

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

IPWorks EPC AAA Function Overview

Contents

1	Introduction	3
1.1	Document History	3
1.2	Purpose.....	4
1.3	Scope	4
2	Overview.....	4
3	IPWorks EPC AAA Description	5
3.1	Network Scenarios	5
3.2	Architecture and Implementation	7
3.2.1	System Architecture (Component Relationship)	8
3.2.2	Message Handling Model	9
3.2.3	Database Schema	12
3.2.4	License	12
3.2.5	Session HA	13
3.3	Common Function and Configuration	14
3.3.1	Authentication Vector and User Profile Storage	14
3.3.2	Session Time-out Management	14
3.3.3	Session Management	16
3.3.4	EPC AAA Server Configuration	19
3.3.5	EAP-AKA/AKA' Identity Management	20
3.3.6	EPC AAA Peer Selection Functionality	21
3.3.7	EPC AAA Server Supporting HSS Redundancy	26
3.3.8	EPC AAA Server Supporting DRA	28
3.3.9	Overload Protection for EPC AAA.....	32
3.3.10	S6b Authentication without Profile (Optional).....	33
4	AAA for Trusted Non-3GPP IP Access Networks Interworking with EPC	35
4.1	Overview	35
4.2	Non-3GPP IP Access Network Initiated Authentication and Authorization	37
4.3	Non-3GPP IP Access Network Initiated Re-Authentication and Re-Authorization	39
4.4	Non-3GPP IP Access Network Initiated Re-Authorization	40
4.5	Non-3GPP IP Access Network Initiated Session Termination	40
4.6	AAA Server Initiated Session Termination on STa Interface ...	41
4.7	PDN GW Initiated Authorization Procedure	41
4.8	PDN GW Initiated Session Termination Procedure	42
4.9	Network Initiated De-Registration by HSS	42
4.10	HSS Initiated Update of User Profile	44
4.11	HSS Initiated P-CSCF Restoration.....	44
5	AAA for Untrusted Non-3GPP IP Access Networks Interworking with EPC	46

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

5.1	Overview	46
5.2	ePDG Initiated Full Authentication and Authorization	48
5.2.1	IMSI Mask Handling Support for SWm+ Interface and SWm Interface	49
5.2.2	IMEI Check Support for Untrusted Non-3GPP Access	51
5.3	ePDG Initiated Re-Authentication and Re-Authorization	52
5.4	ePDG Initiated Re-Authorization	52
5.5	ePDG Initiated Session Termination	53
5.6	AAA Server Initiated Session Termination on SWm/SWm+ Interface	54
5.7	S6b Procedure related with SWm Session	54
5.8	Public Key Authentication	54
5.8.1	Authentication and Authorization over SWm+	55
5.8.2	User Profile and Certificate Management for Non-SIM user ...	56
5.8.3	Support of AAA FE (PKI)	56
5.8.4	Certificate ID Checking	56
5.8.5	OCSP Checking	56
5.9	Network Initiated De-Registration by HSS	57
5.10	HSS Initiated Update of User Profile	58
5.11	HSS Initiated P-CSCF Restoration	60
5.12	WiFi Mobility Management	60
5.12.1	Full Authentication and Authorization with WiFiMM	60
5.12.2	Re-Authentication	62
5.12.3	Getting User Location	62
5.13	SES Support	65
5.13.1	SES Initiated Authentication for 4G Subscriber	66
5.13.2	SES Initiated Authentication for 3G Subscriber	66
5.14	Emergency Service Control	67
5.14.1	SWm+S6b Full Authentication and Authorization with Emergency Service	68
5.14.2	SWm Re-Authorization with Emergency Service	69
5.14.3	SWm+ Authentication and Authorization with Emergency Service	69
5.14.4	Roaming Check for Emergency Service	71
6	Standard Compliance Statement	71
7	Terminology	72
7.1	Abbreviations	72
7.2	Definitions	72
8	References	72

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

1 Introduction

1.1 Document History

Rev	Date	Sign.	Comment
PA1	2016-02-15	EZAIYUA	The first draft is based on 2/155 17-AVA 901 16(PL1), and replace all the description related to control panel caused by v17A WP: AAA Diameter Fundamental function.
PA2	2016-03-21	EZAIYUA	Fix the editoril error"Reference Source not Found".
PA3	2016-3-22	EZAIYUA	Replace all "Configure AAA Diameter" with "Configure EPC AAA".
PA4	2016-5-20	EJIAHLU	Update Section 3.2.4.
PA5-PA9	2016-5-23	ECIAMAO	Fixed TR#HU82094: update Figure 1, correct CPI reference, modify "templentityKey" to "aaatemplentityKey", the section "EPC AAA Server Supporting HSS Redundancy" is deprecaetd.
PA10-PA11	2016-06-08	ECIAMAO	Remove CRL relevant information.
PA12	2016-09-23	EQUUVWT	Update Section 3.3.7, 3.3.8, 5.
PA13	2016-10-21	EQUUVWT	Add Section 3.3.6.
PB1-PB2	2016-11-14	ECIAMAO	Fix display issue for the Figure 5 in PDF version.
PC1-PC2	2017-01-04	EQUUVWT	TR40406, update section 3.8.
C-PD1	2017-02-16	EJIAHLU	MRD47782, add new section 5.13.
E	2017-03-23	EJIAHLU	Update for revision informaiton.
G	2017-04-	ECIAMAO	Correct figure 23, 24, 36, and 37.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

	11		
PH1	2017-08-01	ECIAMAO	Add section "CUDB Support for Non-SIM User".
PJ1	2017-10-30	EJIAHLU	Add the new section "Emergency Service Support"
PK1	2018-01-24	ECIAMAO	C-dia 2.0 uplift: delete the section 3.3.6.1 "How C-diameter Selects Peer in the Peer Connection Table".
L	2018-06-14	EZGUOZI	Update the description in section "EPC AAA Server Supporting HSS Redundancy" due to PIDs' comment #3159463.

1.2 Purpose

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

1.3 Scope

This document is focus on the following points when describing the EPC AAA server:

- Describing 3GPP or RFC specifications implemented by EPC AAA server. For more details, refer to the IPWorks SoC or IWD, see the reference from [10] to [14].
- Describing the main architecture and implement consideration of EPC AAA server.
- Describing the main function implemented by EPC AAA server.

2 Overview

IPWorks EPC AAA server is the protocol server belonging to IPWorks product suite. It is used in EPC network to perform authentication, authorization and, accounting for the user accessing EPC through trusted or untrusted Non-3GPP Access Network.

The server is built under the framework of IPWorks and uses the common O&M function of IPWorks to do the work of operation and maintenance.

Figure 1 describes the process view of EPC AAA server in IPWorks environment:

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

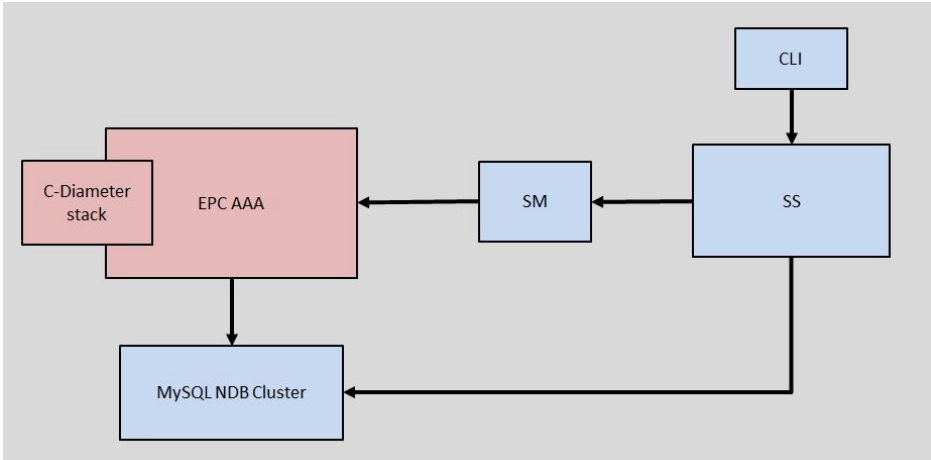


Figure 1 IPWorks EPC AAA Process View

User can use the CLI to view the status of sessions and send command to the EPC AAA server. The dynamic session data is saved in the MySQL NDB Cluster.

3 IPWorks EPC AAA Description

3.1 Network Scenarios

IPWorks AAA can take the role of 3GPP AAA server to provide AAA service for client create IP connectivity using non-3GPP accesses to the Evolved 3GPP Packet Switched domain.

Non-3GPP means that these accesses were not specified in the 3GPP. These technologies include for example WiMAX, cdma2000®, WLAN or fixed networks. The 3GPP standard defines two types of non-3GPP access: trusted and untrusted non-3GPP access as Figure 2. At the same time, the untrusted non-3GPP access provides service for two types of users, SIM user and Non-SIM user. The HPLMN operator of the EPC shall select whether a connected non-3GPP IP access network is a trusted or untrusted IP access network.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

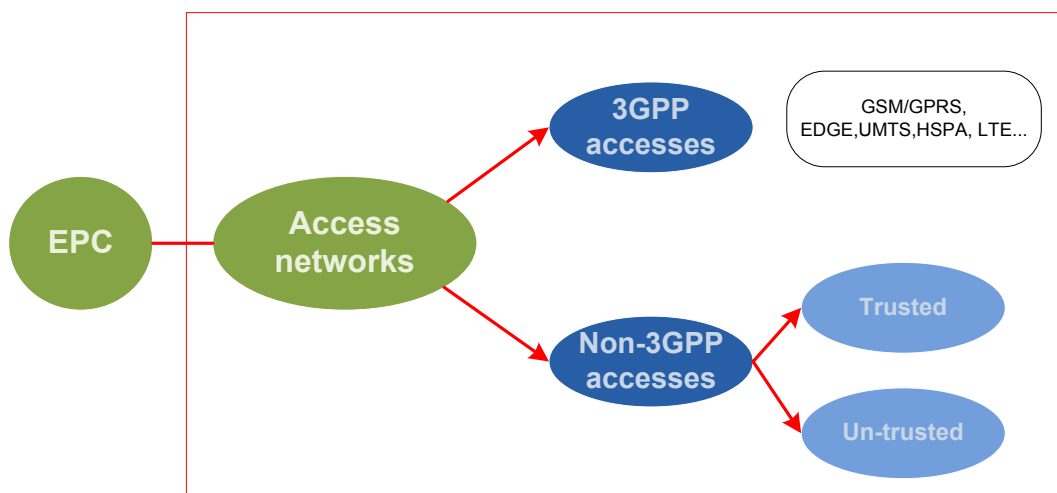


Figure 2 3GPP and Non-3GPP Access Network

In non-3GPP access, IPWorks AAA supports the following AAA reference points. These reference points support both TCP and SCTP protocols. The SCTP protocol supports the multi-homing function. IPWorks supports Diameter over SCTP protocol via SS7 SCTP stack(E-SCTP).

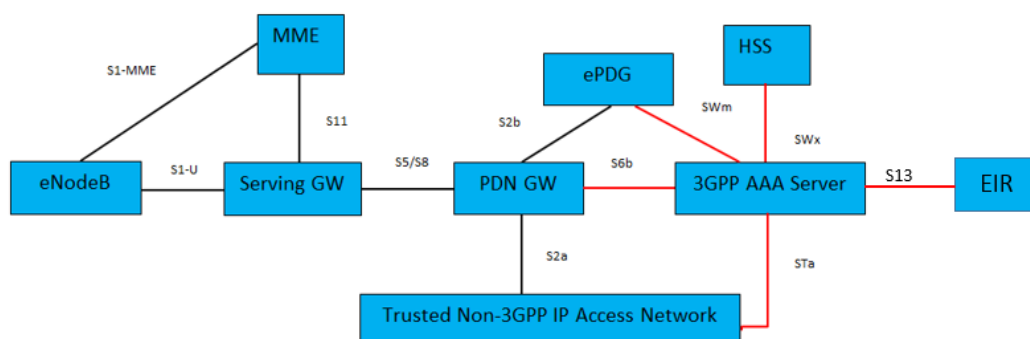


Figure 3 3GPP AAA Server and Neighbouring Nodes in EPC Network

- STa reference point between trusted non-3GPP access and AAA server.

An authentication and authorization procedure is mandatory and it is based on EAP-AKA' (for clarity written here EAP-AKA prime). It is possible to separate the security domain per such trusted non-3GPP access by using the access network id(ANID) within its key derivation function, as far as different ANIDs are used, EAP-AKA prime was specifically developed for this environment. STa is complemented by EAP transport over any L2 towards the UE.

- SWm reference point between ePDG and AAA server:

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

This realizes the mandatory authentication and authorization with IPsec tunnel setup between UE and ePDG. SWm is concatenated to IKEv2 signalling (which in turn encapsulates EAP) towards the UE.

- S6b reference point between PDN GW and AAA server:

It is used to deliver general authorization data (such as, default APN, authorized APNs, PDN type, static IP address), and authorized features of mobility with non-3GPP accesses (for all IP variants within EPS). Additionally subscription data can be conveyed, just like the type of charging and (static) QoS profile and information trace data.

- SWx reference point is located between 3GPP AAA Server and HSS and is used for transport of authentication, subscription, and PDN connection-related data.
- S13 reference point is located between 3GPP AAA Server and EIR and is used to perform the IMEI Check during authentication procedure over SWm interface.

Note:

STa, SWm, S6b and S13 reference points must use the same transport protocol, TCP or SCTP. While for SWx reference point, different transports(The transport item within RouteItem) can use different protocols.

3.2 Architecture and Implementation

EPC AAA server is constructed by different modules. Each module provides certain service to other modules.

Figure 3 illustrates the associativity between those modules.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

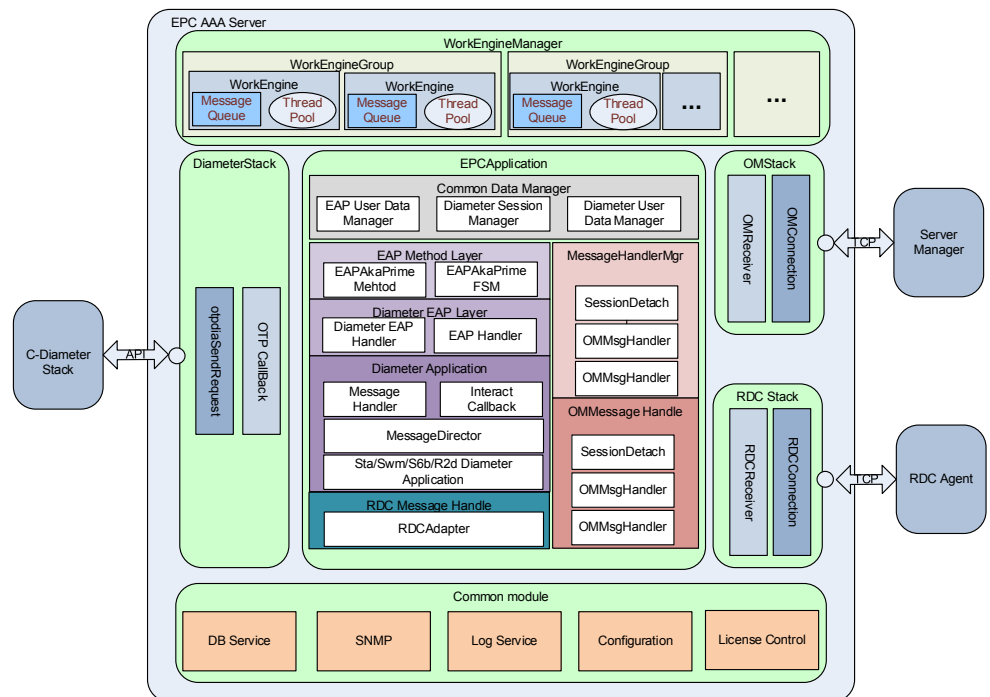


Figure 4 EPC AAA Architecture

3.2.1 System Architecture (Component Relationship)

The components in this architecture are described as follows:

C-Diameter Stack: The 3PP diameter stack is developed by Ericsson. It receives the diameter message and decodes the message to internal structure according to the defined dictionary. It also encodes the diameter message and sends the diameter message out to the peer node.

