

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

IPWorks Wi-Fi AAA Function Overview

Contents

1	Introduction.....	4
1.1	Document History	4
1.2	Purpose	4
1.3	Scope	4
1.4	Document Structure.....	4
2	Survey of Included Function	4
2.1	Overview.....	4
2.1.1	Architecture	4
2.1.2	Supported Functions	5
2.2	Actors	6
2.2.1	Actor: RADIUS Client	6
2.3	Sub-Functions	6
2.3.1	Generic Radius AAA functions	6
2.3.2	Authentication.....	6
2.3.3	Authorization.....	6
2.3.4	Accounting.....	7
2.3.5	Proxy	7
3	Detailed Description.....	7
3.1	Wi-Fi AAA Use Case Scenario	7
3.1.1	Wi-Fi AAA in 3GPP Network	7
3.1.2	Wi-Fi AAA in ENIW Solution.....	8
3.1.3	HSS Integration	13
3.2	Authentication.....	18
3.2.1	EAP Scenarios	18
3.2.2	EAP Authentication Selection.....	22
3.2.3	EAP Authentication (SIM-based).....	23
3.2.4	Web-based Authentication	30
3.3	Authorization.....	30
3.3.1	ODB Based Wi-Fi Subscription	31
3.3.2	APN Based Wi-Fi Subscription.....	31
3.4	Accounting.....	34
4	Operational Conditions.....	34
4.1	Configurable Parameters.....	34
4.2	Commands and User Procedures	34
4.3	Charging	35
4.4	Characteristics	35
5	Statement of Compliance	35
6	Terminology	35

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

6.1	Abbreviations	35
6.2	Definitions	35
7	References	36

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

1 Introduction

1.1 Document History

Rev	Date	Sign.	Comment
PA1	2017-04-10	ECHGCHI	First Draft, based on 7/155 17-AVA 901 16 Uen L
PB4	2017-06-09	ECIAMAO	Update the section 2.3.4 and 3.4. Move the content from this document to "IPWorks Generic AAA Function Overview".
B	2017-06-19	EJIAHLU	<ul style="list-style-type: none">- Remove all the conentes about EAP-TLS, -TTLS, PEAP, LEAP, MSCHAP);- Re-structure the section 3.3.

1.2 Purpose

The purpose of this document is to describe main functions and internal implementation of Wi-Fi AAA server.

1.3 Scope

This document mainly focuses on the authentication, authorization and accounting functions for Wi-Fi Solution based on the RADIUS protocol.

- 3GPP or RFC specifications implemented will be described, while more detail description will refer to the SoC or IWD, see section 5 and section 7.
- Describe the main architecture and implement consideration of Wi-Fi AAA server.
- Describe the main function and configuration implemented by Wi-Fi AAA server.

1.4 Document Structure

-

2 Survey of Included Function

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

2.1 Overview

IPWorks Wi-Fi AAA server is the protocol server belonging to IPWorks product suite. It does the work of authentication, authorization and accounting for the user accessing WLAN network through Access Point.

2.1.1 Architecture

IPWorks Wi-Fi AAA server is built under the framework of IPWorks Radius AAA and use the common O&M function of IPWorks to do the work of operation and maintenance. Beside the general Radius AAA function, the Wi-Fi AAA Server provide some new functionality, include some new EAP authentications, Accounting message

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

forward and mediation. Figure Figure 1 describes the function architecture of Wi-Fi AAA server in IPWorks environment.

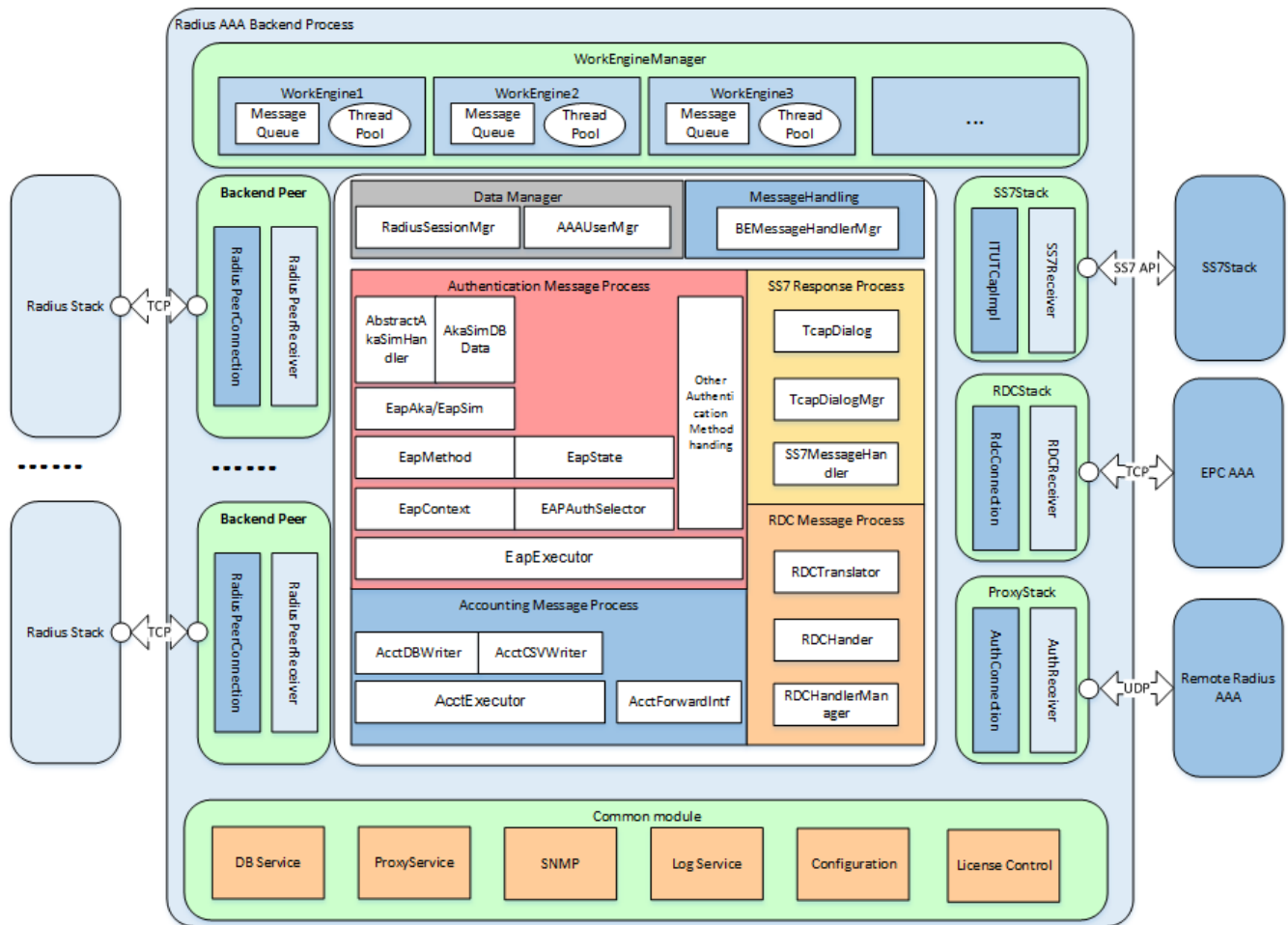


Figure 1 IPWorks Wi-Fi AAA Architecture

2.1.2 Supported Functions

The following figure shows the functions that are supported in the IPWorks Wi-Fi AAA server. A detailed description is presented in the following sections.

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

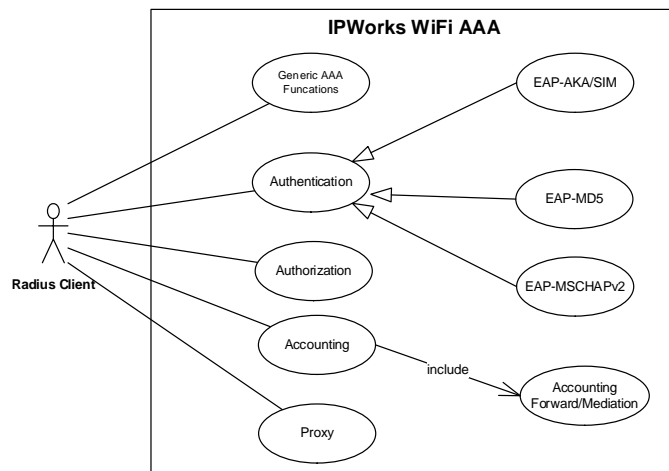


Figure 2 Wi-Fi AAA Server Supported Functions

2.2 Actors

This section describes the actors involved in the AAA server.

2.2.1 Actor: RADIUS Client

The Radius client is responsible for passing user information to designated RADIUS servers, and then acting on the response which is returned.

2.3 Sub-Functions

This section describes the sub-functions of the Wi-Fi AAA server.

2.3.1 Generic Radius AAA functions

Wi-Fi AAA function is based on the Radius AAA Server. That means it could support most of the general IPWorks Radius AAA functions, including authorization, accounting, IP assignment, proxy, Change-of-Authorization and session disconnect, refer to *AAA Function Overview* [1].

2.3.2 Authentication

Authentication provides some mechanisms to check whether the user identity of an entity can match the credential which may be saved in local database or other remote node. Besides the legacy PAP and CHAP authentications, Wi-Fi AAA server implement some new EAP authentications like, SIM-based authentications (EAP-AKA, EAP-SIM).

2.3.3 Authorization

Authorization mechanism is to determine whether a requesting entity is allowed to access a resource and give back some information in the Access-Accept message.

During SIM-based (EAP-AKA/SIM) authentication procedure, IPWorks Wi-Fi AAA server support to query the subscriber information from HLR for authorization. For other authentication methods, Wi-Fi AAA Server support use the legacy authorization based on the preconfigured local policy.

Prepared (also subject responsible if other)		No.	
ECHGCHI		60/155 17-AVA 901 16 Uen	
Approved	Checked	Date	Rev
		2017-04-10	PA1
		Reference	

2.3.4 Accounting

AAA server introduces the accounting message forward/mediation mechanism as enhancement of the legacy accounting facility. For more information, see section [the section Accounting in IPWorks Generic AAA Function Overview](#) [6].

2.3.5 Proxy

IPWorks Wi-Fi AAA supports the Realm based Proxy functionality for all the EAP authentication methods listed below.

- EAP-AKA/SIM

3 Detailed Description

3.1 Wi-Fi AAA Use Case Scenario

3.1.1 Wi-Fi AAA in 3GPP Network

IPWorks Wi-Fi AAA can be used as 3GPP AAA server, which is located within the 3GPP network, to provide SIM/USIM -based Authentication (EAP-AKA/SIM) and Authorization, Accounting (AAA) services to the 3GPP-WLAN Interworking System based on subscription. There are two scenarios be supported between 3GPP systems and Wireless Local Area Networks (WLANs), as Figure shows.

- Unified authentication scenario (WLAN Direct IP Access) : in this scenario WLAN UE access with WLAN AN, AAA is responsible for user authentication and authorization, if successful, UE can directly access IP network with WLAN AN;
- PS domain access scenario (WLAN 3GPP IP Access): in this scenario Tunnel is setup between WLAN UE and PDG with WLAN AN, to allow UE to use PS service.

