PAP	Password Authentication Protocol
RADIUS	Remote Authentication Dial In User Service
SIM	Subscriber Identity Module
SNMP	Simple Network Management Protocol
USIM	UMTS SIM
WLAN AN	WLAN Access Network

## 7.2 Definitions

-

## 8 References

### 8.1 3GPP Technical Specifications

[1]	Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)	3GPP TS 29.061	Release 8
[2]	Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking	3GPP TS 22.234	
[3]	Numbering, addressing, and identification.	3GPP TS 23.003	
[4]	3GPP system to Wireless Local Area Network (WLAN) interworking; System description.	3GPP TS 23.234	

Prepared (also subject responsible if other) <b>ECHGCHI</b>		No. <b>58/155 17-AVA 901 16 Uen</b>		
Approved	Checked	Date <b>2017-08-24</b>	Rev <b>PB1</b>	Reference

- [5] 3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 3. 3GPP TS 29.234
- [6] 3G security; Wireless Local Area Network (WLAN) interworking security. 3GPP TS 33.234

## 8.2 Requests for Comments (RFCs)

- [7] Microsoft Vendor-specific RADIUS Attributes RFC 2548
- [8] Remote Authentication Dial In User Service RFC 2865
- [9] RADIUS Accounting RFC 2866
- [10] RADIUS Accounting Modifications for Tunnel Protocols RFC 2867
- [11] RADIUS Attributes for Tunnel Protocol Support RFC 2868
- [12] RADIUS Extensions RFC 2869
- [13] RADIUS and IPv6 RFC 3162
- [14] Dynamic Authorization Extensions to Remote Authentication RFC 5176
- [15] Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM)Subscriber Identity Modules (EAP-SIM) RFC 4186
- [16] Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) RFC4187

## 8.3 IPWorks Documents

- [17] IWD for IPWorks AAA Server and AAA Client 22/155 19-CSH 109 085
- [18] IPWorks State of Compliance Overview 1/174 02-FGC 101 3188
- [19] AAA Command Line Specification 1/190 74-CSH 109 085
- [20] IPWorks PM IWD with OSS 1/155 19-AVA 901 16
- [21] IPWorks Alarm List 2/006 51-AVA 901 33/2

Prepared (also subject responsible if other) ECHGCHI		No. 58/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-08-24	Rev PB1	Reference

- [22] IPWorks AAA Front End Function Overview 61/155 17-AVA 901 16
- [23] IPWorks EPC AAA Function Overview 57/155 17-AVA 901 16
- [24] IPWorks Generic AAA Function Overview 59/155 17-AVA 901 16
- [25] IPWorks Wi-Fi AAA Function Overview 61/155 17-AVA 901 16
- [26] IPWorks 3GPP AAA Server-Non-3GPP  
Access GW STa Interface 35/155 19-AVA 901 16
- [27] IPWorks 3GPP AAA Server-ePDG SWm  
and SWm+ Interface 36/115 19-AVA 901 16
- [28] Radius STaPlus Interface between IPWorks  
AAA Server and Non-3GPP Access GW 40/155 19-AVA 901 16