Server Manager: The component used by SS&CLI controls the behavior of AAA server, such as triggers the AAA to send out a message.

RADIUS RDC Agent: The component helps translate RADIUS traffic into internal Diameter message and sends them to EPC AAA for handling.

Work Engine Manager: The message handle mechanism inputs the message received to the message queue and uses the thread from the thread pool to call the service interface provided by the application to handle the message.

Message Stacks: Different message stacks help receive and send the messages to or from different interface, including Server Manager, RADIUS RDC Agent, and C-Diameter Stack

EPC Application: This module includes the implementation of the features defined in TS 29.273. In this module, IPWorks EPC AAA handles different traffic according to the message incoming source and Diameter application Id.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

DB Service: The utility module provides the services of accessing and doing the operation to the NDB Cluster.

SNMP: The utility module provides the service that supports sending SNMP counter and alarm to SNMP Master Agent.

Log Service: The utility module provides the service of logging.

Configuration: The utility module provides the service of getting configuration parameters.

3.2.2 Message Handling Model

3.2.2.1 Message Queue and Thread Pool

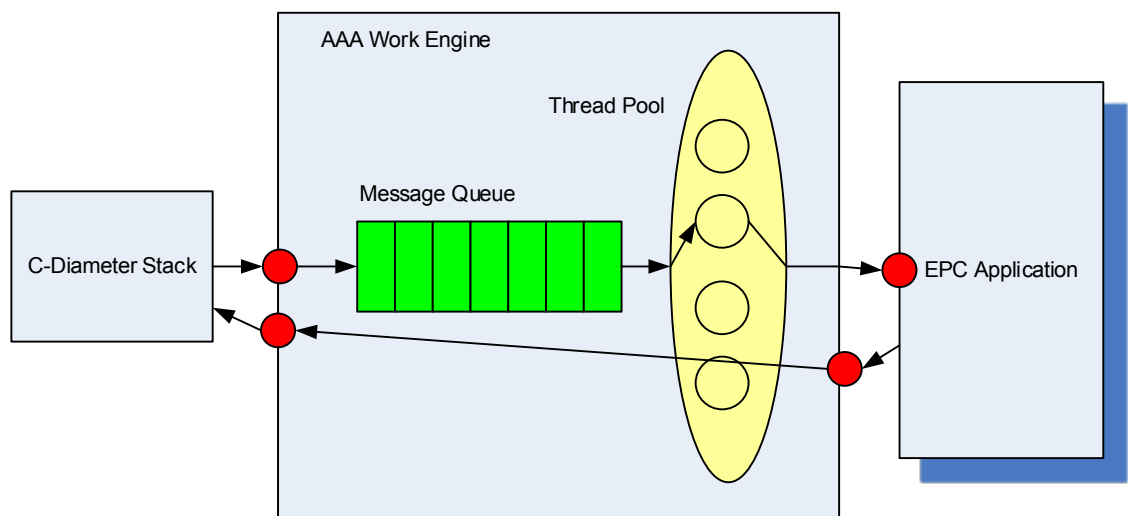
The C-Diameter Stack is responsible to receive the diameter message (request or response) and parse the original message package to the inner message structure defined by C-Diameter.

For IPWorks AAA server, it realizes the callback function that used to receive the incoming message that already parsed by C-Diameter Stack. When it receives the message, it puts the message to the message queue. The message queue is handled using FIFO manner.

The message in the message queue is handled by the thread. Thread pool is created when the system starts up, each thread in the pool listens on the message queue, if the queue is not empty, the thread fetches the message and call the service API provided by the EPC application to handle it.

The work engine also provides interface that used by EPC application to send out request or response message.

The process is described in Figure 4:



Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

Figure 5 Message Handle Process

3.2.2.2 Callback Based Message Intercommunication

When handling the request message from Access GW, ePDG, RDC Agent or PDN GW, new request message might be triggered to fetch user profile or authentication vector information from HSS. After fetch the information needed from HSS, the AAA server will send the corresponding response back to the requester. To handle such situation, callback-based message intercommunication is designed.

If one request message triggers new request message, a callback recording the origin request information is created and mapped to the new request. When the response message corresponding to the new request is back, the callback is triggered to send the response message to the origin request message.

The mechanism is described in Figure 5.

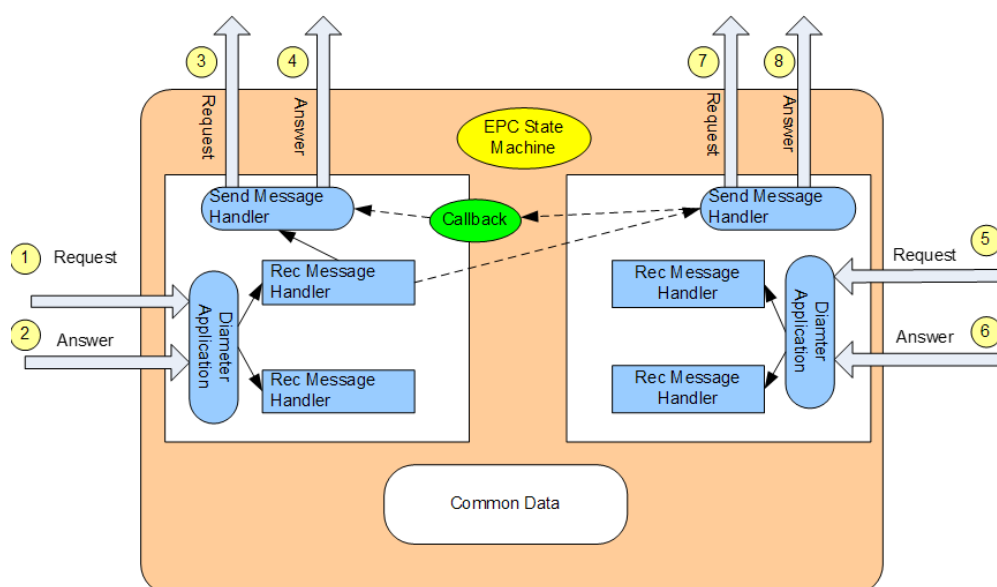


Figure 6 Callback Based Message Intercommunication

3.2.2.3 Layered Message Handle Model

For EPC, AAA server does the authentication and authorization for the user from Non-3GPP Access GW. The authentication is using EAP-AKA/AKA' and EAP-TLS protocol defined RFC 3748, RFC 4187, RFC 5448, and RFC 5216. The EAP-AKA/AKA' and EAP-TLS protocol is carried above the diameter protocol and has its own state management.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

To decouple the relationship between Diameter Protocol, EAP, EAP-AKA/AKA' and EAP-TLS, the architecture of AAA server is divided into different layers, each layer handles the definite protocol and do the work specified by the protocol. Communication between each layer is through clear and limited interface.

The layer architecture of AAA server is described in Figure 6:

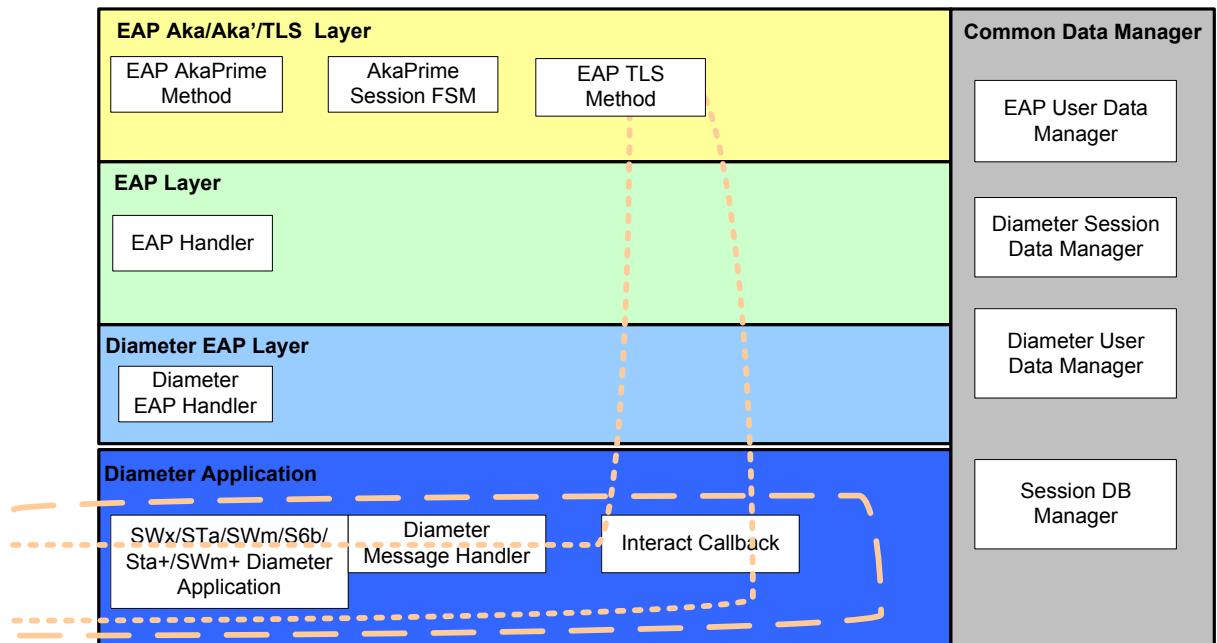


Figure 7 Layer Message Handling Architecture

The description of each layer is shown as follows.

- Diameter Application Layer: the layer handling the diameter message from/to STa, SWm, S6b, SWx, STa+, and SWm+ interface.
- Diameter EAP Layer: the layer that act as adapter between diameter and EAP layer. It will extract the EAP-Payload package from diameter message and send to the EAP layer to handle, or packing the EAP-Payload to the diameter message.
- EAP Layer: the layer that decodes the EAP-Payload package and does the basic verification.
- EAP Aka/ Aka'/TLS Layer: the layer that implements the EAP-AKA/AKA'/TLS algorithm and maintain the state of authentication.
- Besides the protocol layer, there are also the data need to be maintained for diameter session and user. Just as the right part in Figure 6.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

3.2.3 Database Schema

There are four main tables that record the information of session and user profile.

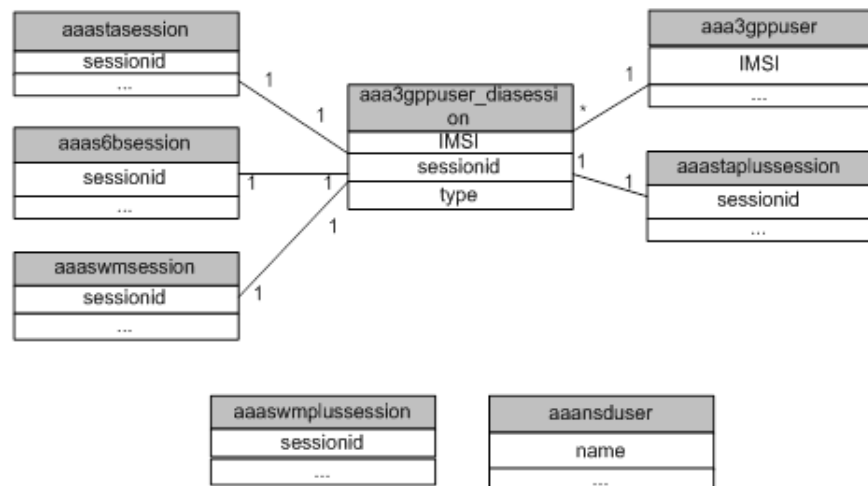


Figure 8 Data Schema Relationship

aaastasession, aaaswmsession, aaaswmpusession, aaastaplusession, and aaas6bsession tables record the session information related to STa, SWm, SWm+, STa+, and S6b interface.

aaa3gppuser table records the user data fetched from HSS.

aaansduser table records the provisioning user data for NSDS solution.

The aaa3gppuser_diasession table records the mapping relationship between aaa user and session bound to it.

The detail description of the table fields refers to the database schema description document.

3.2.4 License

EPC AAA server has four licenses:

- AAA Base - Classic Session Capacity License
- AAA Base - Layered Session Capacity License
- PKI Authentication Support Feature
- WiFi Mobility Support Feature

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

AAA EPC Session Capacity License controls the capacity of the diameter session (including STa session and SWm session).

When AAA Server is deployed in classic architecture, the AAA Base - Classic Session Capacity License is used to control the capacity of the diameter session (including STa session and SWm session).

When AAA Server is deployed in data-layered architecture, the AAA Base - Layered Session Capacity License is used to control the capacity of diameter session.

For more license detail, refer to **License Management**.

3.2.5 Session HA

EPC AAA server supports two or more servers running at the same time sharing database. If one server is down, traffic is not affected because all the session and user data are stored in the database and accessible to all connecting nodes.