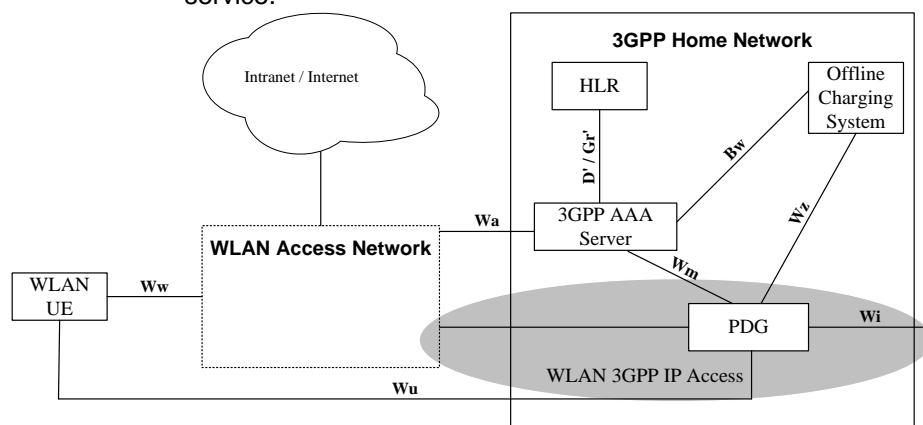


Figure 3 Wi-Fi AAA in 3GPP Network

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

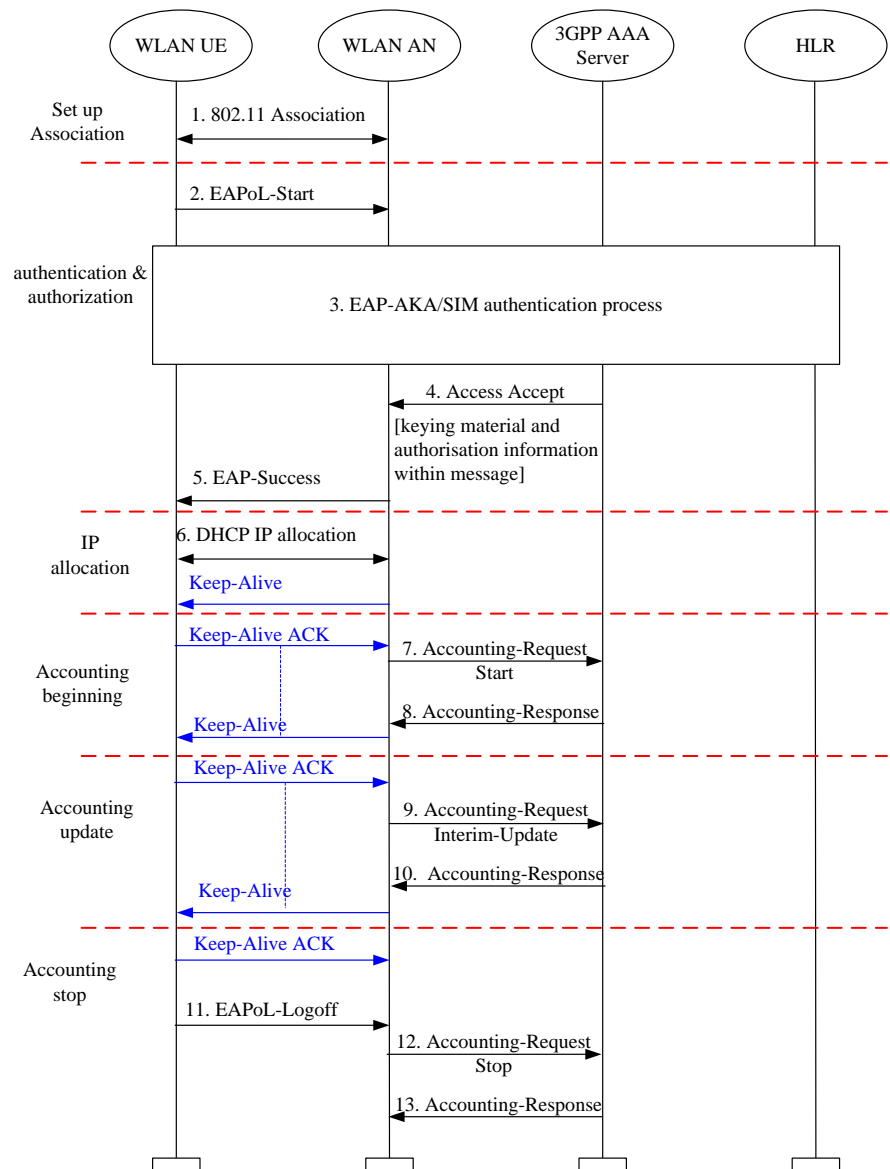


Figure 4 Wi-Fi AAA Working Flow in 3GPP Network

3.1.2 Wi-Fi AAA in ENIW Solution

In ENIW solution, the IPWorks AAA server may connect to different network elements, for example, HLR, BNG/BRAS and SAPC, to provide some EAP authentications, CLIPs handling and accounting message forwarding. The network architecture is described in Figure 5Figure :

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

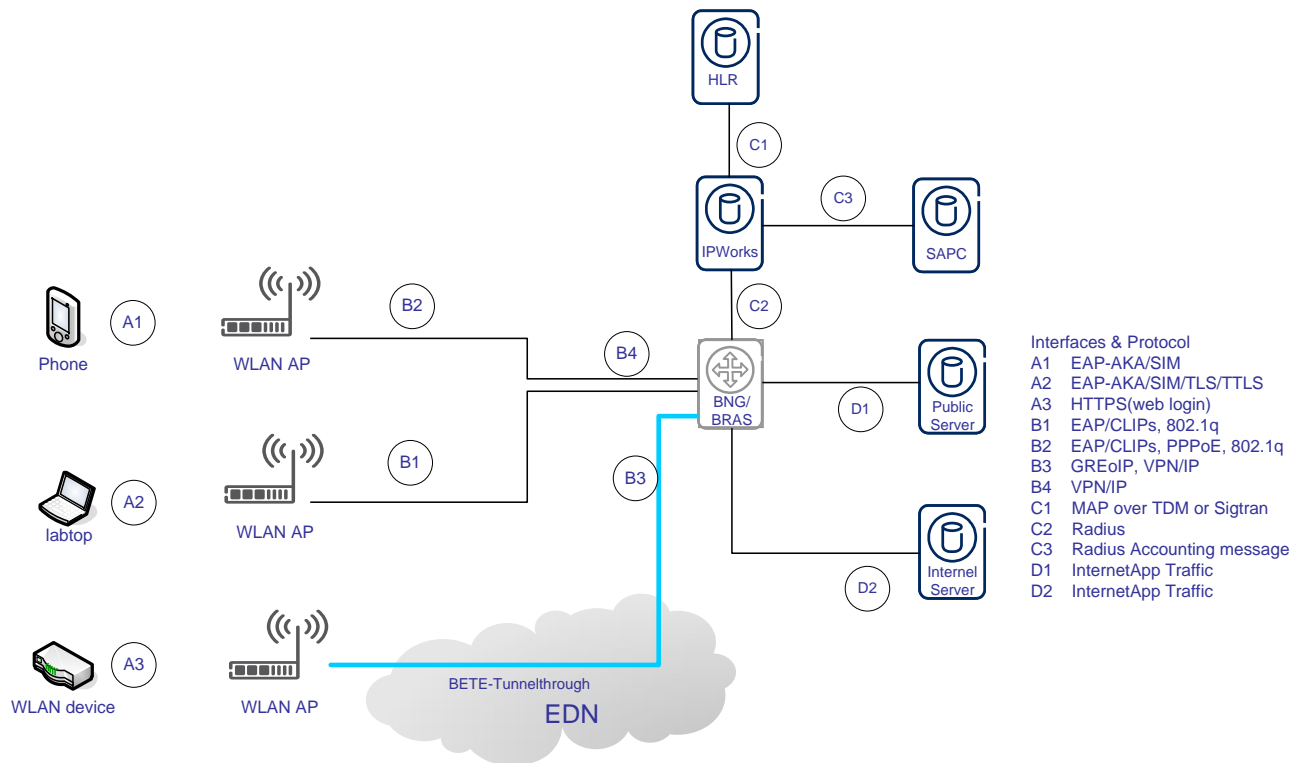


Figure 5 IPWorks AAA in ENIW Solution

Before a device is granted access to the internet or operator service network, the device typically needs to authenticate itself to the network. The following steps give a brief description of messages exchanged between IPWorks AAA and other nodes:

- 1 The devices connect to the access point over the Wi-Fi radio interface using the 802.1x mechanism.
- 2 The access point is acting as authenticator and in this role as a RADIUS client, packaging the EAP information received on the Wi-Fi radio interface through 802.1x into the RADIUS authentication framework.
- 3 During the authentication, the BNG is inside transport path of the RADIUS messages. It will route the traffic from the access points to IPWorks acting as RADIUS proxy and vice versa.
- 4 In case of the SIM-based (EAP-AKA/SIM) authentication, if authentication success, IPWorks will cache some subscriber information which get from HLR in local database.

The following figure gives a brief overview of the possible working flow of Wi-Fi AAA:

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

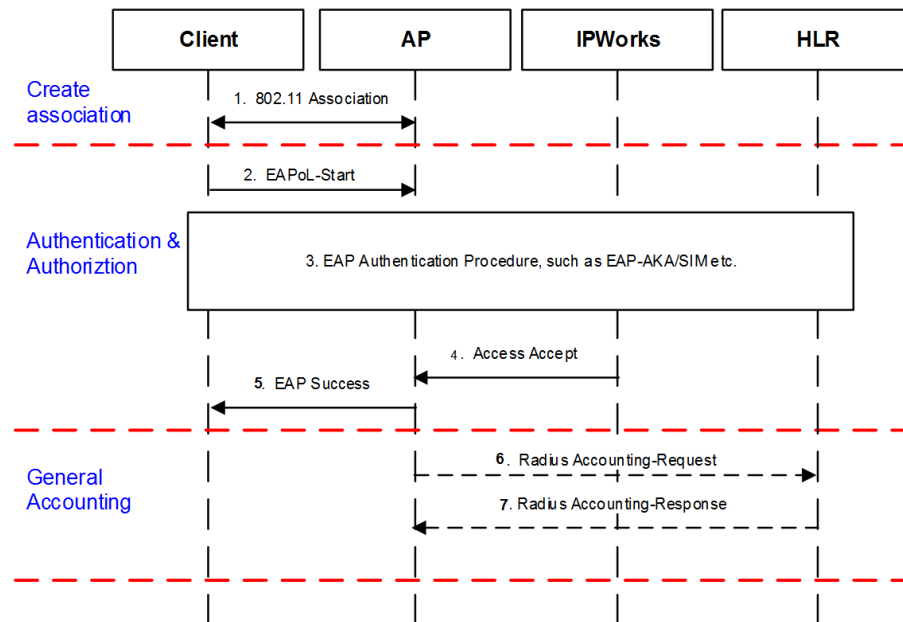


Figure 6 Wi-Fi AAA Working Flow in ENIW Solution

3.1.2.1 Trusted Wi-Fi Support

ENIW solution integrates trusted WLAN access with EPC by setting up S2a GTP tunnel between the Wi-Fi GW and PDN GW.

Using this functionality, operators can seamlessly connect trusted WLAN access network to 3GPP packet core network, optimize capital expenditures by reusing core network capabilities. Subscribers can connect to an operator's WLAN access network, and enjoy services available through the packet core network.

Besides, operators may not want the S2a GTP tunnel setup between Wi-Fi GW and PDN GW for certain subscribers. In this case, on successfully authentication the Wi-Fi GW should route the payload to the BNG for services network/Internet access, without routing through the EPC network.

Triggering Wi-Fi GW to setup a S2a GTP tunnel or not is now supported by IPWorks AAA. IPWorks AAA can authorize subscriber to use S2a GTP tunnel or NSWOW based on APN. If authorization successfully, IPWorks will send different offload indicator to Wi-Fi GW for different types of Wi-Fi service scenarios. For authorization details, see section **Error! Reference source not found.**

When a subscriber is authorized to access to EPC through S2a GTP tunnel, IPWorks will send additional AVPs User-Name, Chargeable-User-Identity, GTP-Tunnel-Data and Offload-Indication to Wi-Fi GW. The value of Offload-Indication is 1 which indicates Wi-Fi GW to setup a S2a GTP tunnel towards PDN GW. Figure 7Figure shows the message flow for the trusted S2a scenario.

When a subscriber is authorized to use NSWOW, IPWorks will send additional AVPs User-Name, Chargeable-User-Identity and Offload-Indication to Wi-Fi GW. The value of Offload-Indication is 0 which indicates Wi-Fi GW not to setup an S2a GTP tunnel towards PDN GW. Figure 8Figure shows the message flow for NSWOW scenario.