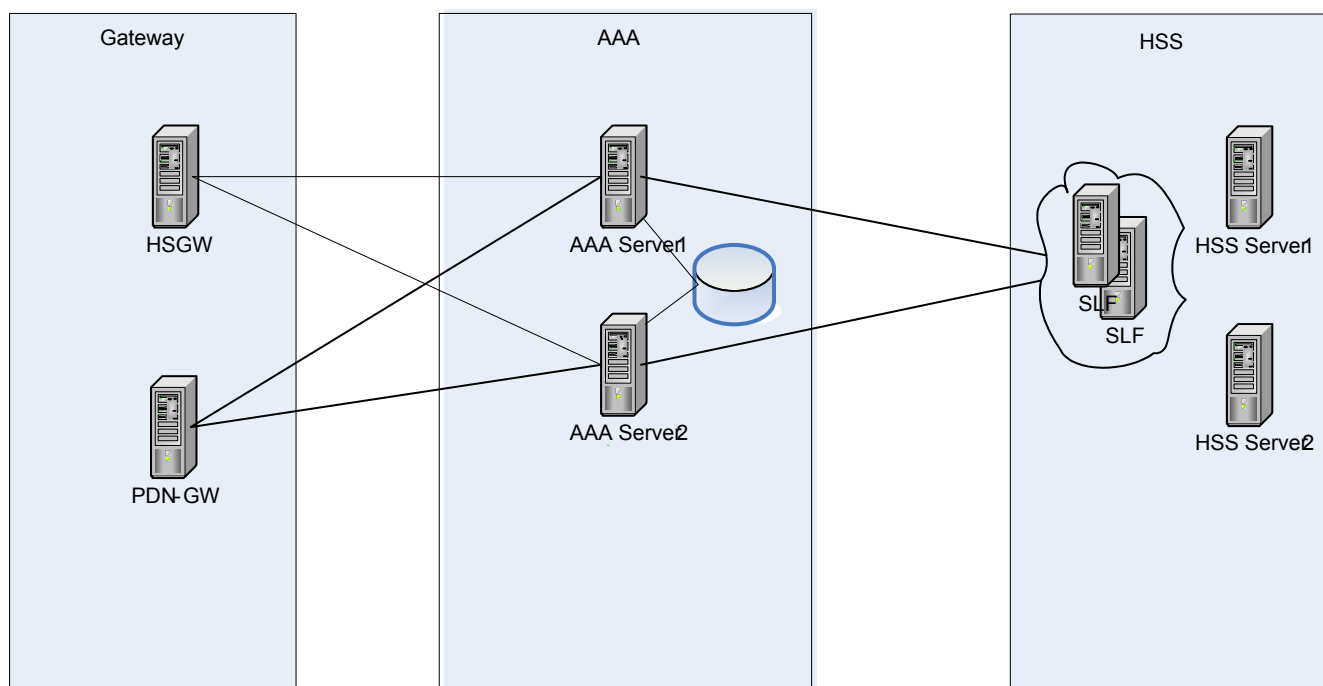


Figure 9 One Typical AAA HA Deployment

Although EPC AAA server supports the session HA, but it does not support EAP authentication HA, which means in the progress of an authentication, the message cannot sent randomly to AAA servers, the whole authentication progress must be finished at one node.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

3.3 Common Function and Configuration

This section describes the functions and configuration that implemented by EPC AAA server.

3.3.1 Authentication Vector and User Profile Storage

The EPC AAA server fetches the authentication vector and user profile from HSS in authentication and authorization procedure.

To improve the performance and support fast re-authentication, the EPC AAA server caches the related information in NDB database for the successful authenticated users. And such cached data is deleted by the EPC AAA server when the last user-related EPC session is terminated.

When a new UE requires accessing EPC through Non-3GPP IP access network, the EPC AAA server requests the vectors from HSS for authentication. By default, five authentication vectors are fetched at a time and each EAP-AKA/AKA' full authentication may consume only one vector; the others are stored in NDB database for using by subsequent authentication. If there are no or not enough vectors in cached data, the EPC AAA server requests the vectors from HSS again. The number of authentication vectors fetched from HSS at a time is configurable, the maximum number is five, and the minimum number is one.

Note: When WiFi Mobility Management feature is enabled, EPC AAA server fetches only one authentication vector from HSS in the MAR message, which ensure that EPC AAA sends the AVP *Visited-Network-Identifier* to HSS in the MAR message for every authentication.

On the other hand, the fetched user profile is also stored in NDB cluster for using by other subsequent session handling procedure, like S6b.

Such cached authentication vector and user profile are removed immediately when all the user-related EPC sessions are terminated.

3.3.2 Session Time-out Management

EPC AAA server tries to clean up the time-out session according to the Authorization-Lifetime and Auth-Grace-Period AVP or Session-Timeout AVP value.

When the Non-3GPP IP Access Gateway performs the initial authentication and authorization, re-authentication and/or re-authorization, the AAA server can bring back the Authorization-Lifetime, Auth-Grace-Period and Session-Time-out AVP to the Non-3GPP IP Access Gateway in the authorization procedure according to the configuration.

AAA server considers the session is timeout in the following two scenarios:

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

- The Non-3GPP IP Access Gateway must complete the re-authentication/re-authorization procedure within the period of Authorization-Lifetime since last successful authentication/authorization. If the Non-3GPP IP Access Gateway does not complete the re-authentication/re-authorization within the period which is the summation of Authorization-Lifetime and Auth-Grace-Period since last successful authentication/authorization, the AAA server will take the related EPC session as timeout and cleanup it.
- The total session life time should not beyond the value which specified in Session-Timeout AVP. Otherwise the AAA server will take the related EPC session as timeout and cleanup it.

Figure 9 shows the procedure sequence for AAA cleanup the timeout sessions for EAP-AKA/AKA' authentication:

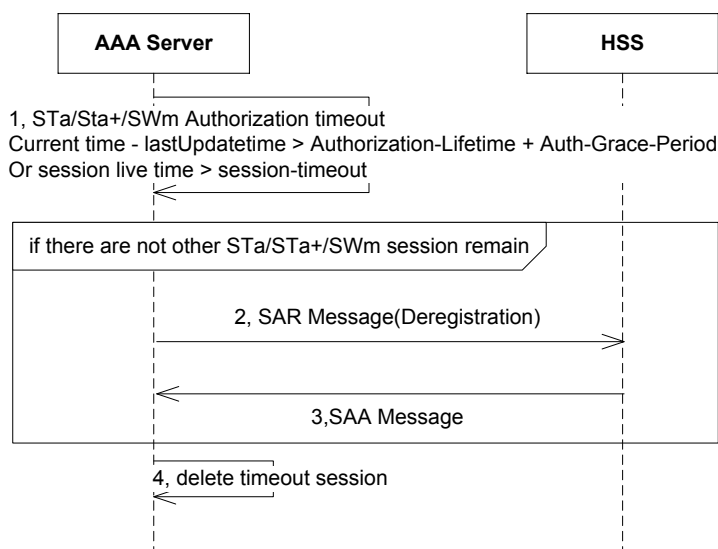


Figure 10 Sequence Diagram of Timeout Session Cleanup for EAP-AKA/AKA' authentication

Figure 9 shows the procedure sequence for AAA cleanup the timeout sessions for EAP-TLS authentication

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

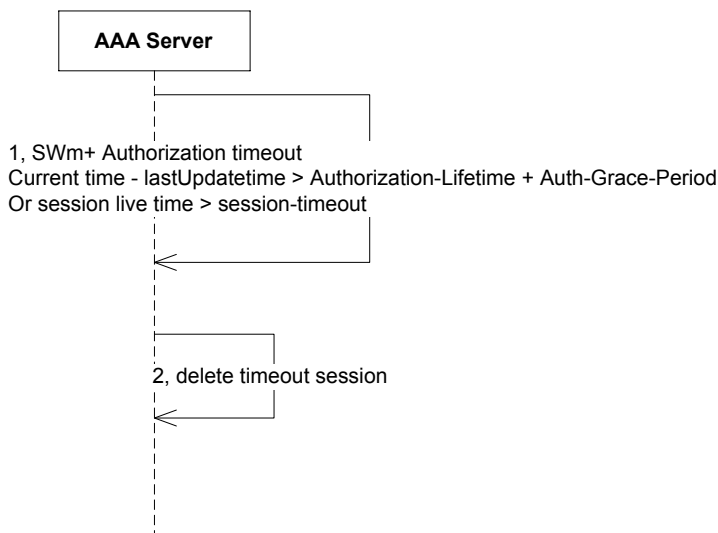


Figure 11 Sequence Diagram of Timeout Session Cleanup for EAP-TLS Authentication

The feature can be configured according to **Configure EPC AAA**, [1].

3.3.3 Session Management

In EPC, there are several types of diameter sessions, include Sta, SWm, SWm+ and S6b session. The Sta, SWm, and SWm+ session are created when the user accesses the EPC from the trusted Non-3GPP Access Network or ePDG and deleted when the user send STR message to terminate the session. The S6b session which is created when the PDN GW update the information to the 3GPP AAA server and deleted when the PDN GW connection is closed.

User can use the CLI to show those sessions, include STa, Sta+, SWm, SWm+, and S6b session, according to the specified filter. The syntax example is shown below:

```
IPWorks> send aaaserver [<aaaservername>] -message="show stasession" -
query="<AVPEXpression_1>[&&<AVPEXpression_2>&&<AVPEXpression_3>...]"
```

The user can also use the CLI to detach the existing diameter sessions, include STa, STa+, and SWm+ session, according to the specified filter. The syntax is shown below:

```
IPWorks> send aaaserver [<aaaservername>] -message="detach stasession" -
query="<AVPEXpression_1>[&&<AVPEXpression_2>&&<AVPEXpression_3>...]"
[-force]
```

For the detailed usage of these two functions, refer to **IPWorks Configuration Management**, Reference [1].

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

Figure 11 shows the detach procedure sequence for EPC AAA sessions.

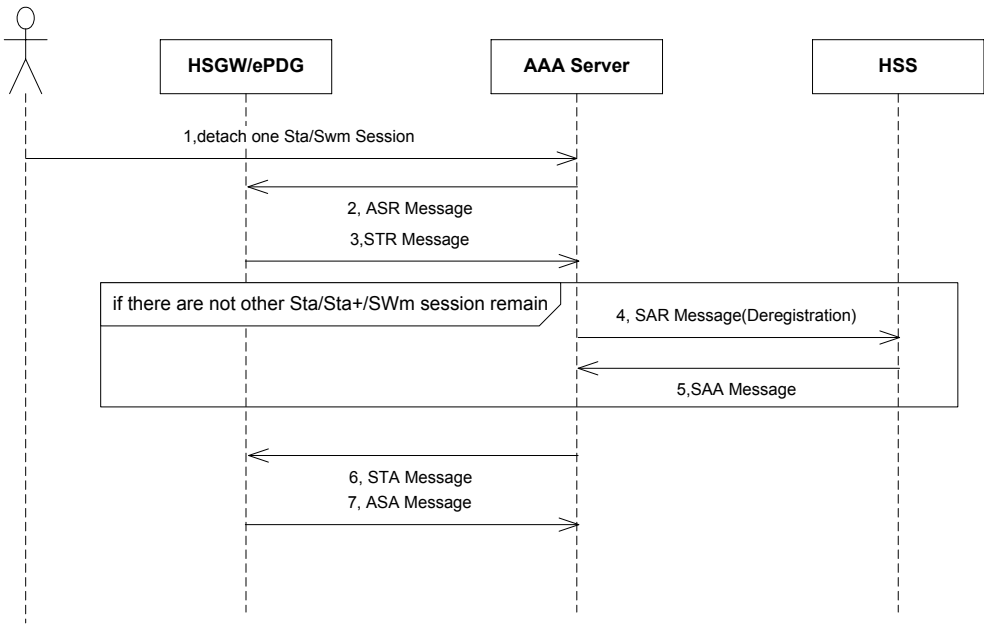


Figure 12 Sequence Diagram of Session Detach Using CLI

As a special case of EPC sessions, STa+ session is used in ENIW Trusted WiFi access solution, when EPC AAA handling the authentication from RADIUS translate agent, a STa+ session will be created. A Sta+ session is always associated with one RADIUS accounting session.

User can use CLI to detach a Sta+ session similar with to detach a Sta session. Figure 12 shows the message sequence flow for detach a Sta+ session.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

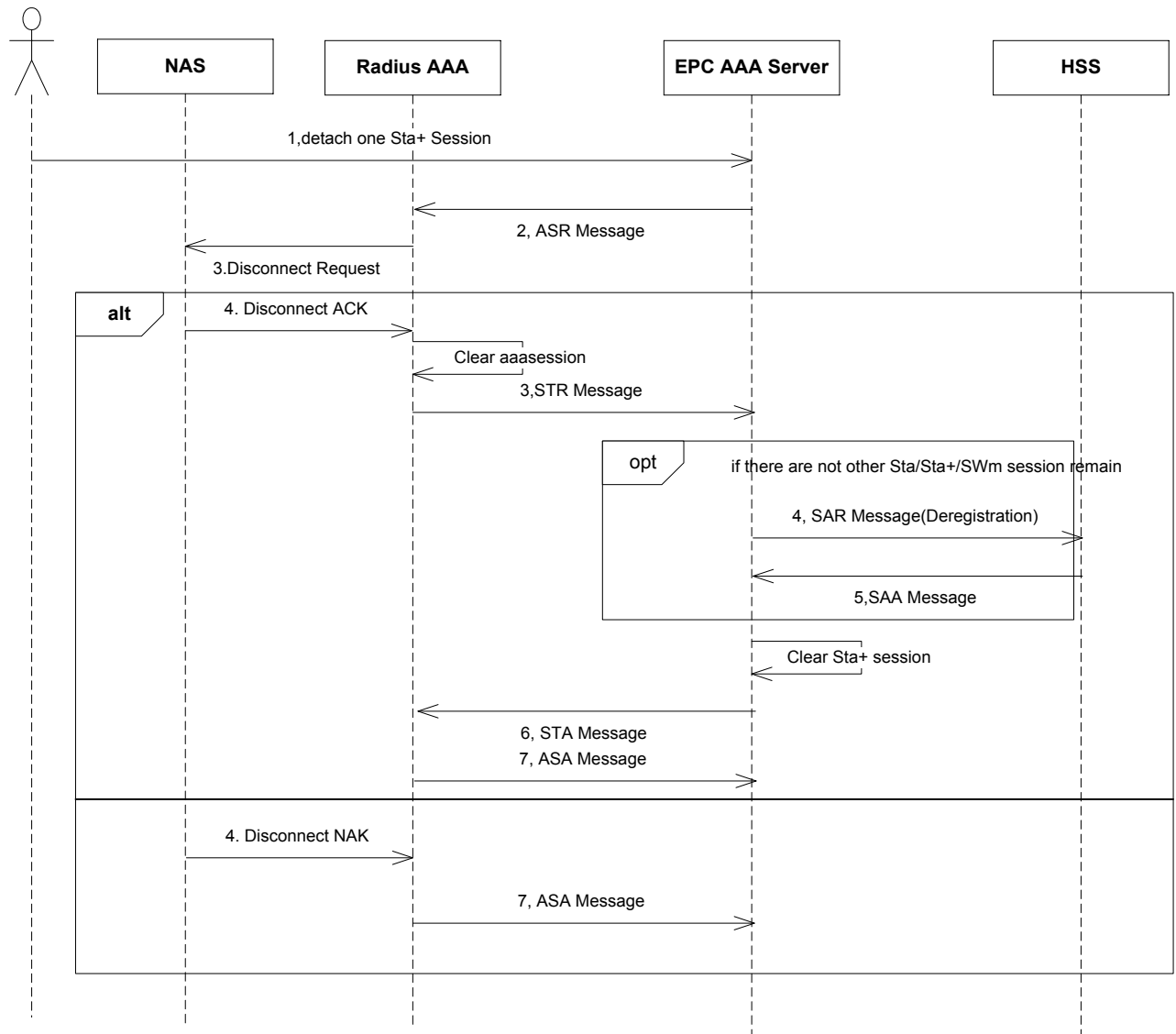


Figure 13 Sequence Diagram of Sta+ Session Detach Using CLI

Another special case of EPC session, SWm+ session is used in Non-Sim Device Solution. Figure 13 shows the message sequence flow for detaching a SWm+ session.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