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

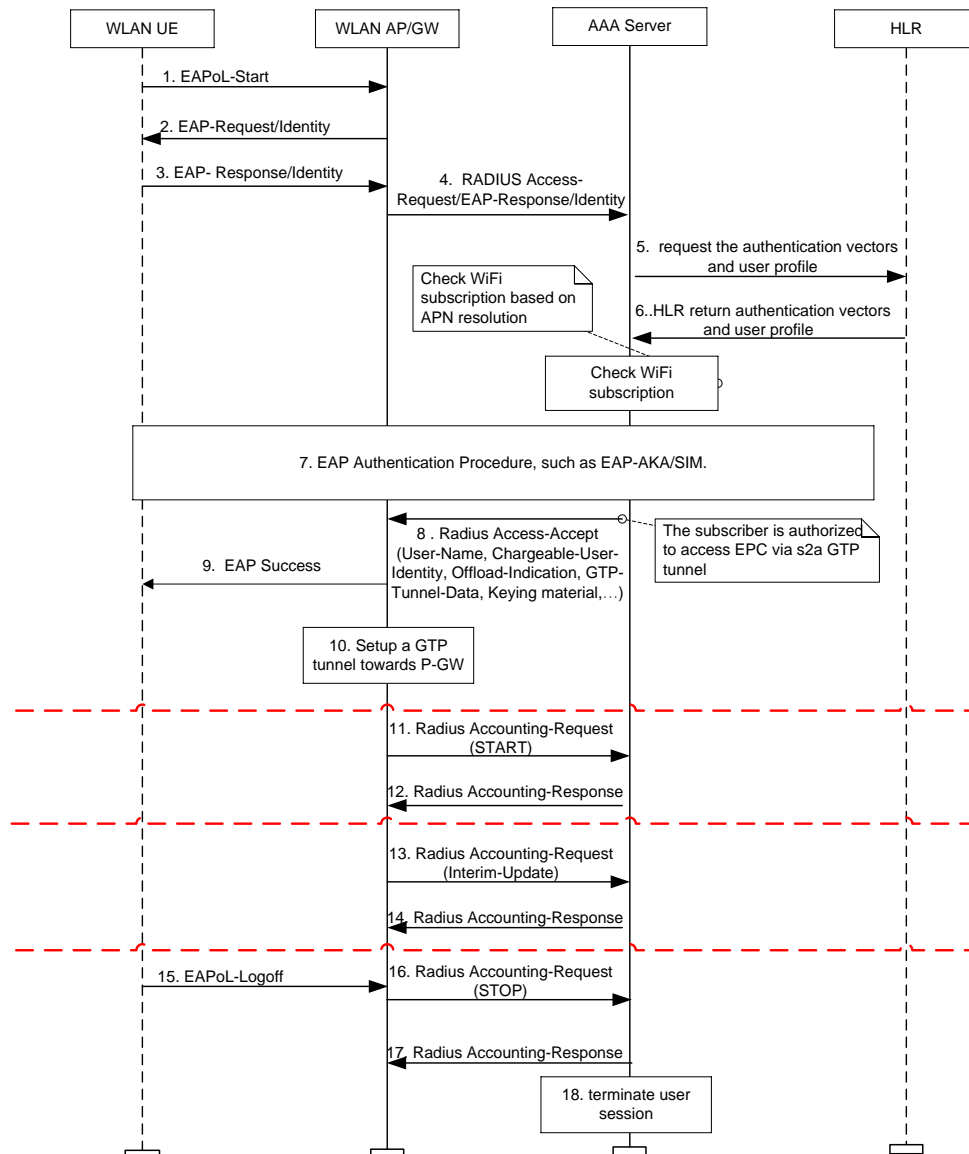


Figure 7 Message Flow for Trusted S2a Scenario

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen	
Approved	Checked	Date 2017-04-10	Rev PA1
		Reference	

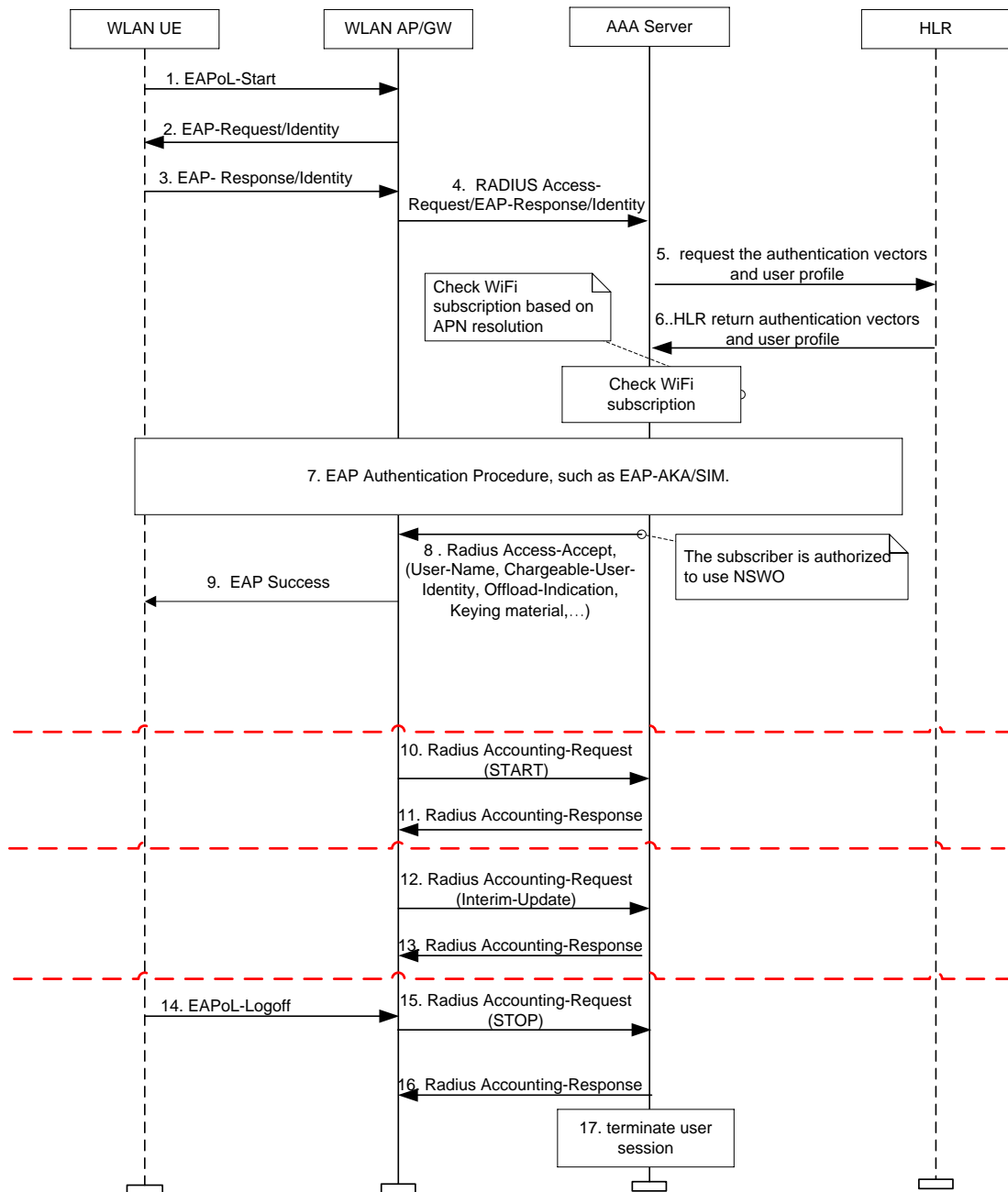


Figure 8 Message Flow for NSW0 Scenario

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

3.1.3 HSS Integration

The solution of HSS integration supports the retrieval of the user authentication vectors and profiles from HSS (in case of the LTE/4G user), without changing the existing capability of WiFi Access Network (i.e. using Radius as the protocol for EAP authentication).

For EAP-SIM authentication (2G/3G user), only HLR is selected for retrieving user authentication vector and profile.

For EAP-AKA' authentication (4G user), only HSS is selected for retrieving user authentication vector and profile.

For EAP-AKA authentication (3G/4G user), IPWorks AAA communicates with HSS via SWx Diameter interface, if no subscription in HSS, IPWorks performs a fallback to HLR for retrieval of user authentication vector and 3G user profile data.

S6b procedure triggered by PDN GW is supported by AAA for EAP-AKA based authenticated users for trusted WiFi support in HSS.

3.1.3.1 HLR only Mode

When a subscriber is authorized to access EPC via S2a GTP tunnel, IPWorks sends additional AVPs User-Name, Chargeable-User-Identity, GTP-Tunnel-Data and Offload-Indication to WiFi GW. The value of Offload-Indication is 1 which indicates WiFi GW to set up an S2a GTP tunnel towards PDN GW. Figure 16 shows the message flow for the trusted S2a scenario.

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

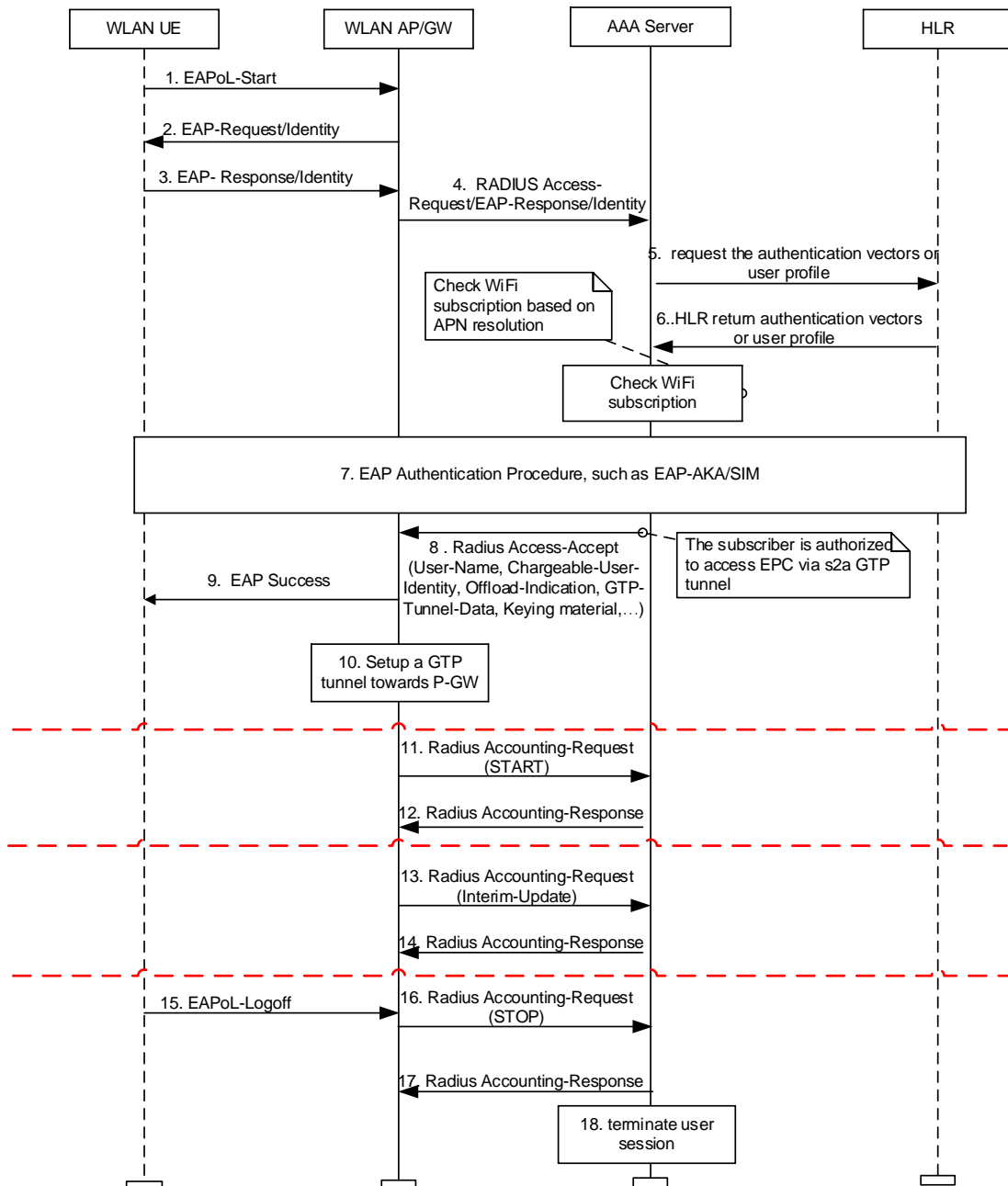


Figure 16 Message Flow for Trusted S2a Scenario

When a subscriber is authorized to use NSWO, IPWorks sends additional AVPs User-Name, Chargeable-User-Identity and Offload-Indication to WiFi GW. The value of Offload-Indication is 0, which indicates WiFi GW not to set up an S2a GTP tunnel towards PDN GW. Figure 17 shows the message flow for NSWO scenario.