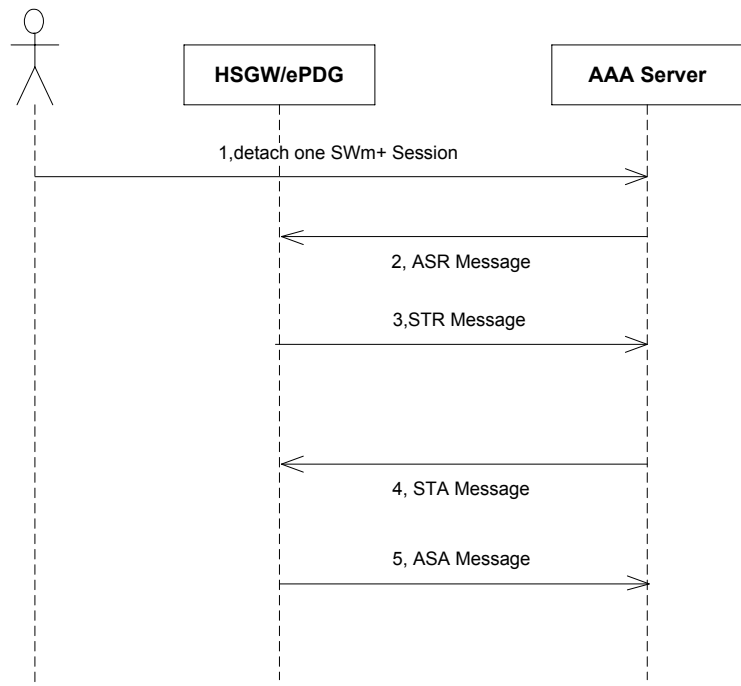


Figure 14 Sequence Diagram of SWm+ Session Detach Using CLI

3.3.4 EPC AAA Server Configuration

The EPC AAA server configuration consists of the following two configurations:

- C- Diameter Stack Configuration
- EPC AAA Server Configuration

3.3.4.1 C-Diameter Stack Configuration

The C-Diameter Stack is a component that IPWorks AAA server uses as the protocol front end. It covers the following tasks:

- Setting up and managing the connection with the Diameter peers.
- Receiving and sending the Diameter message.
- Parsing the Diameter message and processing the basic Diameter protocol error.
- Listening and accepting the connection from the client of AAA (such as Non-3GPP IP Access Gateway and PDN Gateway)
- Setting up the connection to the server of AAA, such as HSS

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

For the detailed parameter descriptions and configuration examples, refer to Section *Configuring C-Diameter Stack* in **Diameter Stack Configuration Guide**.

3.3.4.2 EPC AAA Server Configuration

For the detailed configuration, refer to **Configure EPC AAA**, [2].

3.3.5 EAP-AKA/AKA' Identity Management

IPWorks EPC AAA server support the EAP-AKA and EAP-AKA' authentication method respectively in SWm and STa authentication procedure as specified in RFC 4187 and RFC 5448. This section will give some description about the Identity management implement in IPWorks EPC AAA server.

3.3.5.1 Identity Generate

During EAP-AKA/AKA' authentication procedure, IPWorks EPC AAA server will generate unique Pseudonyms and unique Fast Re-authentication Identities for a user as specified in RFC4187 section 4. The Pseudonyms and Fast Re-authentication Identities format is according to the description in 3GPP TS23.003 section 14.

As a component part of the Pseudonyms or re-authentication identities, the temporary identities are used for distinguishing different identities. IPWorks EPC AAA will generate such temporary identities according to 3GPP TS 33.234 section 6.4.

A 128-bit encryption key shall be used for the generation of temporary identities for a given time determined by the operator. Once that time has expired, a new key shall be configured at all the IPWorks AAA servers. The old key shall not be used any longer for the generation of temporary identities, but the AAA servers must keep a number of suspended (old) keys for the interpretation of received temporary identities that were generated with those old keys. The number of suspended keys kept in the AAA servers (up to 16) should be set by the operator, but it must be at least one, to avoid that a just-generated temporary identity becomes invalid immediately because of the expiration of the key. IPWorks stores those encryption keys in database as below schema:

KeyValue (Char32)	Key0 (Char32)	Key1 (Char32)	Key2 (Char32)	...	Key15 (Char32)	Active key id (Smallint)	number of suspended keys (Smallint)
----------------------	------------------	------------------	------------------	-----	-------------------	-----------------------------	--

Operator could manage those encryption keys through CLI as the following example:

```
IPWcli> modify aaatempIdentityKey -set KeyValue="test1234";SuspendedKeysNumber=3
```

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

IPWcli> list **aaatempIdentityKey**

[**aaatempIdentityKey** test1234]

KeyValue : test1234

suspendedKeyNumber: 3

3.3.5.2 Qualcomm Customized EAP-AKA Identity

As a Qualcomm customized function, IPWorks EPC AAA server allows UE embedding the MAC address into EAP-AKA Identity. The Qualcomm customized Identity format as follows:

- (0/2/4)IMSI@**MAC**:nai.epc.mnc<xxx>.mcc<yyy>.3gppnetwork.org

[0262800502800000@00-26-CA-B6-E8-
00:nai.epc.mnc080.mcc262.3gppnetwork.org]

When received such format identity, IPWorks EPC AAA server removes the MAC address from the EAP-AKA identity realm for MK calculating to generate keying material.

3.3.6 EPC AAA Peer Selection Functionality

When EPC AAA server sends out the outgoing request message, it will use peer selection function to select the peer that EPC AAA will send the message to.

C-diameter stack implements peer selection functionality. It will first check the peer connection table to see whether there is a matched direct connection peer. If there is a matched peer, the message will be sent to the peer. If not, C-diameter will use the configured otpdiaSelector to perform the peer selection.

3.3.6.1 How C-diameter Selects Peer with the OtpdiaSelector

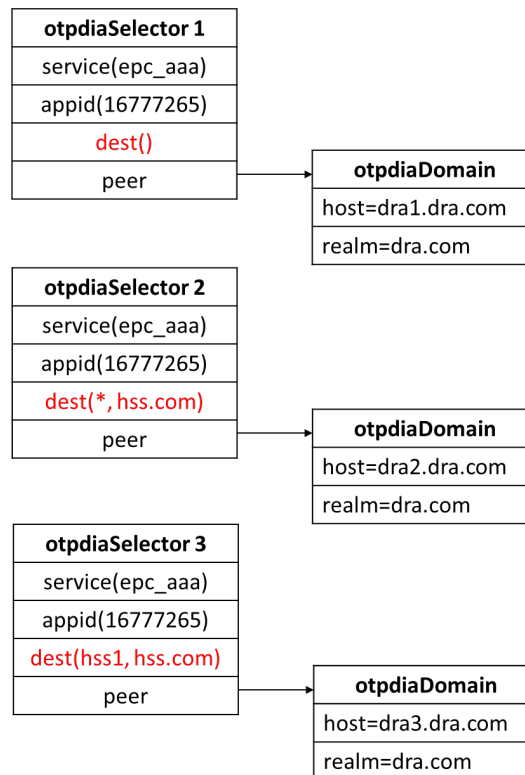
OtpdiaSelector has the following attributes: service, application id, destination, and peer. The service, application id and destination of an outgoing request are matched against configured otpdiaSelector objects to determine the applicable otpdiasector. If otpdiasector is found, the outgoing request message will be sent to the peer in the selected otpdiasector. For the detail concept of otpdiaSelector, please refer to C-diameter documents.

Here is the otpdiaSelector match rule:

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

- a. For destination field, the match preference is: specific Destination-Host before specific Destination-Realm before empty destination.

For example: There are following configured otpdiaSelector.

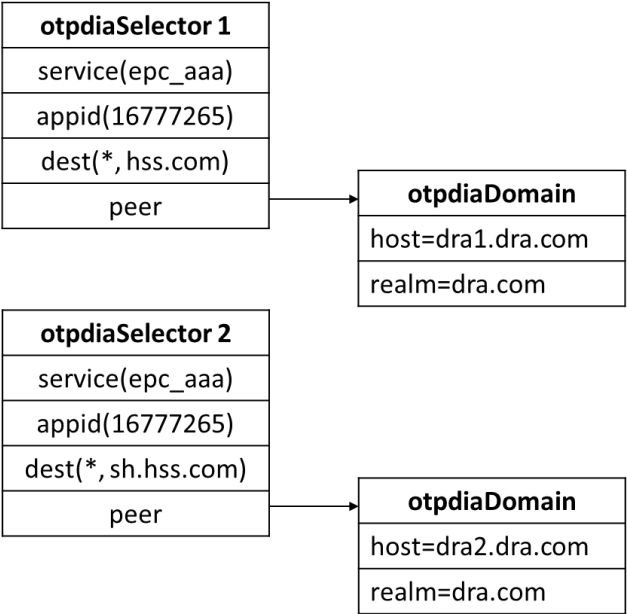


For different outgoing diameter request message, the matched otpdiaSelector is:

Outgoing diameter request Message			Matched selector
Application-Id	Destination-Host	Destination-Realm	
16777265	hss1	hss.com	otpdiaselector 3
16777265	hss2	hss.com	otpdiaselector 2
16777265	hss3	ericsson.com	otpdiaselector 1

- b. Longest match is applied for Destination-Realm.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

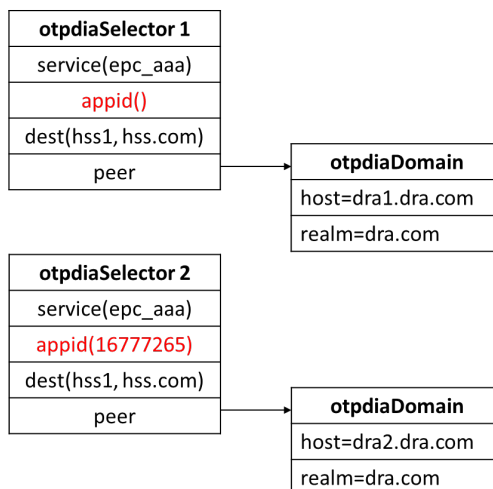


For different outgoing diameter request message, the matched otpdiaSelector are:

Outgoing diameter request Message			Matched selector
Application-Id	Destination-Host	Destination-Realm	
16777265	hss1	hss.com	otpdiasector 1
16777265	hss2	sh.hss.com	otpdiasector 2
16777265	hss3	bj.hss.com	otpdiasector 1

- c. For destination field, the match preference is: specific application ID before empty application ID.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference



For different outgoing diameter request message, the matched otpdiaSelector are:

Outgoing diameter request Message			Matched selector
Application-Id	Destination-Host	Destination-Realm	
16777265	hss1	hss.com	otpdiaselector 2
16777217	hss1	hss.com	otpdiaselector 1

3.3.6.2 C-diameter Selects Peer in Redundant Way

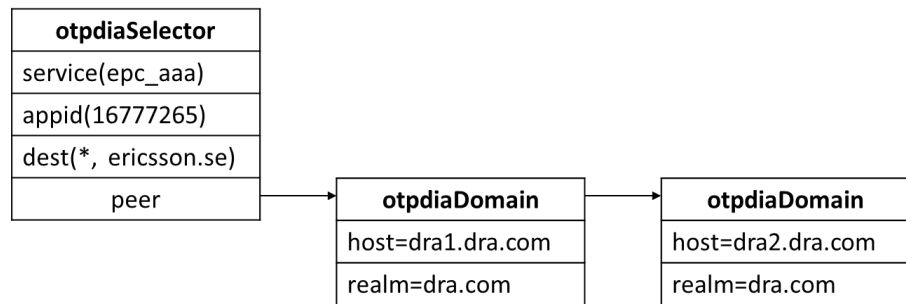
In the otpdiaSelector, the peer points to a list of otpdiaDomain. otpdiaDomain contains the peer host and realm. C-diameter can select the peer in failover or load sharing way. There are two typical scenarios: HSS Redundancy and DRA Redundancy, which will be illustrated in 3.3.7 and 3.3.8.

3.3.6.2.1 C-diameter Selects Peer in Failover Way

For a given otpdiaSelector, the list of OptdiaDomain instances pointed at by the peer attribute are interpreted as being in order of preference. That's how C-diameter implements the peer selection in failover way.

For example, assume following otpdiaselector is found for outgoing request message, per the configuration, this outgoing request message will be sent to peer with host (dra1.dra.com). If Diameter AAA loses connection with peer (dra1.dra.com), it will select peer (dra2.dra.com) to send the outgoing request message. If the lost connection is back, peer (dra1.dra.com) is selected to send the outgoing request message.

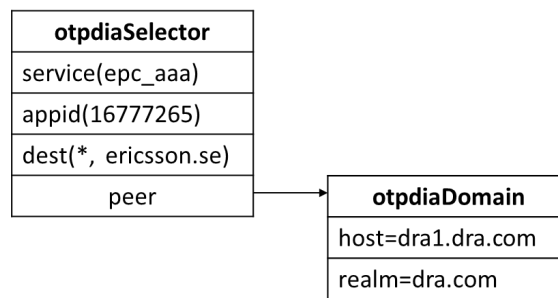
Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference



Diameter stack management tool is used to configure these diameter stack parameters. For this example:

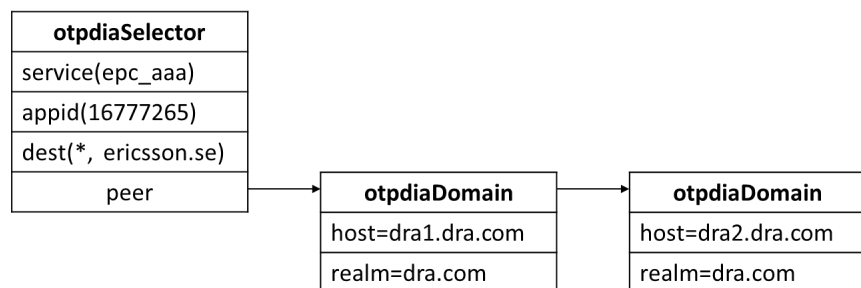
```
# dia-route-ctr --cmd add --app "SWx" --dest "[*], ericsson.se" --peer "[dra1.dra.com], dra.com"
```

The configured otpdiaSelector will be:



```
# dia-route-ctr --cmd add --app "SWx" --dest "[*], ericsson.se" --peer "[dra2.dra.com], dra.com"
```

The configured otpdiaSelector will be:



```
# SC-1:~ # dia-route-ctr --cmd list
```

RouteTable:

```
-----
id:    1
app:   SWx
dest:  host = *, realm = ericsson.se
```

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

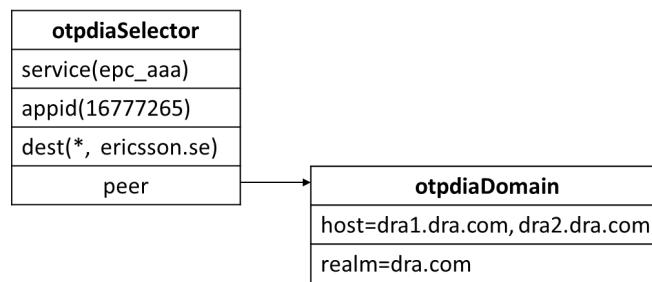
```
peer:  host = ['dra1.dra.com'], realm = dra.com
priority: 1
```

```
-----
id:    2
app:   SWx
dest:  host = *, realm = ericsson.se
peer:  host = ['dra2.dra.com'], realm = dra.com
priority: 2
```

3.3.6.2.2 C-diameter Selects Peer in Load Sharing Way

For a given otpdiaSelector, if OtpdiaDomain specifies more than one peer host attribute, the peers will be selected in random way. That's how C-diameter implements the peer selection in load sharing way.