Prepared (also subject responsible if other)

No.

ECHGCHI

60/155 17-AVA 901 16 Uen

Approved

Checked

Date

Rev

Reference

2017-04-10

PA1

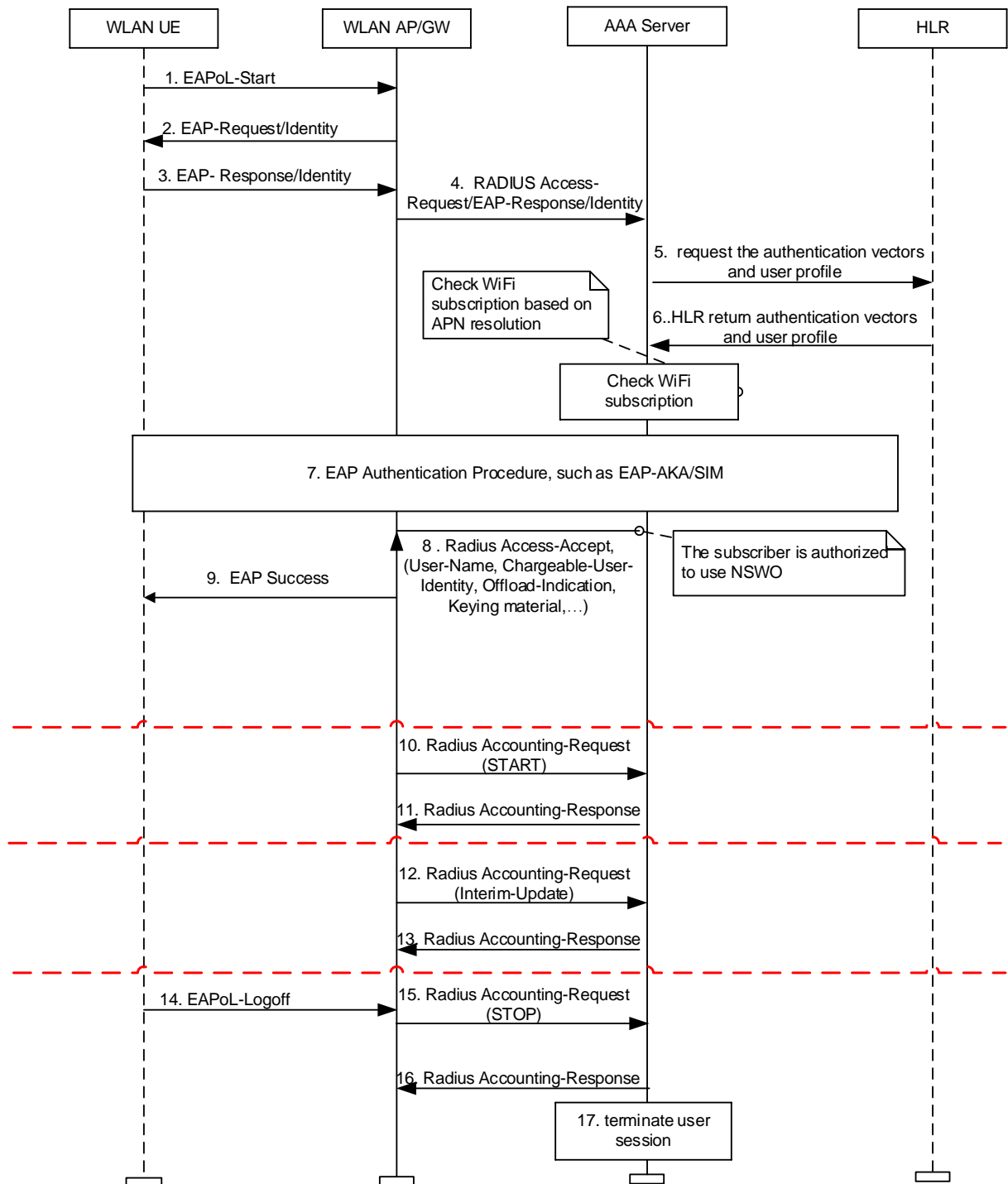


Figure 17 Message Flow for NSWO Scenario

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

3.1.3.2 HSS only Mode

In some scenarios (for LTE subscriber access), IPWorks AAA needs to get the authentication vectors and subscriber profile from HSS and the following s6b procedure is also needed. Here, the working procedure is similar with the typical Diameter Trusted WiFi access EPC network, so IPWorks AAA will mediate the incoming EAP-AKA/AKA' procedure to IPWorks EPC AAA module for handling through an internal interface, as shown in the following figure.

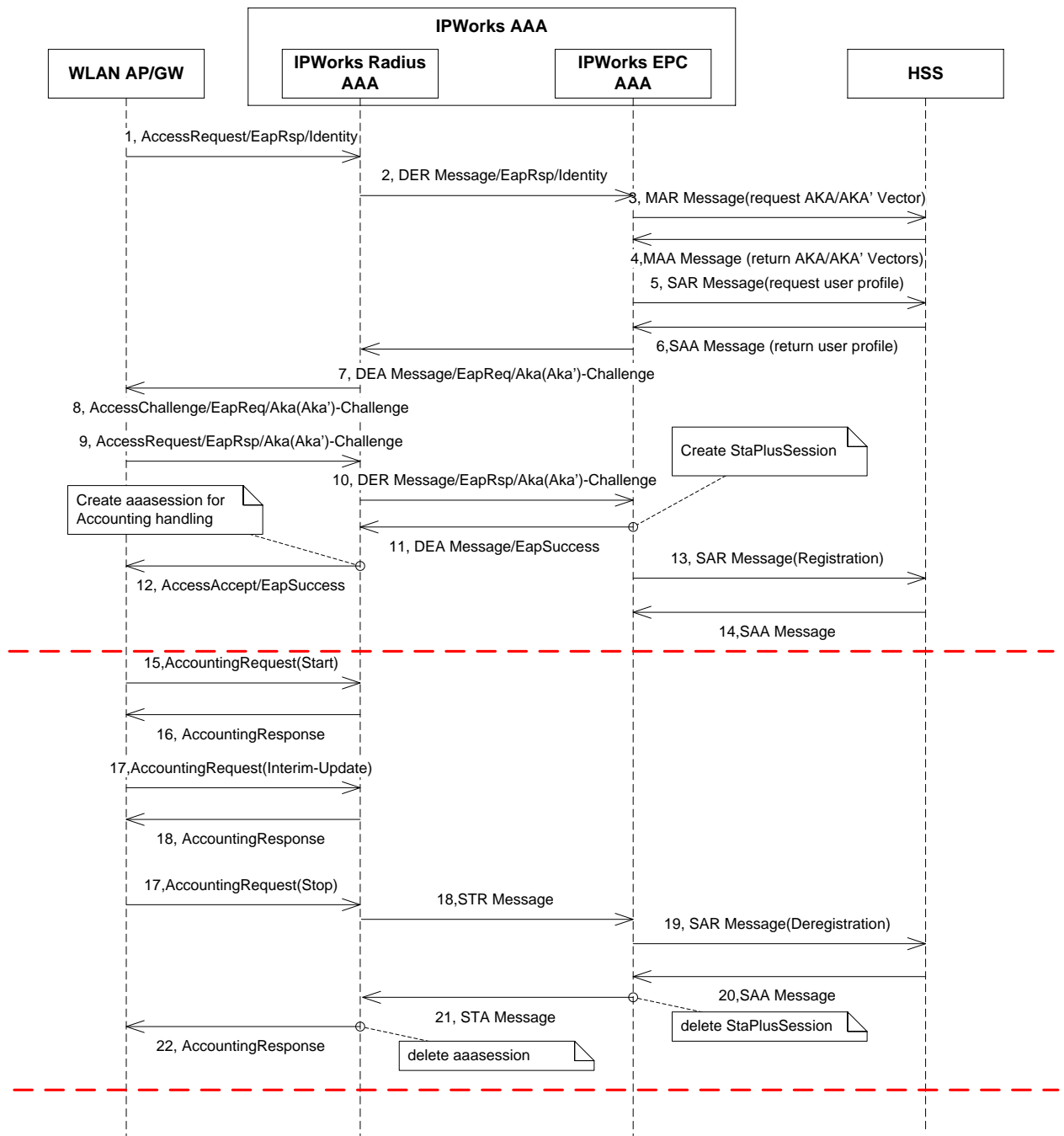


Figure 18 Message Flow for HSS only mode message procedure

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

Note: In general Diameter conveyed authentication, if the HSS indicates that the user is currently being served by a different AAA Server in the authentication procedure, the AAA Server shall respond with the Result-Code set to DIAMETER_REDIRECT_INDICATION and Redirect-Host set to the Diameter identity of the AAA Server currently serving the user. Since Radius Protocol cannot convey the redirect information, such redirection scenario cannot be supported here.

3.1.3.3 HSS Preferred

Consider the AAA cannot distinguish the LTE and non-LTE subscriber from the authentication message directly; IPWorks Radius WiFi AAA can work in HSS preferred mode. In this mode, IPWorks will mediate the EAP-AKA authentication request through the internal Diameter interface to EPC AAA module for handling firstly.

If HSS finds the subscriber information, it shall return the authentication vectors and subscriber profile. Then IPWorks AAA will process the authentication request as same as described in **Section HSS only Mode**. Otherwise, IPWorks EPC AAA module may receive “Diameter_Error_User_Unknown” error from HSS, Then IPWorks AAA server will fall back to HLR only mode for this authentication request and try to retrieve the vectors and subscriber profiles from HLR as below figure shows.

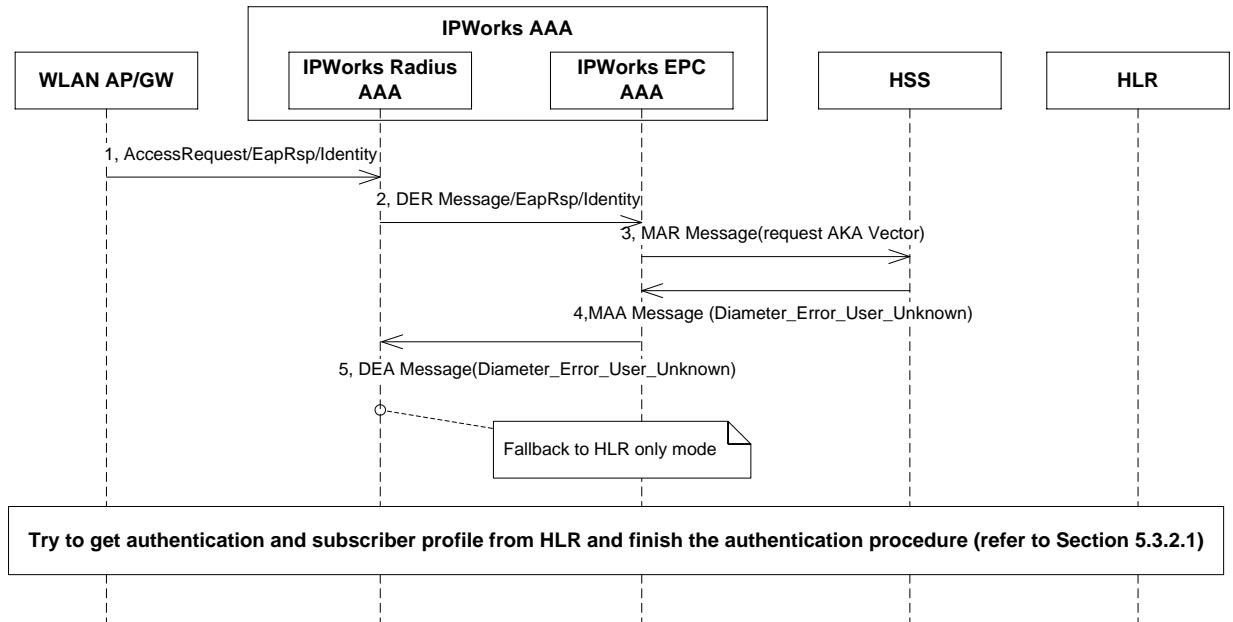


Figure 19 Message Flow for HSS fall back to HLR mode message procedure

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

3.1.3.4 S6b Support

For S2a access scenario in ENIW solution, IPWorks AAA supports PDN-GW initiates the authorization process by sending the Diameter AAR message for HSS only or HSS preferred mode.

In IPWorks AAA, all the S6b messages are handled by IPWorks EPC AAA server. Such handling procedure is based on the results and subscriber profiles which are generated by the preceding authentication procedures.

For HSS only mode, the authentication procedure is finished by EPC AAA server and an aaastaplusession is created in database. The following s6b procedure is handled base on such "aaastaplusession".

For HSS preferred mode, in case of the authentication procedure is finally fall back to HLR mode, EPC AAA tries to find the related active "aaasession" according the IMSI value and return the success Diameter AAA message.

For the detailed S6b procedure, refer to **section PDN GW Initiated Session Termination Procedure** and **section HSS Initiated Update of User Profile** in **IPWorks EPC AAA Function Overview**, Reference [18].

3.2 Authentication

IPWorks Wi-Fi AAA server use Radius protocol to convey the EAP authentications, this section will describe the EAP authentication implemented by Wi-Fi AAA server. Currently, all the EAP authentications are implemented in a plugin process named "a3backend". Figure 20 shows the protocol structure which be supported by IPWorks Wi-Fi AAA server.

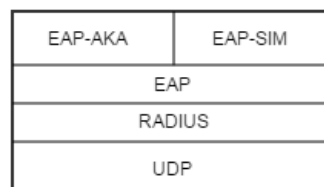


Figure 20 Wi-Fi AAA Protocol Structure

3.2.1 EAP Scenarios

An EAP conversation may use a sequence of EAP methods. A common example of this is an identity request followed by a single EAP authentication method such as an MD5-Challenge. In general, the peer and authenticator use only one authentication method (Type 4 or greater) within an EAP conversation, after which the authenticator must send a Success or Failure packet.

To meet such requirement, IPWorks handles different EAP methods in a unified mode. A complete EAP method conversation shows below.

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

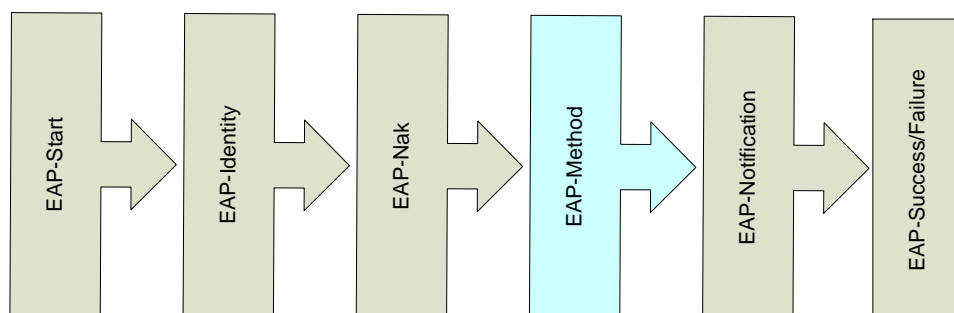


Figure 21 EAP Types Sequence

Before handling an actual EAP authentication method (Type 4 or greater), IPWorks AAA could handle different common EAP type sequences which may be assembled with EAP-Start, EAP-Identity and EAP-NAK according to different EAP initial packet.

If handling the actual EAP authentication method failed, IPWorks support to sending EAP-Notification before sending EAP-Failure according to each different EAP authentication method configuration, if this actual EAP authentication allow.

Below sections illustrate some possible conversation scenarios between an authenticating peer, NAS, and IPWorks server, based on RFC3579 Appendix A shows.

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

3.2.1.1 Normal EAP Authentication Flow

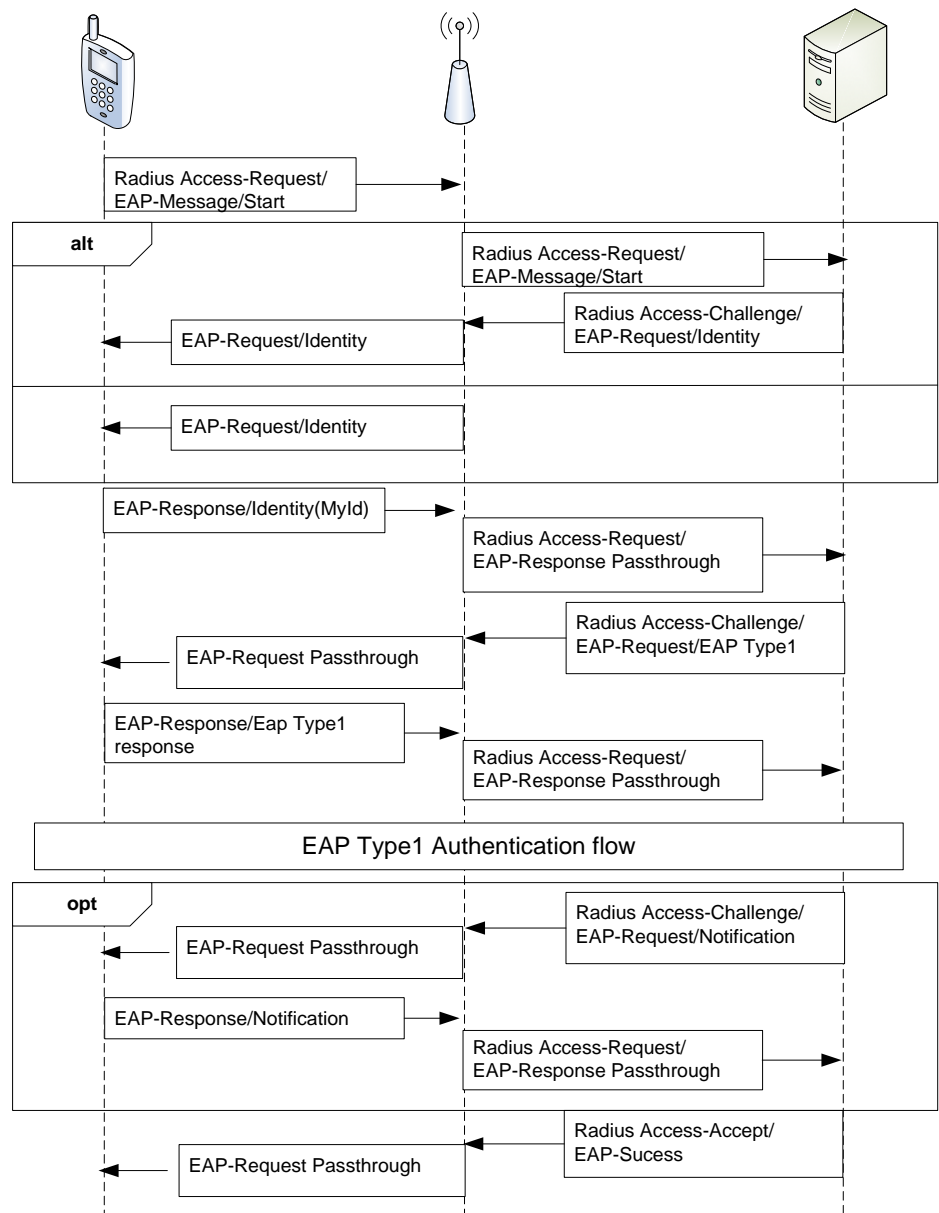


Figure 22 Normal EAP Authentication Flow

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

3.2.1.2 Peer Refuse Proposed EAP Method with NAK

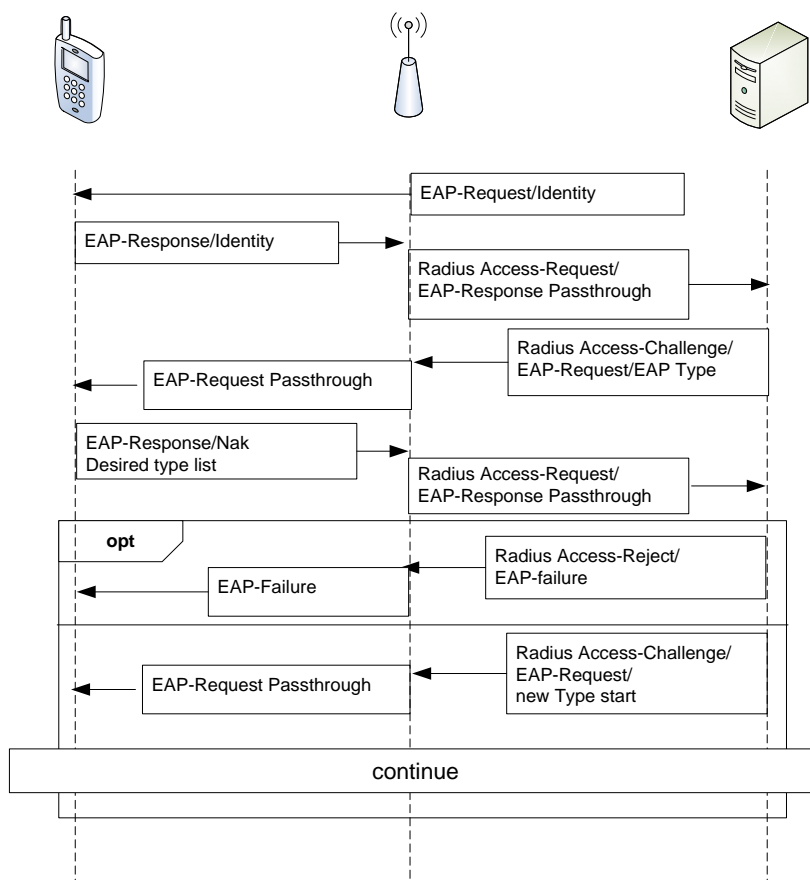


Figure 23 Peer Refuse EAP Method Proposed by AAA Server

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

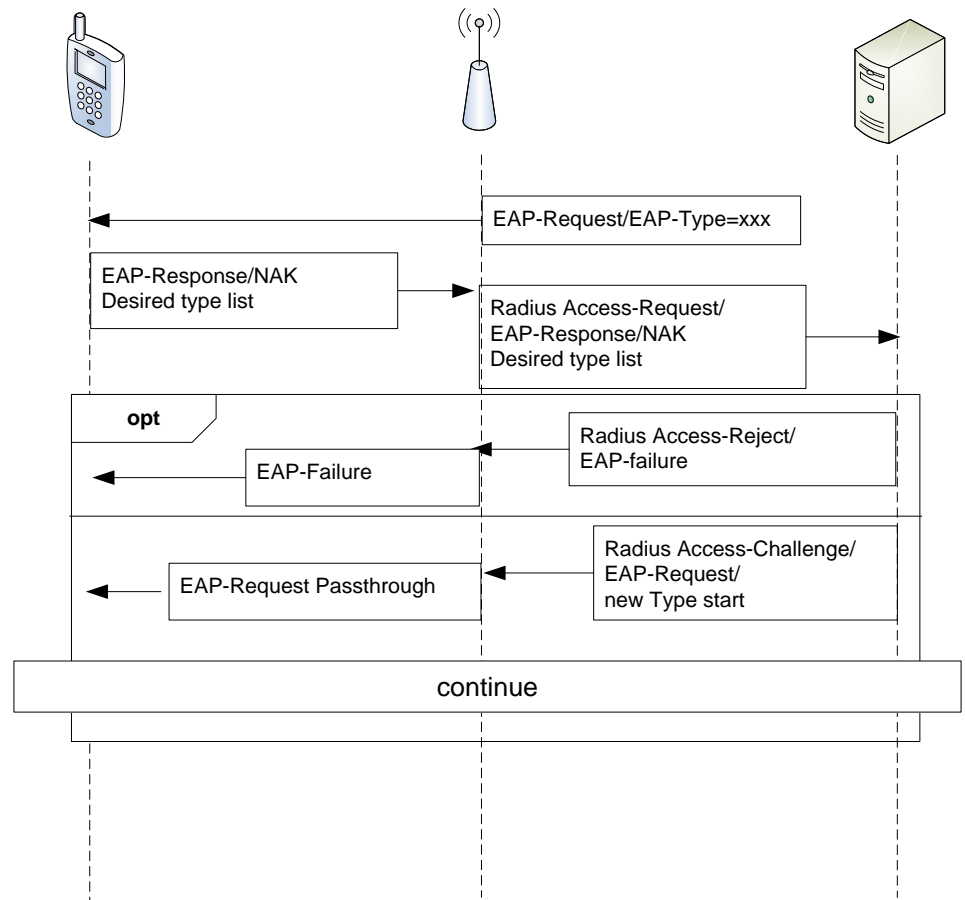


Figure 9 Peer Refuse EAP Method Proposed by NAS

3.2.2 EAP Authentication Selection

If NAS send EAP Start or EAP-Response/Identity as initial packet to AAA server, IPWorks will use the value of EAP-Response/Identity to select the default EAP authentication.