For example, assume following otpdiasselector is found for outgoing request message, per the configuration, this outgoing request message will be sent to peer with peer (dra1.dra.com) and peer (dra2.dra.com) randomly.



Diameter stack management tool is used to configure these diameter stack parameters. For this example:

```
# dia-route-ctr --cmd add --app "SWx" --dest "[*, ericsson.se" --peer "[
dra1.dra.com, dra2.dra.com], dra.com"
```

```
# dia-route-ctr --cmd list
RouteTable:
```

```
-----
id:    1
app:   SWx
dest:  host = *, realm = ericsson.se
peer:  host = ['dra1.dra.com', 'dra2.dra.com'], realm = dra.com
priority: 1
```

3.3.7 EPC AAA Server Supporting HSS Redundancy

The EPC AAA supports the HSS redundancy.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

- When EPC AAA server connects to HSS servers directly,
 - For the first SWx request for a new user, EPC AAA server uses the failover and load-sharing policy to select one of active HSS peers in the configured HSS and send the SWx request to the selected HSS server. The HSS server sends the respond to the EPC AAA server with a Destination-Host information.
 - The subsequent SWx requests for the same user including the certain Destination-Host for the selected HSS, shall be sent to the selected HSS server.
- When EPC AAA server connects to HSS server via DRA,
 - For the first SWx request for a new user, EPC server AAA sends the request to one DRA and the DRA shall implement failover or load-sharing policy to route the SWx request to one HSS server. The HSS server sends the respond to the DRA with a Destination-Host information.
 - The subsequent SWx requests for the same user including the certain Destination-Host for the selected HSS, shall be routed to the selected HSS server by DRA.

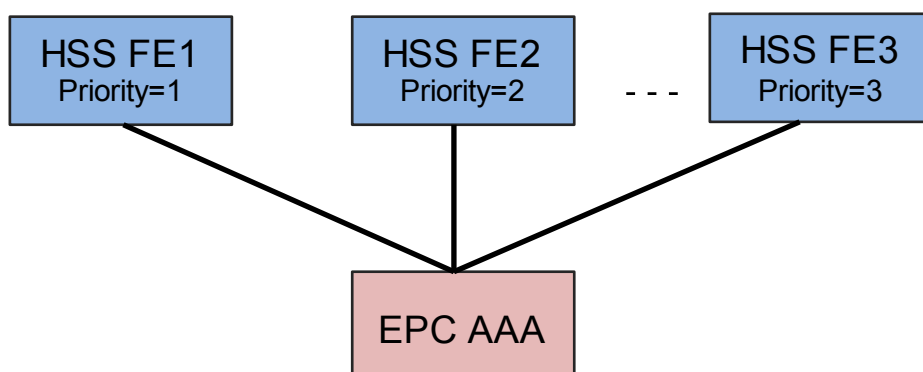
Note: The EPC AAA Server supports EIR Redundancy. The EIR redundancy mechanism is same as HSS redundancy.

3.3.7.1 HSS Redundancy Mode

The redundancy is either in failover mode or load-sharing mode, which depends on the way to configure the HSS information through the diameter stack management tools. For the detailed configuration, refer to Section *Configuring Diameter Route in Diameter Stack Configuration Guide*.

3.3.7.1.1 Failover Mode

In the failover mode, the EPC AAA server always selects highest priority and available HSS to send requests based on user sessions. Failover happens when the connection of the HSS server with highest priority is lost as shown in Figure 14.



Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

Figure 15 EPC AAA in Failover Mode

For example, the priority of HSS FE 1,2,3 is 1,2,3 respectively in the failover mode. When HSS FE 1 connection is lost, the EPC AAA server sends all requests to HSS FE 2.

- If HSS FE 1 connection is recovered, the EPC AAA server sends all requests back to HSS FE 1.
- If HSS FE 2 connection is lost and HSS FE 1 is not recovered, the EPC AAA server sends all requests to HSS FE 3.

3.3.7.1.2 Load-sharing Mode

In the load-sharing mode, the EPC AAA server distributes the load based on user sessions among the active connection of the HSS servers as shown in Figure 15.

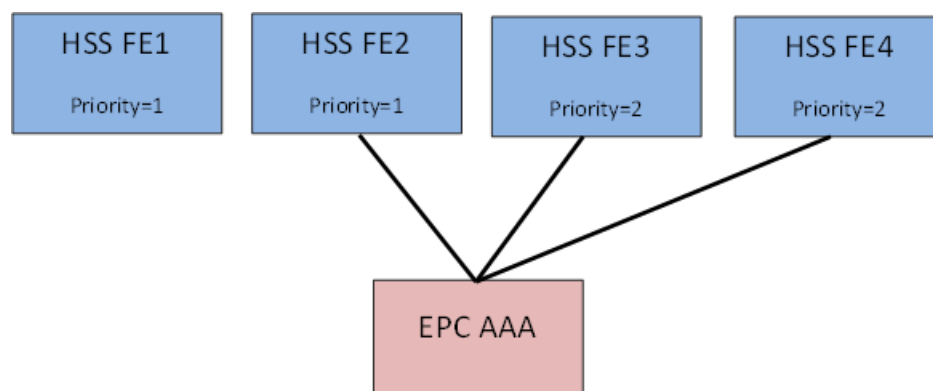


Figure 16 EPC AAA in Load-sharing Mode

For example, HSS FE1 and HSS FE2 have the same priority 1; HSS FE3 and HSS FE4 have the same priority 2. The EPC AAA server distributes the load between HSS FE1 and HSS FE2. When the HSS FE1 server connection is lost, the EPC AAA server distributes all load of HSS FE2; if the HSS FE2 server connection is also lost, the EPC AAA server distributes the load between HSS FE3 and HSS FE4. Once both HSS FE1 and HSS FE2 or any one is recovered, the EPC AAA server redistributes the load HSS FE1 and/or HSS FE2.

3.3.8 EPC AAA Server Supporting DRA

The EPC AAA server supports DRA (Diameter Routing Agent) deployment. In this scenario, the diameter route must be configured.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

When the EPC AAA server sends out request, it will use destination realm and application id as the match condition to search peer in diameter route table. Matching condition follows the longest match principle.

If only one peer meets the match condition, the EPC AAA server will send the request message to that peer. If two or more peers meet the match condition, the EPC AAA server will use failover or load-sharing strategy to select an active peer from the matched peers to send the request.

3.3.8.1 EPC AAA Server Supporting Network Architecture by Using DRA

The EPC AAA server supports three deployments with surrounding nodes:

1. Direct connection
2. Deployment with DRA
3. Hybrid deployment with DRA

In this section, it only describes the deployment with DRA or Hybrid deployment with DRA.

3.3.8.1.1 Deployment with DRA

In this EPC network architecture, all the interfaces use the same DRA as shown in Figure 16.

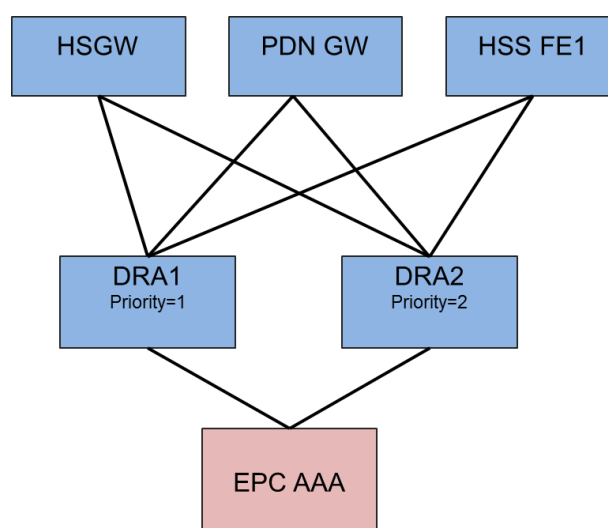


Figure 17 Deployment with DRA

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

For example, the interface SWx (HSS), S6b (PDN GW), and STa (HSGW) use the same DRA (DRA1 and DRA2). All requests that EPC AAA send to HSS, PDN GW, and HSGW are routed by DRA1 and DRA2. DRA1 and DRA2 are failover (the priority of DRA1 and DRA2 is 1 and 2 respectively).

3.3.8.1.2 Hybrid Deployment with DRA

In Figure 18, some interfaces use DRA while some interfaces do not use in this EPC network architecture.

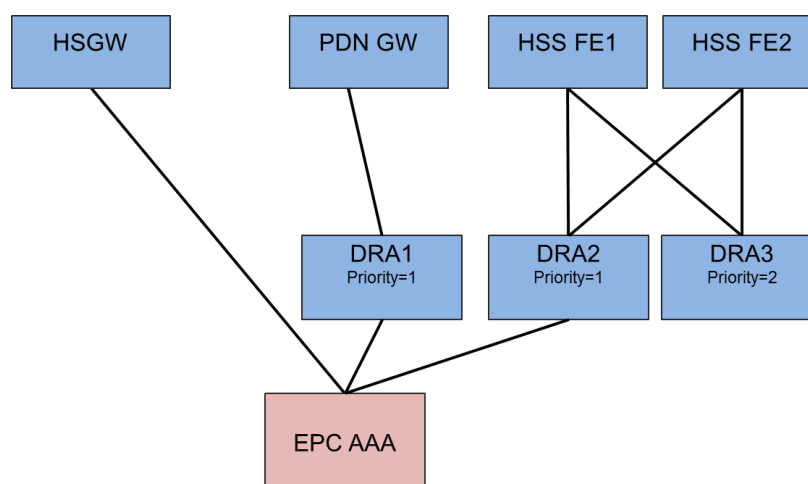


Figure 18 Hybrid Deployment with DRA

For example, the interface SWx (HSS) and S6b (PDN GW) use different DRA. The interface STa (HSGW) does not use DRA.

The request that EPC AAA sends to HSS is routed by DRA2 and DRA3, DRA2 and DRA3 is failover (the priority of DRA2 and DRA3 is 1 and 2 respectively). The request that EPC AAA sends to PDN GW is routed by DRA1, the message that EPC AAA sends to HSGW is directly sent to HSGW.

3.3.8.2 DRA Redundancy Mode

The redundancy is either in failover mode or load-sharing mode, which depends on the way to configure the DRA information to the diameter route. For the detailed configuration, refer to *Section Configuring Diameter Route in Diameter Stack Configuration Guide* [2].

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

3.3.8.2.1 Failover Mode

In the failover mode, the EPC AAA server selects highest priority and available DRA to send request based on user messages. Failover happens when the connection to the DRA with highest priority is lost as shown in Figure 18.

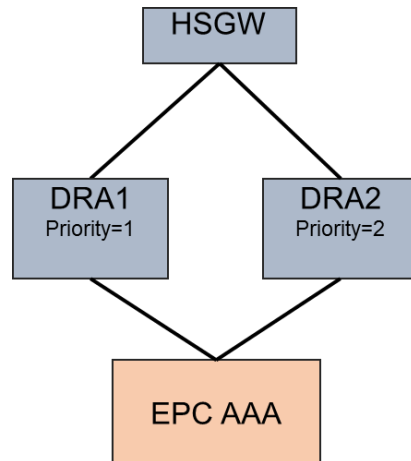


Figure 19 EPC AAA in Failover Mode with DRA

For example, HSGW uses DRA1 and DRA2, the priority of DRA1 and DRA 2 is 1 and 2 respectively in the failover mode. When DRA1 connection is lost, the EPC AAA server sends all requests to DRA2. If DRA1 connection is recovered, the EPC AAA server sends all requests back to DRA1.

3.3.8.2.2 Load-sharing Mode

In the load-sharing mode, the EPC AAA server distributes the load based on user messages among the active connection of the DRA as shown in Figure 19.

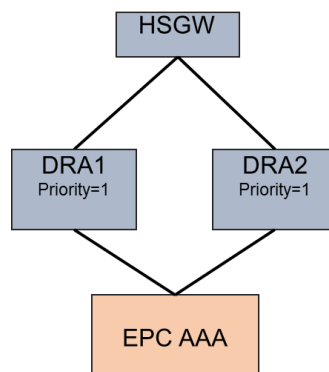


Figure 20 EPC AAA in load-sharing Mode with DRA

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

For example, the HSGW uses DRA1 and DRA2, DRA1 and DRA2 have the same priority 1. The EPC AAA server distributes the load between DRA1 and DRA2.

When the DRA1 server connection is lost, the EPC AAA server distributes all load of DRA2. Once DRA1 is recovered, the EPC AAA server redistributes the load between DRA1 and DRA2.

3.3.9 Overload Protection for EPC AAA

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. The following table shows the capacity of EPC AAA server in overload status:

Incoming traffic load	The capacity / engineered capacity
1 * engineered capacity	100%
2 * engineered capacity	95%
3 * engineered capacity	85%

3.3.9.1 Overload Detection

In IPWorks Radius AAA server, the incoming traffic messages are buffered in the message queue. The working threads use non-blocking way putting message to queue, if queue is full, put message fail, EPC AAA server is overload.

When the incoming traffic load on EPC AAA server is below its engineered capacity, the length of message queue is very short because all messages to be processed are handled by the working threads. But when the load exceeds the engineered capacity, the message queue accumulates. If the message queue is full, it triggers the Overload Control mechanism.

3.3.9.2 Overload Control

In IPWorks EPC AAA server, the incoming traffic messages are sorted to two message queues. The working engine threads will be also sorted to two groups, one group with low priority and less resources(threads), small buffer size for handling initial EAP-Identity DER(we call it DER work engine group), another group with high priority and large buffer size for all other messages (for example, DER AKA-challenge..., STR/ASA/AAR/RAA).

When the EAP- Identity DER queue is full, EPC AAA server stops handling the initial DER (containing EAP-IDENTITY) by replying Result-Code "DIAMETER_TOO_BUSY". And the requests for ongoing sessions and active sessions are handled normally.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

Note:

In theory, if we control the DER message queue handling well, the high priority Queue are full. However, in case the high priority queue is full, server handles the message in two different modes. For the Request message, include DER, STR, AAR, AAA server replies Result-Code "DIAMETER_TOO_BUSY", for the response message, include ASA, RAA, the thread is hang until the message is put into the queue.

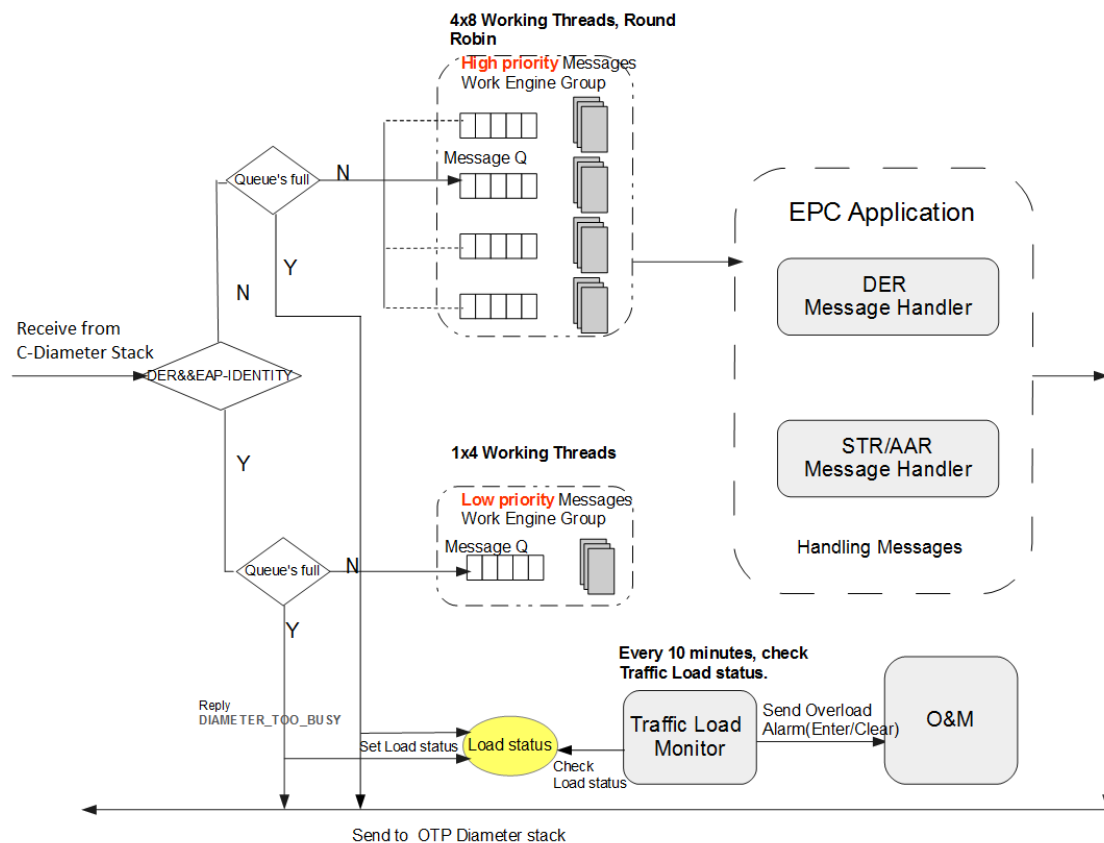


Figure 21 Protection Mechanism

- First, IPWorks EPC AAA server receives Diameter messages from C-Diameter Stack, and put them in the message queue. If message queue is full, C-Diameter Stack directly replies Result-Code "DIAMETER_TOO_BUSY" in its callback routine.
- Then, EPC Application module always gets all messages existed in message queue, and handle it as usual.

3.3.10 S6b Authentication without Profile (Optional)

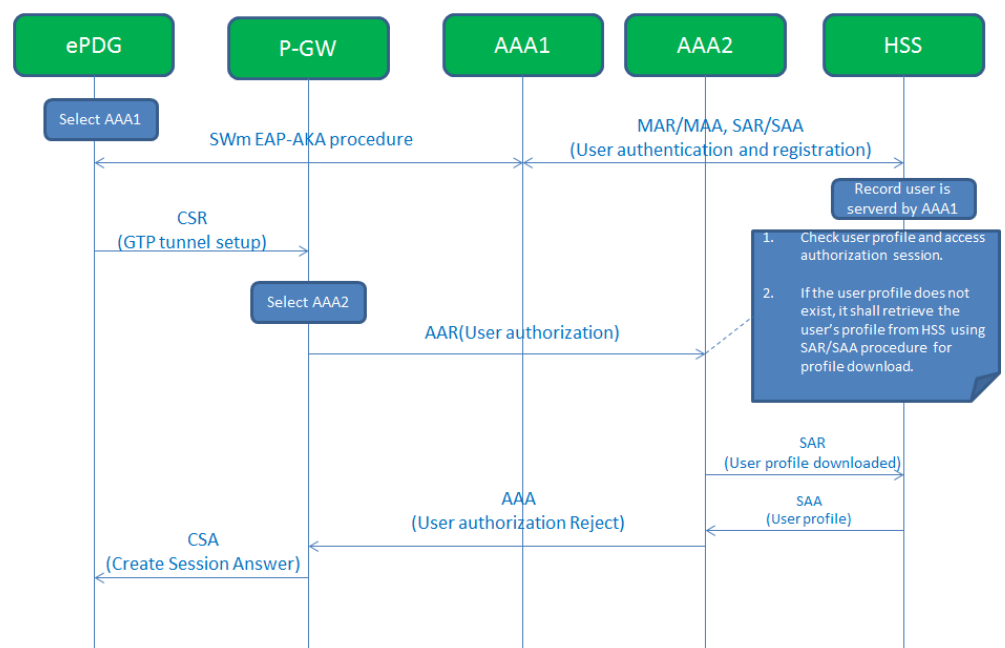
This section introduces the S6b authorization without user profile function.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

When AAA Server receives the Authorization Request from PDN GW, AAA Server must check whether the user profile is available. If the user profile does not exist in AAA Server, AAA Server retrieves the user profile from HSS. After that, the AAA Server handles the authentication procedure according to the different configuration as following:

- The function is configured as **disabled**.

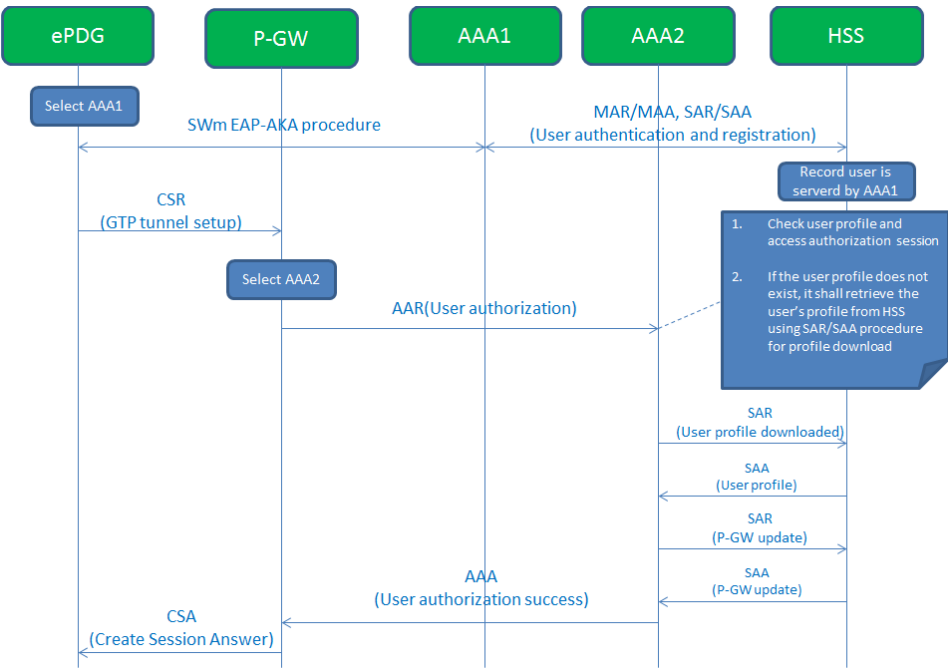
The authorization is rejected by setting the Result-Code to DIAMETER_AUTHORIZATION_REJECTED. It means that the user has no active access authorization procedure which is considered as an error situation.



- The function is configured as **enabled**.

The authorization procedure is continued just as the user profile exists in AAA server.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference



4 AAA for Trusted Non-3GPP IP Access Networks Interworking with EPC

The section describes the Trusted Non-3GPP IP access networks to access EPC scenario implemented by IPWorks AAA server.

4.1 Overview

IPWorks EPC AAA server is used in EPC network as the 3GPP AAA server to do the authentication, authorization and accounting works for users who want to access the EPC through the trusted Non-3GPP IP Access Network, such as CDMA2000 HSGW.

In EPC network, the IPWorks AAA server connects to three network elements: HSS, PDN GW, and HSGW. The AAA server connects to HSGW through STa interface, connects to PDN GW through S6b interface, and connects to the HSS through SWx interface. The network architecture is described in Figure 21.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

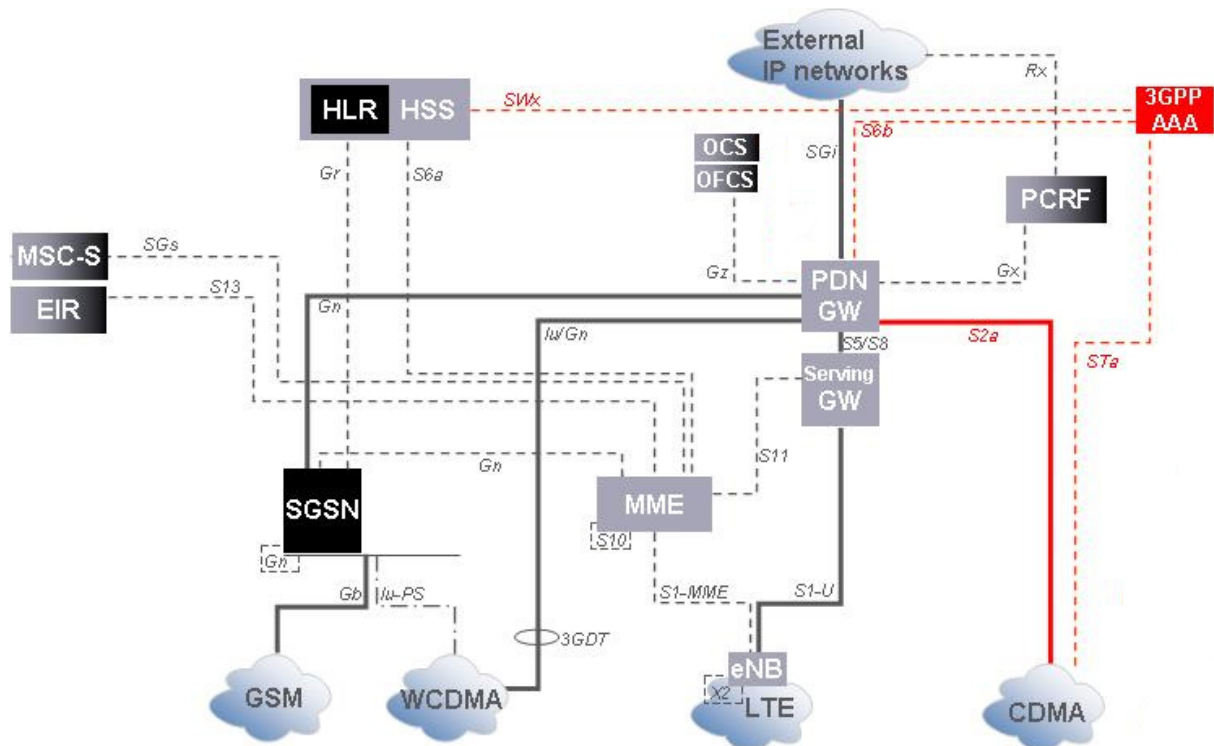


Figure 22 Trusted Non-3GPP IP Access Networks to Access the EPC

When the user starts the initial attach process with PMIPv6 on s2a interface, it first triggers the authentication and authorization process in STa interface to the 3GPP AAA server. The authentication use EAP-AKA' as authentication method which requires the authentication vector from HSS. After the authentication is successful, user profile is downloaded from the HSS which is used to authorize the user. When the Non-3GPP Access GW connects to the PDN GW and send the Proxy-Binding-Update message to PDN GW, the PDN GW will update the PDN GW identity and APN corresponding to UE's PDN connection to 3GPP AAA server, which updates the information to HSS.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

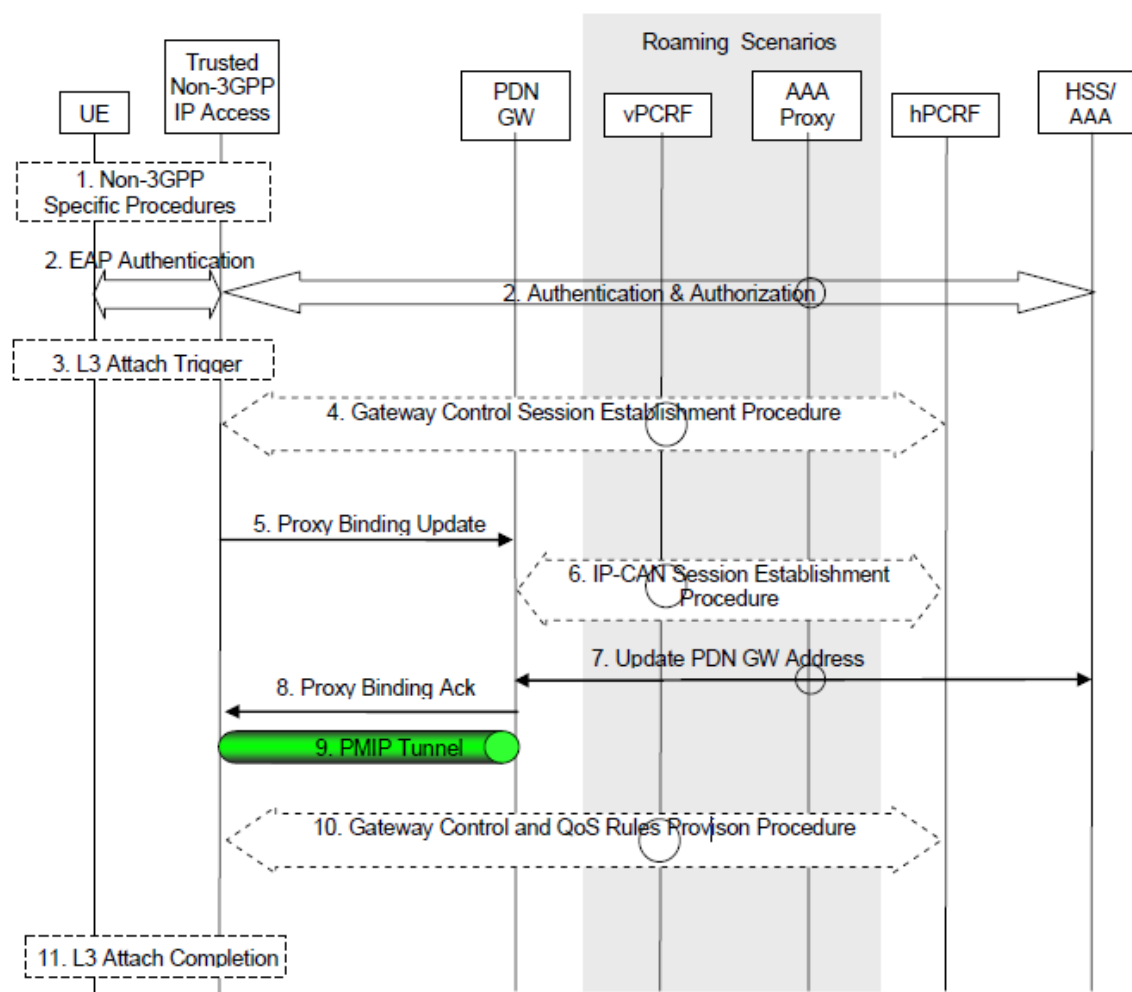


Figure 23 Initial Attachment with Network-based Mobility Management (MM) Mechanism over S2a

The following sections describe the concrete protocol functions implemented by EPC AAA server. But the description only cares about main function implemented; the detail degree of implementation and the limitation are referred to the document of IWD and SoC.