Operator could configure to use different mode to pick up an EAP method as proposal, such selection mode include:

1 Based on database

IPWorks could use the value of EAP-Response/Identity to select the default EAP authentication according the user profile primarily. Operator can use the CLI to specify the default EAP authentication method for specific user, as below:

```
IPWorks>create aauser -set username=<user name>;password=<AAA
UserPwd>[ ;authmethod=<EAPMD5>]
```

2 Based on identity format

IPWorks could also select the default EAP method according the EAP-Response/Identity value format. Operator can specify the Identity format using regular express. A typical usage example of this mode is EAP-AKA/SIM. As the protocol specified, the authenticator may distinguish the different EAP-AKA/SIM scenario according a digit prefix, like below:

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

"0<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org", for EAP AKA authentication
 "1<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org", for EAP SIM authentication
 "2<PseudonymUsername>@aaa<ID>.wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org", for EAP AKA authentication
 "3<PseudonymUsername>@aaa<ID>.wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org", for EAP SIM authentication
 "4<Re-authenticationUsername>@aaa<ID>.wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org", for EAP AKA authentication
 "5<Re-authenticationUsername>@aaa<ID>.wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org", for EAP SIM authentication

Then the regular express format of selector may as below:

EapAKA=1

identityFormat="^[024].+ "

EapSIM=1

identityFormat="^[135].+ "

3 Identity first

In this mode, AAA server will use the EAP-Response/Identity value to match all defined regular express, if failed; AAA server will then try to search the database as mode 1.

4 Database information first

Opposite with mode 3, AAA server could also search the database firstly. Then check all the regular express.

If neither identity format nor the database user profile can help locate a default EAP method, AAA server will use a predefined default EAP method as proposal.

3.2.3 EAP Authentication (SIM-based)

The SIM-based EAP authentication which be supported by IPWorks Wi-Fi AAA server include EAP-AKA and EAP-SIM. Both the two authentications use MAPv3 signaling procedures to get the authentication vectors and subscriber profile from HLR. Some more detailed information can be found in 3GPP AAA Server-WLAN Access Network Wa Interface Description[2] and 3GPP AAA Server-HLR D'/Gr' Interface Description[3].

3.2.3.1 Data Cache for EAP-AKA/SIM

To improve the performance and support fast re-authentication, IPWorks will cache the related information in NDB database for the successful authenticated subscribers. Such cached data will be deleted by IPWorks under either two conditions:

- 1 The subscriber is offline for a long time and then the cached data will be expired. The default threshold is 24 hours.
- 2 In Gr' interface, if IPWorks received some notification from HLR in below scenario, the cached data will be deleted.
 - a If the subscriber information is changed, HLR will use insert Subscriber Data to IPWorks and IPWorks will check whether the Wi-Fi subscription changes, refer to *3GPP AAA Server-HLR D'/Gr' Interface Description* [3]. If yes, IPWorks will delete the cached data.

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

- b If the subscriber has been removed from HLR or this subscriber login from other node, HLR will send `cancelLocation` message to IPWorks. Then IPWorks will delete the cache data.
- c If IPWorks received reset message from HLR (happens when HLR has problem or be restarted), all the cached data got from the HLR will be cleaned.

3.2.3.2 EAP-AKA/SIM Authentication Vectors Usage

During SIM-based (EAP-AKA/SIM) authentication, IPWorks will try to get the authentication vectors from the cached data. If there are no enough vectors in cached data, it will request five vectors from HLR by sending `sendAuthenticvationInfo` service in one time.

For EAP-AKA authentication, every authentication will use one vector and the remnant vectors will be saved in the cached data. For EAP-SIM authentication, in each authentication process, two or three GSM RANDs of authentication vectors will be issued during EAP-SIM challenges and after that the first authentication vector shall be discarded. For example, we have five groups of authentication vectors. For the first authentication, use the first and the second vectors, and then discard the first one. For the second authentication, use the second and third vectors. Follow the former step for the later authentication.

3.2.3.3 EAP-AKA/SIM Authentication Vector Translation

When receive the `sendAuthenticvationInfo` request, HLR will give back different type vectors to IPWorks according to the subscriber type. Generally, a 3G user using USIM card will request an EAP-AKA authentication and HLR will give back quintuplet vectors and a 2G user using SIM card will request EAP-SIM authentication and HLR will give back triplet vectors.

In one special case, a 3G user may use a SIM card and request EAP-SIM authentication, but the HLR still sends quintuplets, IPWorks supports to convert those quintuplets into triplets to meet the requirement of EAP-SIM.

3.2.3.4 HD SS7 Stack Support

Wi-Fi AAA Functions support to deploy the EAP-AKA/SIM on a distributed SS7 environment, Horizontal Distribution (HD). In HD mode, the SS7 stack module will be started on several different hosts for redundancy. That means several AAA servers could bind to the same distributed SS7 stack and if the stack process on one host is down, the query traffic could still be sent out through the stack process on other hosts.

Currently, IPWorks AAA server supports to distribute the SS7 stack and AAA server on two hosts. The following figure illustrates the possible deployment.

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen	
Approved	Checked	Date 2017-04-10	Rev PA1
		Reference	

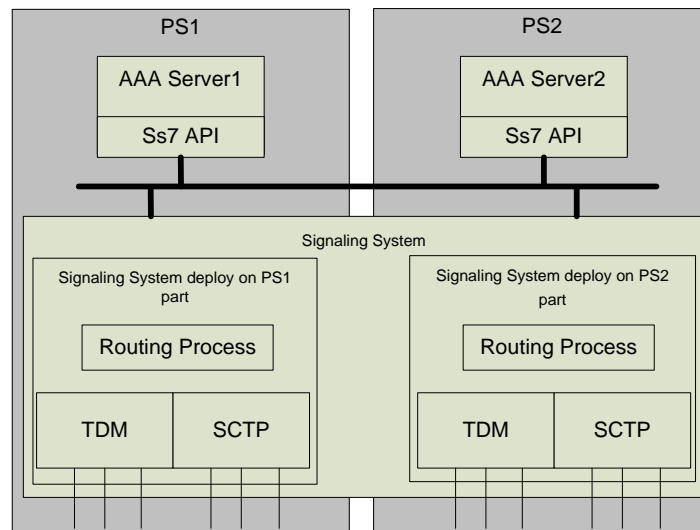


Figure 10 AAA Server Deployed on HD SS7 Stack

Note: Base on HD SS7 stack, IPWorks AAA support handling SIM-based (EAP-AKA/SIM) authentication in double active mode. That means the AAA servers on two hosts (PS1 and PS2) could handle AAA traffic at the same time. And HLR will consider it is communicating with a single AAA server, since both the AAA servers is using one SS7 stack.

Such behavior will also bring us a limitation when HLR send a notification to IPWorks to cancel the access ability of a cached subscriber. When the notification reach the SS7 stack, stack will send it to one AAA server for handling, and if the other AAA server is handling and accept the authentication request for the subscriber at the same time, although HLR has revoked its access ability.

3.2.3.5 Customization Setting for EAP-AKA/SIM

In EAP-AKA/SIM authentication implementation, there are some customization behaviours in the context of ENIW solution.

1 Put subscribers IMSI in Access-Accept.

In EAP-AKA/SIM authentication, the client may choose to use pseudonym identity or fast re-authentication identity for authentication. Generally IPWorks AAA Server will get the User-Name attribute value from Access-Request and put it into Access-Accept message.

But sometimes the NAS may need to identity the authentication user from Access-Accept, IPWorks supports to put the user IMSI into User-Name AVP in "Access-Accept" packet in EAP-AKA/SIM authentication. Since it's not recommended to unnecessarily send un-ciphered subscriber data (IMSI) over air interface, the last trusted radius proxy on the way down to the subscriber should remove this information before sending it to the subscriber.

2 Always return CUI attribute in Access-Accept.

According to section 2.1 in RFC 4372, Chargeable-User-Identity (CUI) should not be replied if it is not contained the Access-Request packet. By default, the AAA server doesn't include the CUI attribute in the Access-Accept packet if the Access-Request packet doesn't contain the CUI. However, in some solutions, the NAS client doesn't send CUI in the Access-Request packet to the AAA server but

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

demands the reply of the CUI in the Access-Accept packet. IPWorks provide a switch configure item for sending CUI attribute anyway.

3 Always return Subscriber Charging Characteristics in Access-Accept

In some solutions, the Subscriber Charging Characteristics information is needed to be extended to network elements in order to differentiate the post-paid and pre-paid subscribers. The "Subscriber Charging Characteristics" is mapped into a Radius Vendor Specific AVP and then be sent to next network element, such as NetOP policy manager.

To support this solution, IPWorks provide a configurable switch for sending Subscriber Charging Characteristics anyway.

3.2.3.6 EAP-SIM Authentication Flow

EAP-SIM is a method for authentication and session key distribution that uses the Global System for Mobile Communications (GSM) Subscriber Identity Module (SIM). The EAP-SIM mechanism specifies enhancements to GSM authentication and key agreement whereby multiple authentication triplets can be combined to create authentication responses and session keys of greater strength than the individual GSM triplets. The mechanism also includes network authentication, user anonymity support, result indications, and a fast re-authentication procedure.

Wi-Fi AAA supports the EAP-SIM and fast re-authentication as Figure 11 and Figure 12 show.