4.2 Non-3GPP IP Access Network Initiated Authentication and Authorization

The procedure is triggered when the UE attaches to the EPC using the s2a reference point. The authentication is based on EAP-AKA'. The Diameter message is DER and DEA. During the procedure of authentication and authorization, the AAA server fetches the authentication vector and user profile from HSS. After the authentication and authorization is successful, the AAA server does the registration in HSS.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

If the 3GPP AAA Server receives a request message not related to any existing session and recognizes that the AAA-Failure-Indication AVP is included in the request message, the 3GPP AAA Server will include the AAA-Failure-Indication AVP over the SWx interface while retrieving the access authentication and authorization data from the HSS.

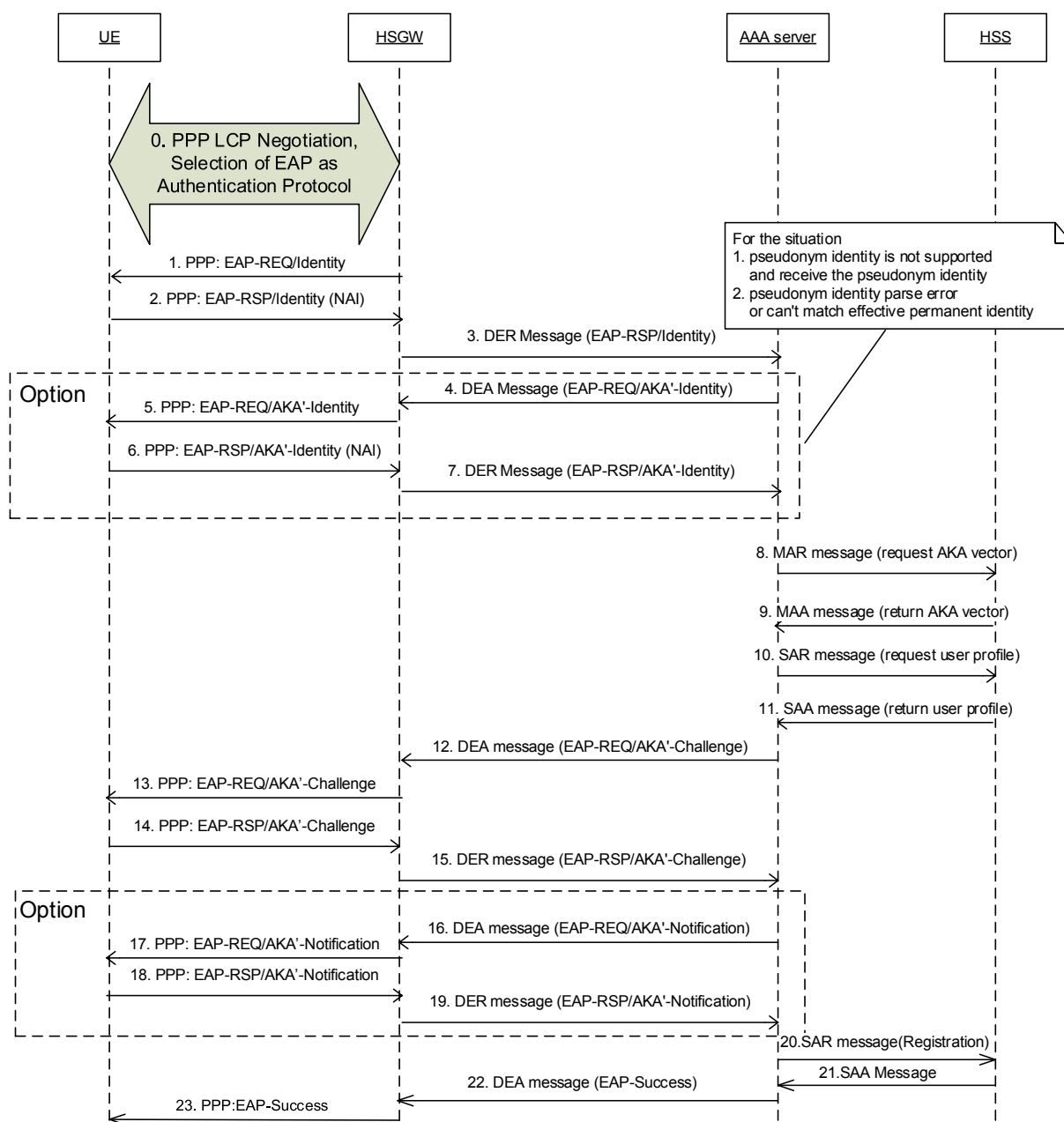


Figure 24 STa Authentication and Authorization using EAP-AKA' Full Authentication

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

4.3 Non-3GPP IP Access Network Initiated Re-Authentication and Re-Authorization

The procedure is triggered when the Trusted Non-3GPP IP Access Network wants to do the re-authentication and re-authorization according to local policy.

The re-authentication procedure can use both the normal EAP-AKA' full authentication (refer to section 4.2) and EAP-AKA' fast re-authentication, IPWorks takes the authentication request which has the same session-id with one existed STa session as re-authentication request and check the related AVP value should be match with the existed session.

The Re-authentication and Re-Authorization procedure can also be triggered by HSS (not implemented yet).

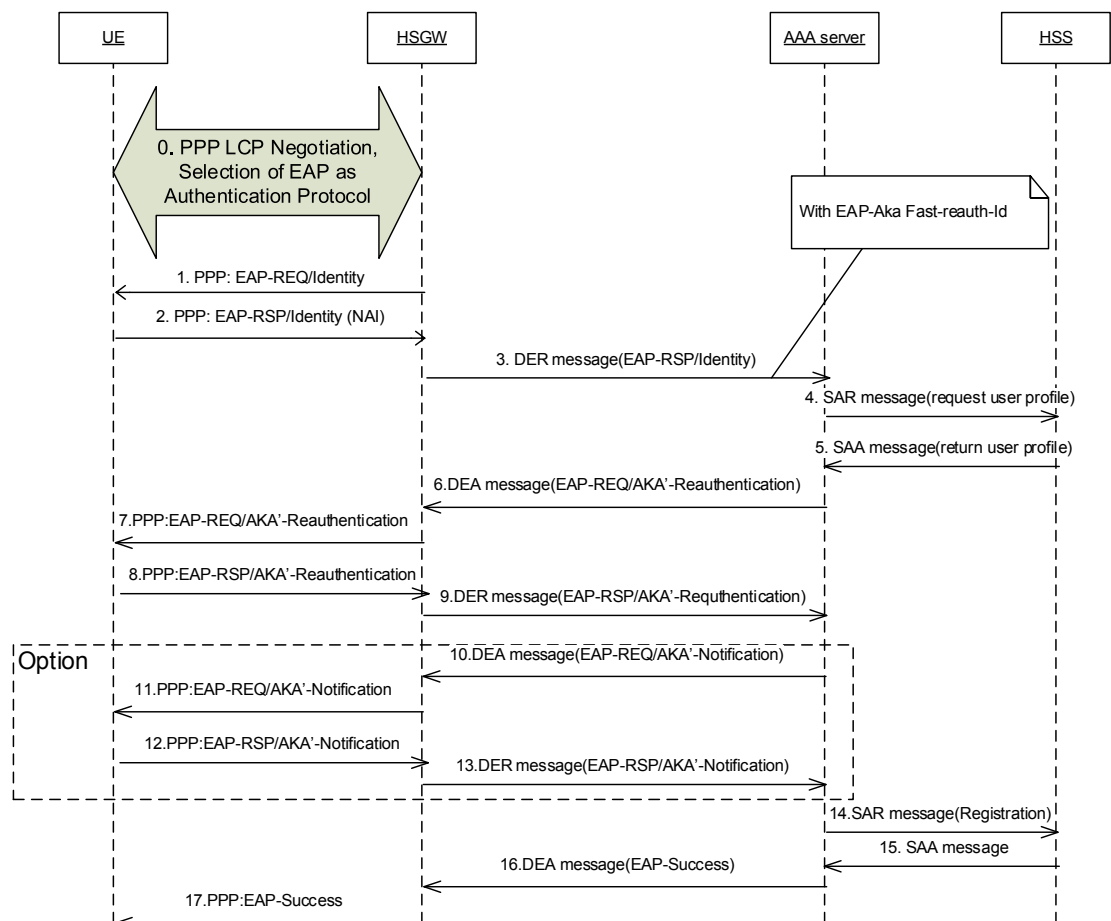


Figure 25 STa Re-Authentication and Authorization Using EAP-AKA' Fast-Reauthentication

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

4.4 Non-3GPP IP Access Network Initiated Re-Authorization

The procedure is triggered by the Trusted Non-3GPP IP Access Network for check if there is any modification in the user authorization parameters previously provided by the 3GPP AAA server.

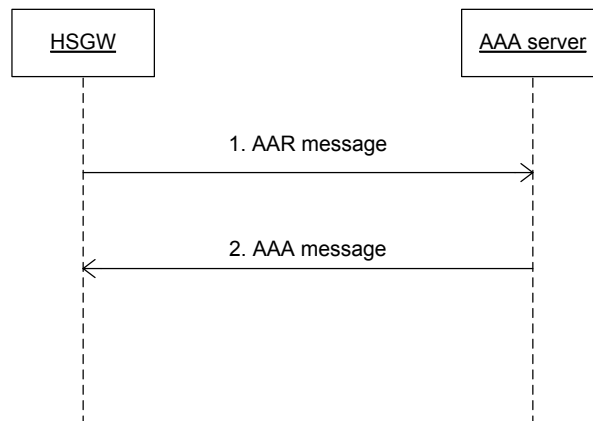


Figure 26 Non-3GPP IP Access Network Initiated Re-Authorization

4.5 Non-3GPP IP Access Network Initiated Session Termination

This procedure is triggered when the user connection is to be released, the Non-3GPP IP Access Network informs the 3GPP AAA server to remove Non-3GPP access information. After receive the session termination message the AAA server will do deregistration in HSS and delete the local STa session related.

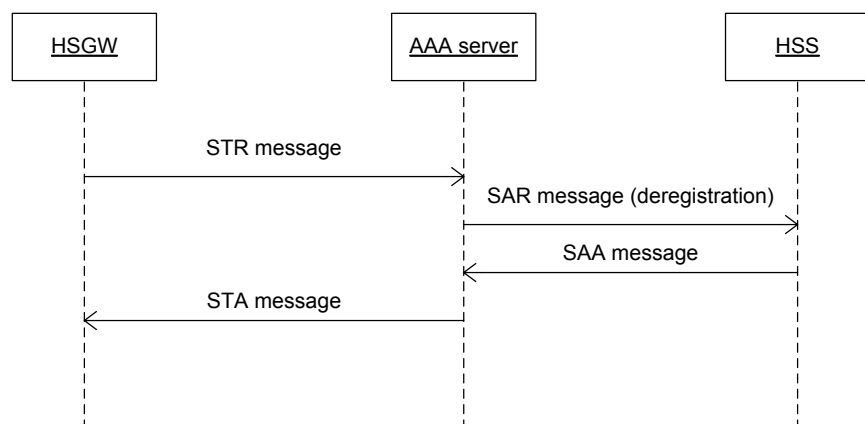


Figure 27 Non-3GPP IP Access Network Initiated Session Termination

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

4.6 AAA Server Initiated Session Termination on STa Interface

This procedure is triggered when the system administrator wants to detach the user from the 3GPP AAA server. The procedure is based on Diameter session abort messages. In EPC AAA server, the user can abort a STa session using CLI which triggers the ASR message sent to the HSGW, when HSGW receive the message it sends the STR message to AAA server to terminate the session, then the AAA server does the deregistration in HSS and deletes local STa session.

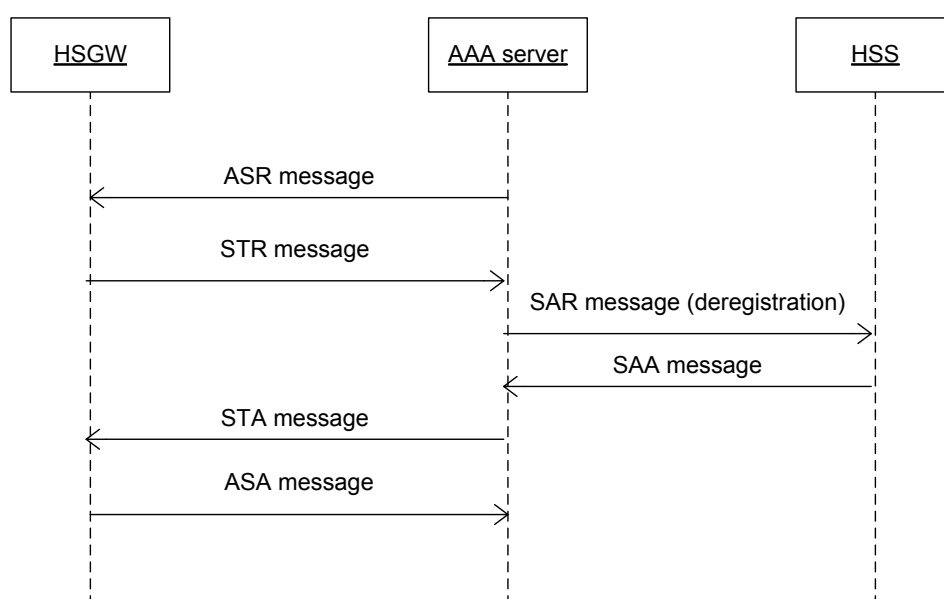


Figure 28 AAA Server Initiated Session Termination on STa Interface

4.7 PDN GW Initiated Authorization Procedure

This procedure is triggered when the PDN GW receives a PBU message from the MAG, the PDN GW initiates an authorization procedure by sending an Authorization Request message to the 3GPP AAA server, to update the PGW Address for the APN, as well as to download any UE-specific APN profile information.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

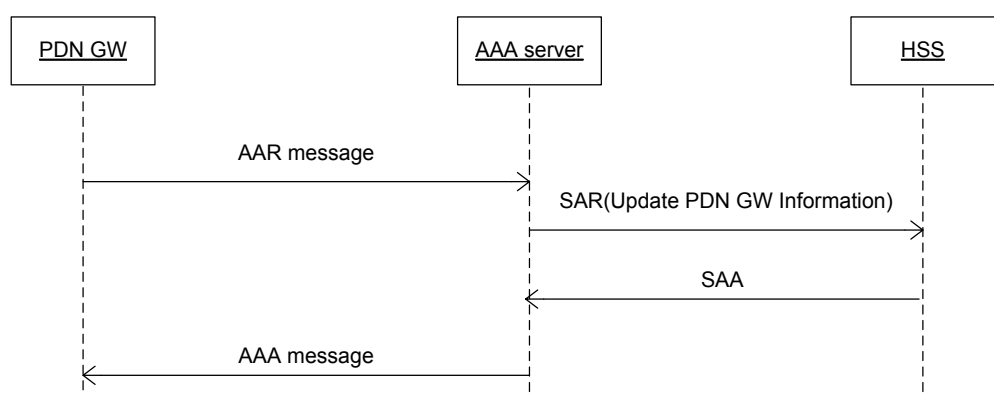


Figure 29 PDN GW Initiated Authorization Procedure

4.8 PDN GW Initiated Session Termination Procedure

This procedure is triggered by PDN GW when the UE disconnect a PDN connection associated to an APN. When receiving the session termination message, the AAA server will delete related local S6b session.