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

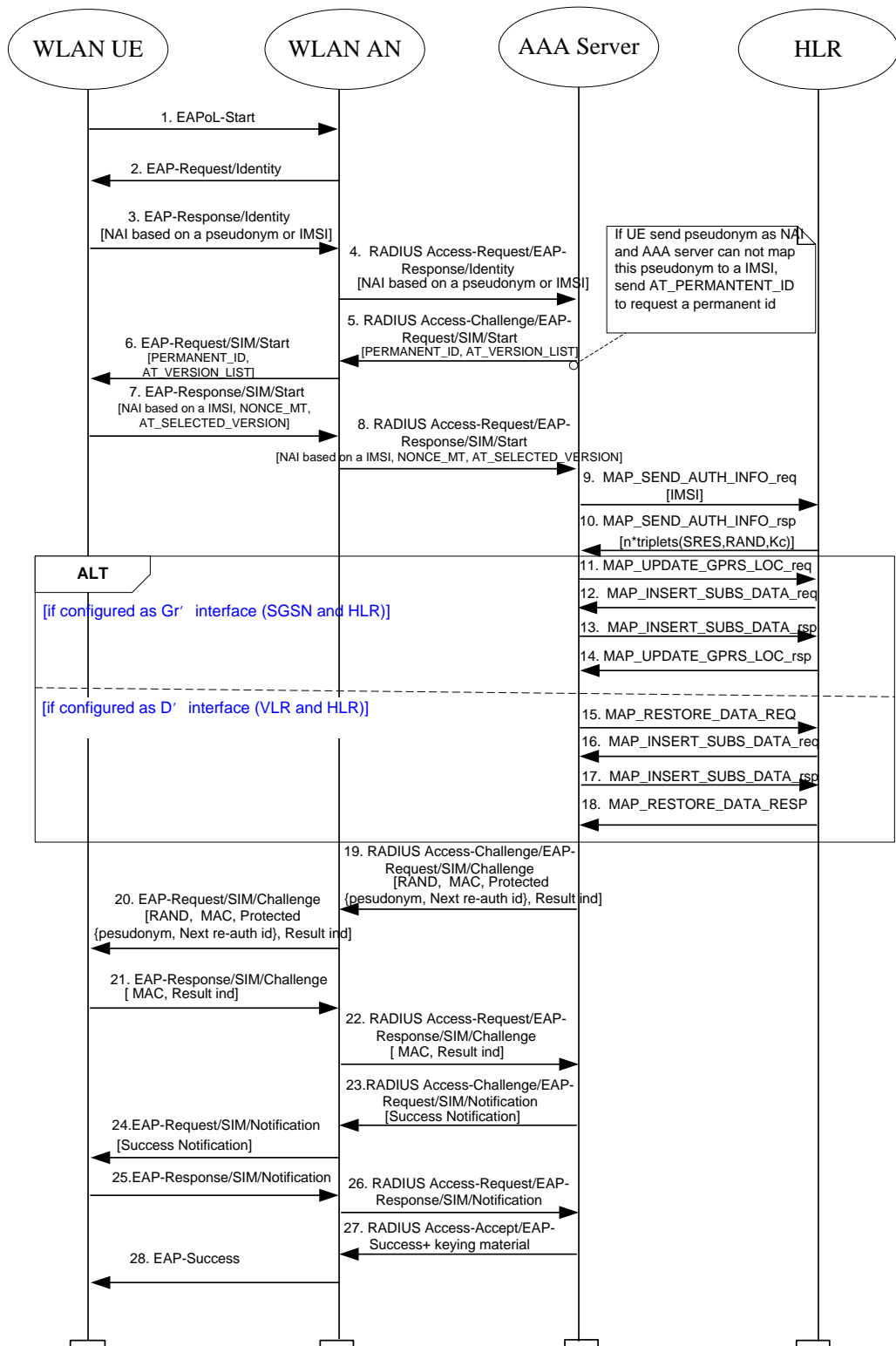


Figure 11 Full Authentication and Authorization

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

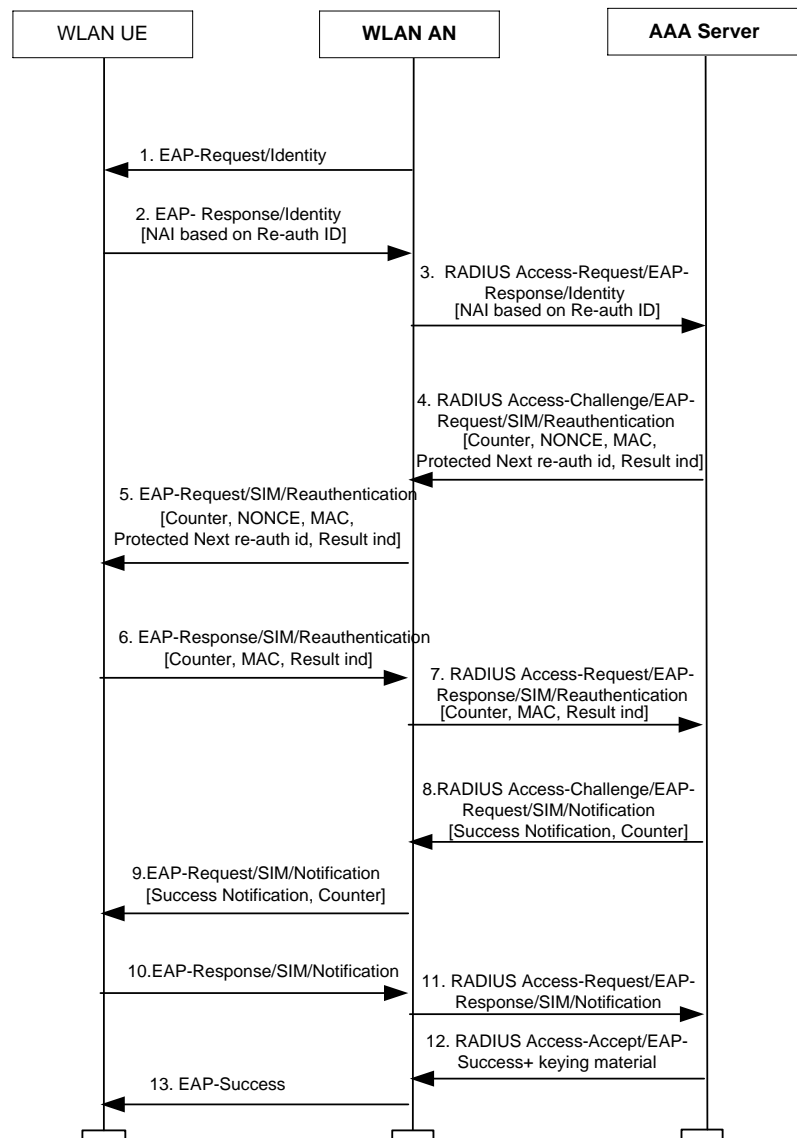


Figure 12 EAP-SIM Fast Re-authentication

3.2.3.7 EAP-AKA Authentication Flow

EAP-AKA is a method for authentication and session key distribution that uses the Authentication and Key Agreement (AKA) mechanism. AKA is used in the 3rd generation mobile networks Universal Mobile. WLAN AAA use the method for authentication when a 3G user try to access WLAN network.

WLAN AAA supports the EAP-AKA full authentication and fast re-authentication as Figure 13 and Figure 14 show.

Prepared (also subject responsible if other)

No.

ECHGCHI

60/155 17-AVA 901 16 Uen

Approved

Checked

Date

Rev

Reference

2017-04-10

PA1

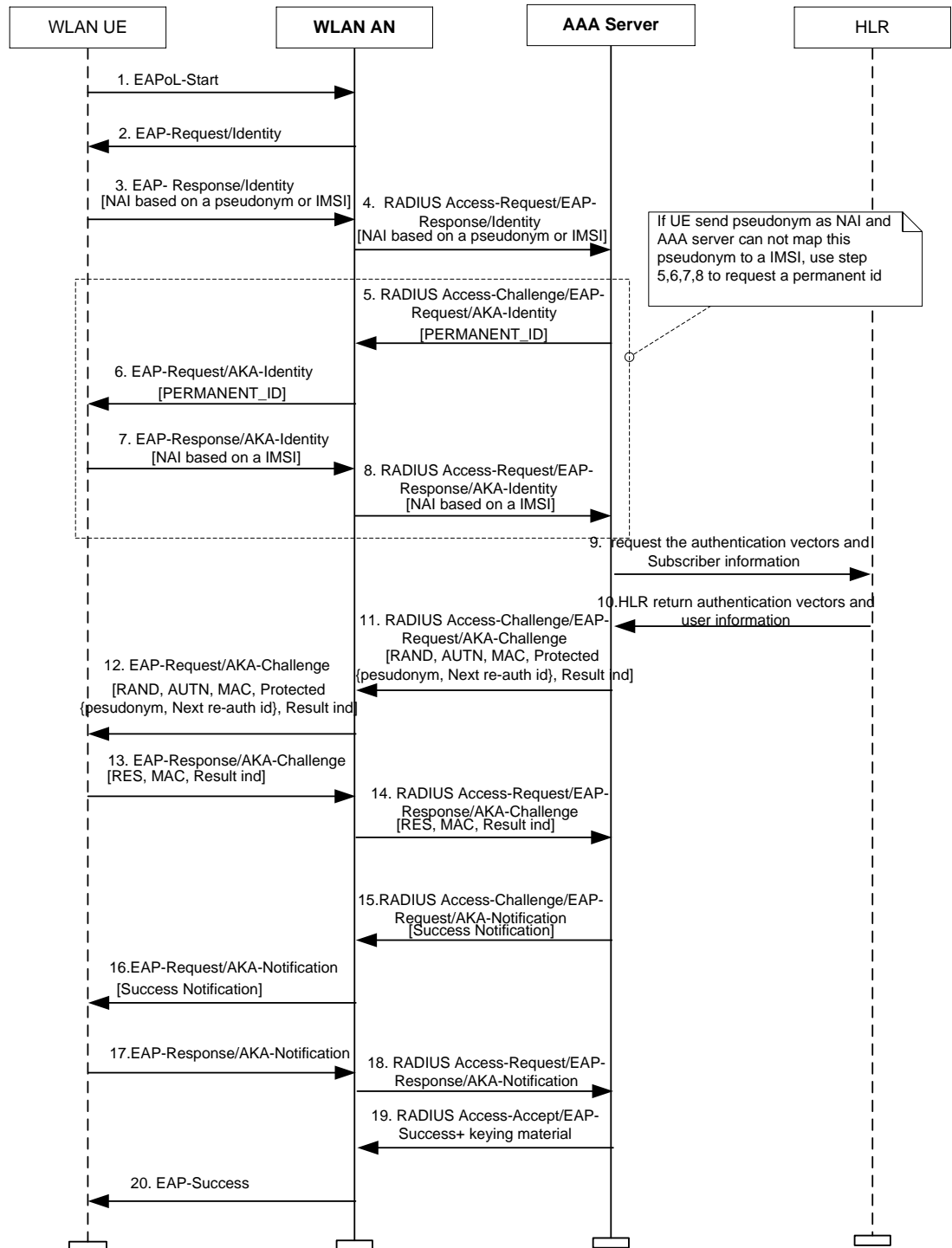


Figure 13 EAP-AKA Full Authentication

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

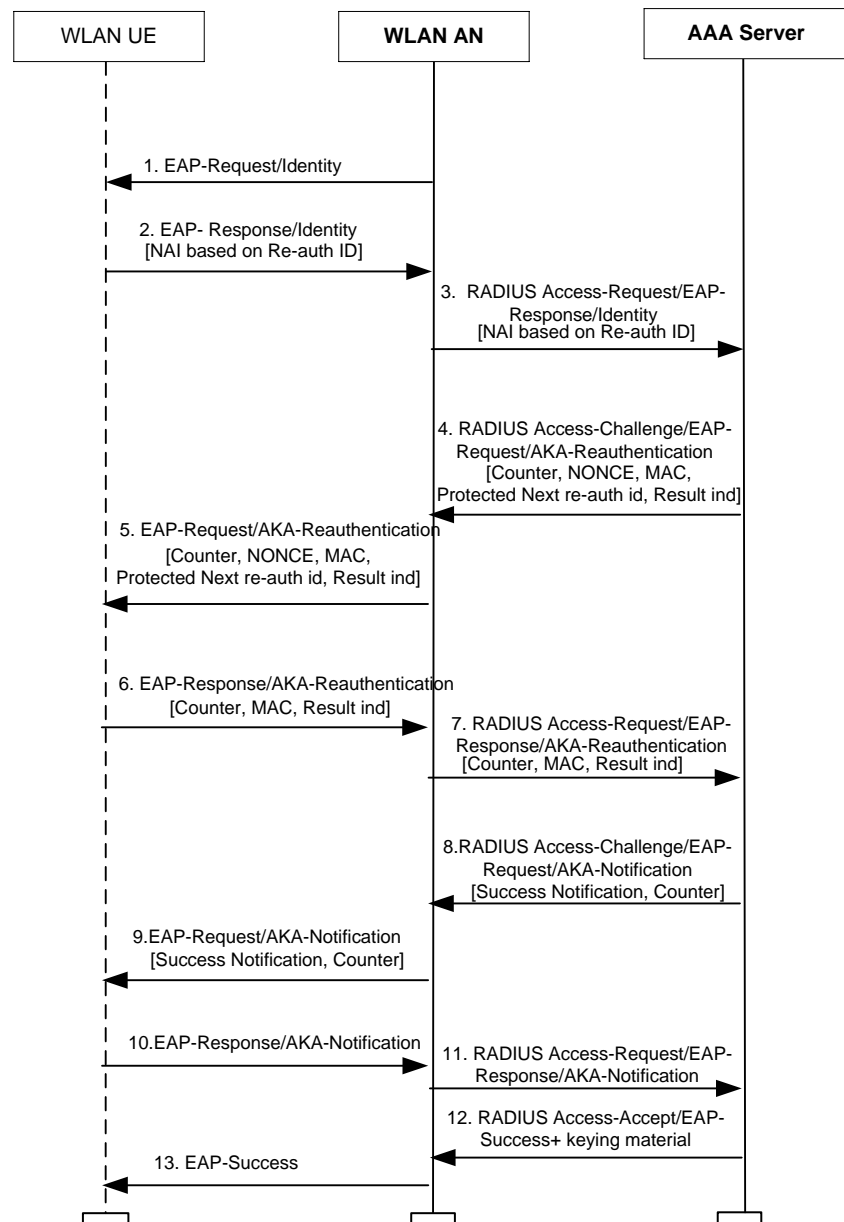


Figure 14 EAP-AKA Fast Re-authenticationEAP Authentication (Non-SIM based)

A pre-condition (of a function) is the state that the system must be in before performing the function.

3.2.4 Web-based Authentication

Web-based authentication uses PAP and CHAP methods, for detailed description on PAP and CHAP, refer to **Section PAP** and **Section CHAP** in **IPWorks Generic AAA Function Overview**, [Reference \[7\]](#).

3.3 Authorization

Since the user profile is stored in HLR for EAP-AKA/SIM user, the authorization procedure is different from the general authorization. During the EAP-AKA/SIM

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

authentication process, IPWorks AAA will send MAP_UPDATE_GPRS_LOCATION or MAP_RESTORE_DATA operation to HLR to get subscriber information. After the HLR received either of those two operations, HLR will send the MAP-INSERT-SUBSCRIBER-DATA operation to AAA server with related information.

IPWorks AAA server decides whether to allow the subscriber to access to WLAN network based on the subscriber data. Now IPWorks AAA supports to authorize subscriber based on either ODB or APN returned from HLR.

3.3.1 ODB Based Wi-Fi Subscription

If the user has a contract for accessing WLAN network, and the Wi-Fi subscription is stored in ODB, HLR will return a flag in Operator Determined Barring HPLMN data.

User can configure any bit flag in odb-HPLMN-Data as WLAN accessible flag as below definition shows:

```
odb-HPLMN-Data    BIT STRING {  
    plmn-SpecificBarringType1 (0 ),  
    plmn-SpecificBarringType2 (1 ),  
    plmn-SpecificBarringType3 (2 ),  
    plmn-SpecificBarringType4 (3 )} ( SIZE( 4 .. 32 ) ) OPTIONAL,
```

If a subscriber is allowed to access WLAN network, the bit value of specified plmn-SpecificBarringType should be set as 1, otherwise 0. On the other hand, if such authorization checks can be ignored also if user configure Wi-Fi AAA to not check any odb-HPLMN-Data flag.

3.3.2 APN Based Wi-Fi Subscription

3.3.2.1 APN with Wi-Fi Subscription Indication

If the user has a contract for accessing to the WLAN network, and the Wi-Fi subscription is stored in APN, the APN must be provisioned in HLR firstly. The APN consists of two parts: one is Wi-Fi subscription indication and the other is APN name string.

For example, if the Wi-Fi subscription indication is "lbo" and the APN name string is "cmnet.mnc000.mcc460.gprs", the provisioned APN in HLR is "lbo.cmnet.mnc000.mcc460.gprs".

If a subscriber is allowed to access to WLAN network, the APN retrieved from HLR includes both the Wi-Fi subscription indication and APN name string, which must match those configured in IPWorks AAA.

- A subscriber can apply NSWO scenario if Wi-Fi subscription indication of the APN matches the NSWO subscription;
- A subscriber can apply S2a scenario if Wi-Fi subscription indication of the APN matches the S2a subscription, and S2a scenario is enabled by IPWorks AAA.

Both the Wi-Fi subscription indication and APN name string also need to be configured in IPWorks AAA server.

Subscriber Information Retrieval

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

By using the Gr' interface, IPWorks AAA sends the request of MAP_UPDATE_GPRS_LOCATION to HLR to retrieve the subscriber information. Then HLR returns a GPRSDataList containing the APN to IPWorks AAA.

GPRSDataList Format

GPRSDataList ::= SEQUENCE SIZE (1.. maxNumOfPDP-Contexts)
OF PDP-Context

```
PDP-Context ::= SEQUENCE {  
    pdp-ContextId ContextId,  
    pdp-Type (16) PDP-Type,  
    pdp-Address (17) PDP-Address OPTIONAL,  
    QoS-Subscribed (18) QoS-Subscribed,  
    vplmnAddressAllowed (19) NULL OPTIONAL,  
    apn (20) APN,  
    ext-QoS-Subscribed (0) Ext-QoS-Subscribed OPTIONAL,  
    PDP-ChargingCharacteristics  
    (1) ChargingCharacteristics OPTIONAL,  
    ext2-QoS-Subscribed (2) Ext2-QoS-Subscribed OPTIONAL,  
    ext3-QoS-Subscribed (3) Ext3-QoS-Subscribed OPTIONAL  
}
```

For example:

The APN name string configured in IPWorks AAA is "cmnet.mnc000.mcc460.gprs" and subscription indication is configured as the following:

Subscription indication in IPWorks AAA	Value of Subscription Indication
S2a subscription indication	"S2a"
NSWO subscription indication	"lbo"
Preferred subscription indication	"S2a"

When an APN is retrieved from HLR, the logic of checking which type of Wi-Fi service scenario is as follows:

Note:

The name string of APN retrieved from HLR must match with that in IPWorks AAA. If not match, subscriber is not allowed to access either type of Wi-Fi service.

- If the Wi-Fi subscription indication of the APN matches the S2a subscription indication configured in IPWorks, such as "s2a", that's a trusted S2a scenario.
IPWorks AAA sends additional AVPs (Chargeable-User-Identity, User-Name, Offload Indication, and GTP-Tunnel-Data) in the Access-Accept message to Wi-Fi GW.
The Value of Chargeable-User-Identity is MSISDN, and the value of User-Name is IMSI.
The Value of Offload-Indication is 1, which indicates Wi-Fi GW to setup an S2a GTP tunnel towards the PDN Gateway.

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

The GTP-Tunnel-Data contains the following information which is used by Wi-Fi GW to setup a GTP-Tunnel to PDN GW.

- PDN Type
 - Restriction Type
 - APN-AMBR
 - Bearer QoS
 - APN Name
 - Charging Characteristics
 - Primary PDN GW IP Address
 - Secondary PDN GW IP Address
- If the Wi-Fi subscription indication of the APN matches the NSWO indication configured in IPWorks AAA, such as "lbo", that's a NSWO scenario.

IPWorks AAA sends additional AVPs (Chargeable-User-Identity, User-Name, and Offload-Indication) in the Access-Accept message to Wi-Fi GW.

The Value of Chargeable-User-Identity is MSISDN, and the value of User-Name is IMSI.

The Value of Offload-Indication is 0, which indicates Wi-Fi GW not to setup an S2a GTP tunnel towards the PDN GW.
 - If the Wi-Fi subscription indication of the APN matches both the S2a indication and NSWO indication, such as "s2a.lbo", IPWorks AAA chooses the preferred one. In this case, the preferred subscription indication is "s2a", so this is an S2a scenario.
 - If the Wi-Fi subscription indication of the APN matches neither the S2a indication nor NSWO indication, IPWorks AAA will send Access-Reject to NAS.
 - If S2a scenario is disabled by IPWorks AAA, IPWorks will only check if the APN match the NSWO indication.

If several APNs are retrieved from HLR, IPWorks AAA will check the APNs one by one. If there is one APN which satisfies the condition, AAA will allow the subscriber to access to WLAN network.

3.3.2.2 APN without Wi-Fi Subscription Indication

IPWorks AAA server also supports authorization for APN without Wi-Fi subscription indication (Enhanced Wi-Fi Authorization).

The APN provisioned in HLR does not need the Wi-Fi subscription indication. The APN consists of one part: the APN name string.

For example:

The provisioned APN in HLR is "cmnet.mnc000.mcc460.gprs".

With Enhanced-WiFi-Authorization enabled, If a subscriber is allowed to access to WLAN network, the APN retrieved from HLR must not match those in the black list configured in IPWorks AAA. And the Network Access Mode must not be 1 (for GPRS only).

If S2a scenario is enabled by IPWorks AAA, subscriber is allowed to apply S2a scenario when the APN retrieved from HLR match those in S2a APN list.

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

For example, the APN name string configured in IPWorks AAA is "cmnet" and APN without Wi-Fi subscription indication configured as the following:

```
<Enhanced-Wifi-Authorization>
<S2A-APN-List>
  <S2A-APN Name="cmnet"></S2A-APN>
</S2A-APN-List>
<APN-Blacklist>
  <Blacklist-APN Name="coop"></Blacklist-APN>
</APN-Blacklist>
</Enhanced-Wifi-Authorization>
```

When the APNs retrieved from HLR, the logic of checking which type of Wi-Fi service scenario is as follows:

For each APN returned from HLR, it must not include any match in the blacklist configured in IPWorks AAA. And corresponding NAM returned must not equals to 1. Otherwise, the access request shall be rejected.

Then, the following logic in the table is executed for each APN. If there is one APN which satisfies the condition, AAA will grant the subscriber to access to Wi-Fi network.

If...	Then..
S2A-APN matches	It is trusted S2a scenario. IPWorks AAA does the same actions in S2a scenario as described in section 3.3.2.1
S2A-APN does not matches	It is NSW0 scenario. IPWorks AAA does the same actions in NSW0 scenario as described in section 3.3.2.1.

If several APNs are retrieved from HLR, IPWorks AAA will check the APNs one by one. Once there is one APN satisfies the condition, i.e. the APN is not in blacklist, and the Network Access Mode is not 1, AAA will allow the subscriber to access to WLAN network.

3.4 Accounting

Refer to the section *Accounting* in *IPWorks Generic AAA Function Overview* [6].

4 Operational Conditions

4.1 Configurable Parameters

IPWorks Wi-Fi AAA server can be configured through Ericsson Command-Line Interface (ECLI), please refer to *Configure Radius AAA* .

4.2 Commands and User Procedures

Please refer to *IPWorks AAA Parameter Description* [5] and *Command Line Interface User Guide for IPWorks SS* [7] for IPWorks CLI commands about IPWorks AAA server.

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

4.3 Charging

-

4.4 Characteristics

-

5 Statement of Compliance

RFC 3579	24/174 02-AVA 901 16 Uen A
RFC 3748	26/174 02-AVA 901 16 Uen A
RFC 4186	30/174 02-AVA 901 16 Uen A
RFC 4187	31/174 02-AVA 901 16 Uen A
RFC 5281	55/174 02-AVA 901 16 Uen PA1
RFC 5126	56/174 02-AVA 901 16 Uen PA1

6 Terminology

6.1 Abbreviations

AAA	Authentication, Authorization, Accounting
AKA	Authentication and Key Agreement
AMBR	Aggregate Maximum Bit Rate
APN	Access Point Name
AUTN	Authentication Token
AUTS	Authentication Token for re-synchronization
AV	Authentication Vector
AVP	Attribute-Value Pair
ENIW	Ericsson Network Integrated Wi-Fi
NSWO	Non-Seamless WLAN offload
ODB	Operator Determined Barring
SIM	Subscriber Identity Modules
TWAN	Trusted WLAN Access Network

6.2 Definitions

AAA	Authentication, Authorization, Accounting. A service that verifies the identity of users who request access to a network, determines and enforces their policies (the activities, resources, and services they are permitted to use and perform), and measures their use of the network for billing purposes.
-----	---

Prepared (also subject responsible if other) ECHGCHI		No. 60/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2017-04-10	Rev PA1	Reference

7 References

- [1] AAA Function Overview 1/155 17-CRA 119 1235
- [2] 3GPP AAA Server-WLAN Access Network Wa Interface Description 16/15005 19-AVA 901 16
- [3] IPWorks 3GPP AAA Server-HLR D'/Gr' Interface 41/155 19-AVA 901 16
- [4] Configure Radius AAA 49/1543-AVA 901 33/2
- [5] IPWorks AAA Parameter Description 2/190 84-AVA 901 33/2
- [6] IPWorks Generic AAA Function Overview 59/155 17-AVA 901 16
- [7] Command Line Interface User Guide for IPWorks SS
2/1553-AVA 901 33/2
- [8] Extensible Authentication Protocol Method for Global System for Mobile
Communications(GSM) Subscriber Identity Modules (EAP-SIM)
<http://www.ietf.org/rfc/rfc4186.txt>
- [9] Extensible Authentication Protocol Method for 3rd Generation Authentication and Key
Agreement (EAP-AKA)
<http://www.ietf.org/rfc/rfc4187.txt>
- [10] Extensible Authentication Protocol (EAP)
<http://www.ietf.org/rfc/rfc3748.txt>
- [11] RADIUS (Remote Authentication Dial In User Service) Support For Extensible
Authentication Protocol (EAP)
<http://www.ietf.org/rfc/rfc3579.txt>
- [12] IPWorks EPC AAA Function Overview 57/155 17-AVA 901 16