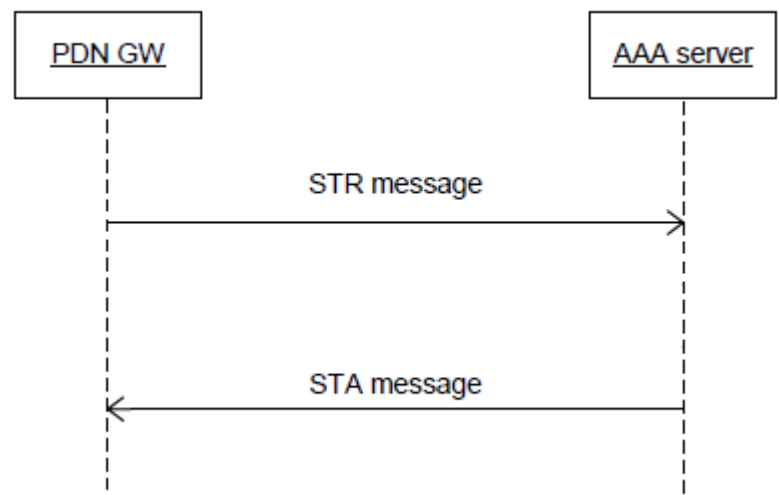


Figure 30 PDN GW Initiated Session Termination Procedure

4.9 Network Initiated De-Registration by HSS

This procedure is triggered by HSS to remove a previous registration and all associated state. When the de-registration procedure is initiated by HSS, indicating that a subscription has to be removed, the 3GPP AAA Server subsequently triggers the detach procedure via the STa interface.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

The HSS shall send the Deregistration-Reason AVP indicating the reason for the de-registration, the possible reason codes are listed as follow:

- **NEW_SERVER_ASSIGNED:** The HSS indicates to the AAA Server that a new AAA Server has been allocated to the user. The AAA Server shall not send ASR message to HSGW.
- **PERMANENT_TERMINATION:** The Non-3GPP subscription or service profile(s) has been permanently terminated. AAA Server should clean up user data and related sessions from local repository, and send ASR to HSGW for the active session. STR message is not required in this case, so the Auth-Session-State AVP in ASR message is set to the value NO_STATE_MAINTAINED.

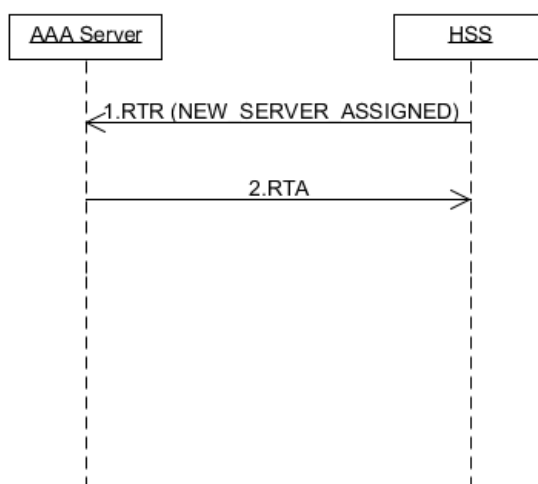


Figure 31 De-Registration with Reason Code NEW_SERVER_ASSIGNED

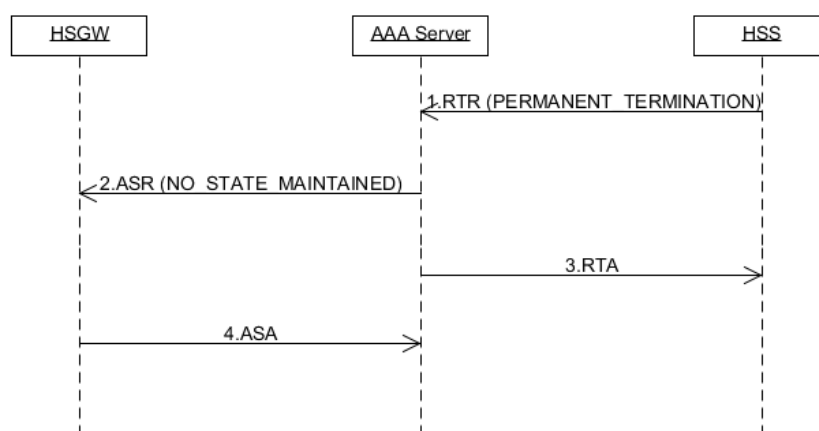


Figure 32 De-Registration with Reason Code PERMANENT_TERMINATION

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

4.10 HSS Initiated Update of User Profile

The procedure is invoked by the HSS in the following case:

- Indication to AAA Server of change of non-3GPP subscriber profile within HSS. AAA Server shall update user profile in local repository, and then send RAR to HSGW with the Re-Auth-Request-Type AVP set to AUTHORIZE_ONLY. AAA Server shall also send RAR to PDN GW if the "Support RAR in S6b" feature is enabled.

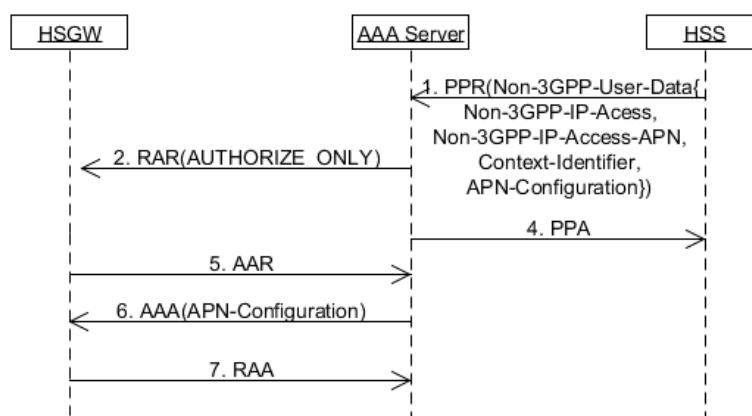


Figure 33 SS Initiated Update of User Profile

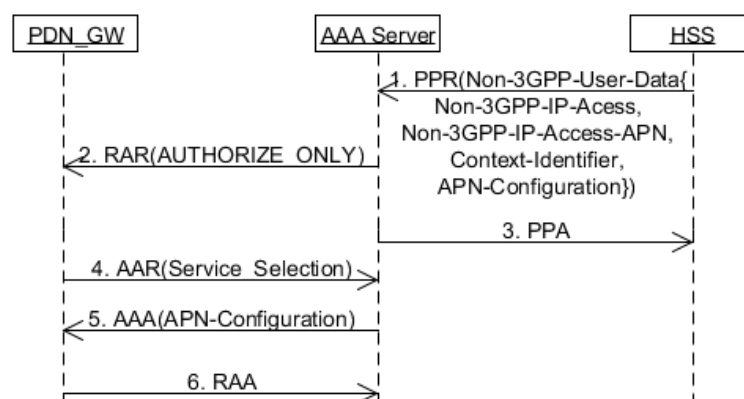


Figure 34 HSS Initiated Update of User Profile with Supporting RAR in S6b

4.11 HSS Initiated P-CSCF Restoration

If there is a stored information that IMS PDN connection is established via a WLAN access, with checking that the PGW supports the HSS-based P-CSCF restoration for WLAN, the 3GPP AAA Server must send a P-CSCF restoration indication to the PGW over S6b in a RAR command.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

- For the basic P-CSCF restoration mechanism, the PDN GW must send a Session Termination Request to the 3GPP AAA Server.

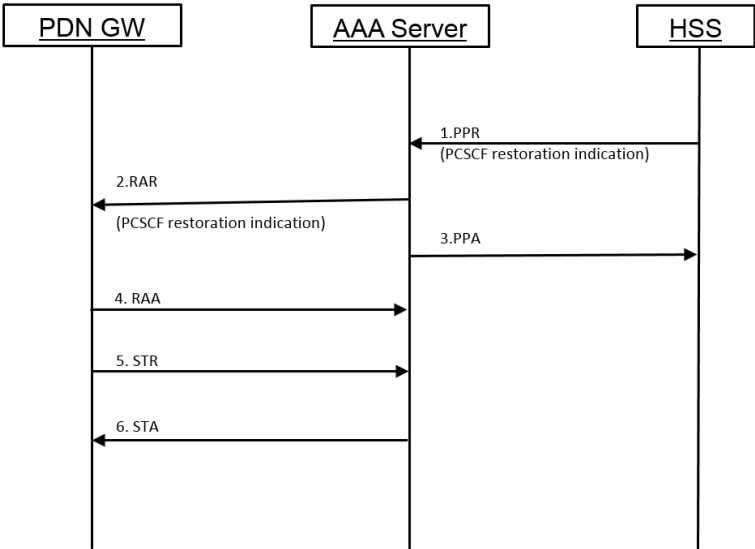


Figure 35 Basic P-CSCF Restoration Mechanism

- For the extended P-CSCF restoration mechanism, the PDN GW might send the authorization request with only mandatory AVPs.

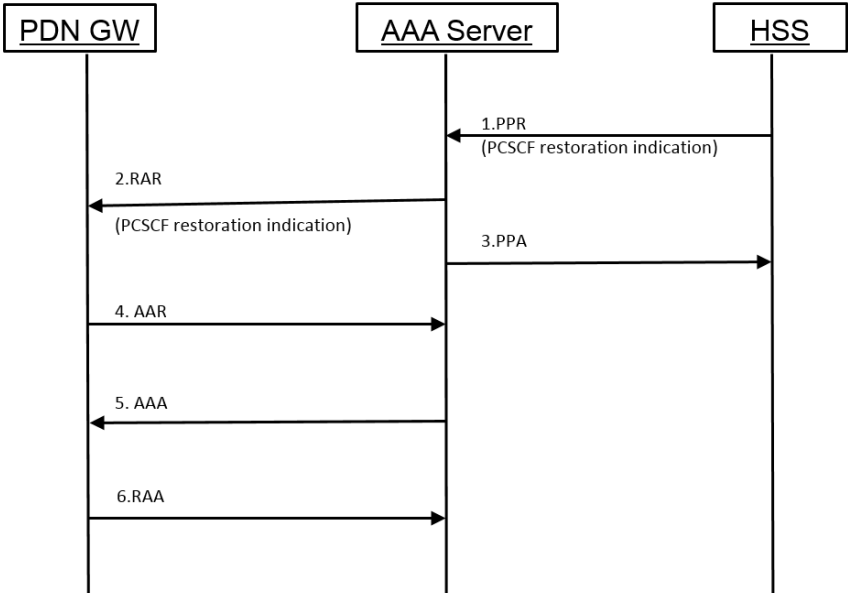


Figure 36 Extended P-CSCF Restoration Mechanism

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

5 AAA for Untrusted Non-3GPP IP Access Networks Interworking with EPC

The section describes the Untrusted Non-3GPP IP access EPC network scenario and other customized scenarios implemented by IPWorks AAA server.

5.1 Overview

This access scenario is based on 3GPP spec TS23.402 with the introduction of the evolved Packet Data Gateway (ePDG) node. It requires an EAP client in the device with IPsec support. No impact on the Wi-Fi core or Wi-Fi RAN, legacy Wi-Fi hotspot networks work. IPsec tunnels are terminated in the ePDG - a new mobile core node introduced for this purpose. The ePDG maps the IPsec tunnels into GTP or PMIP tunnels terminated in the Packet Gateway P-GW.

The SWm interface is used for additional authentication parameters including subscription profiles and S2b option selection (which tunnel type to use). The S6b interface is used between IPWorks AAA server and P-GW for tunnel authentication, static QoS, and mobility (if applicable), etc.

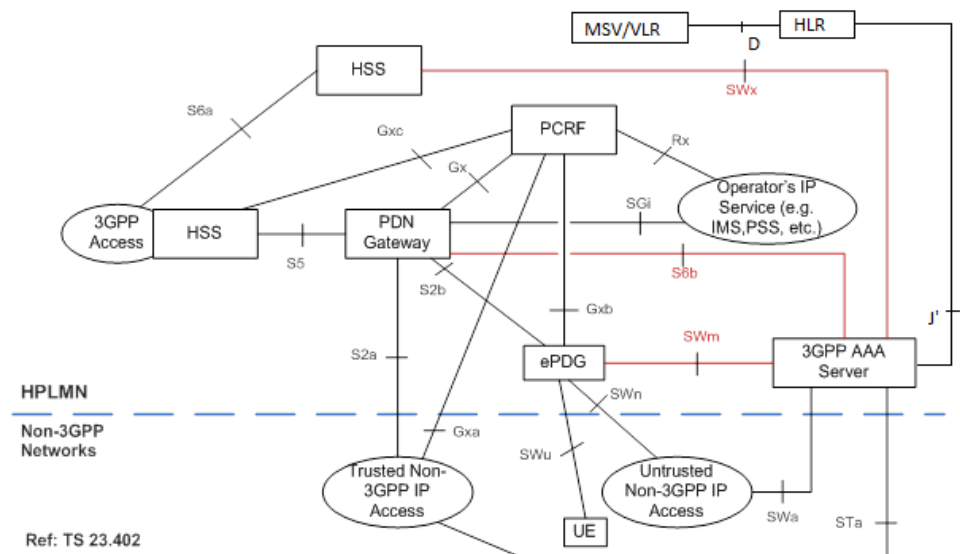


Figure 37 Untrusted Non-3GPP IP Access Networks to Access the EPC

When the user starts the initial attach process with GTP on s2b interface, it will first trigger the authentication and authorization process in SWm interface to the 3GPP AAA server. The authentication use EAP-AKA/AKA' as authentication method which required the authentication vector from HSS, or use EAP-TLS as authentication method. These two authentication methods are selected according to the prefix string in EAP-Response/Identity.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

- For SIM user, 3GPP AAA server provides the authentication service with EAP-AKA and EAP-AKA' authentication method. After the authentication is successful, user profile is downloaded from the HSS which is used to authorize the user. Some additional information is returned as part of the reply from IPWorks AAA server to the ePDG, include the PDN GW information, APN-AMBR, static QoS Profile and Trace Information if applicable.
- For Non-SIM user, 3GPP AAA server provides the authentication service with EAP-TLS authentication method. The user profile and authentication parameter are provisioned and managed by IPWorks in whole traffic lifecycle. In addition, CRL (Certificate Revocation List) for this scenario is uploaded by the SFTP service and 3GPP AAA server will dynamically load this CRL.

Then ePDG sends a Create Session Request message to the PGW, the PGW updates the PDG GW identity and APN corresponding to UE's PDN connection to 3GPP AAA server, which updates the information to HSS.

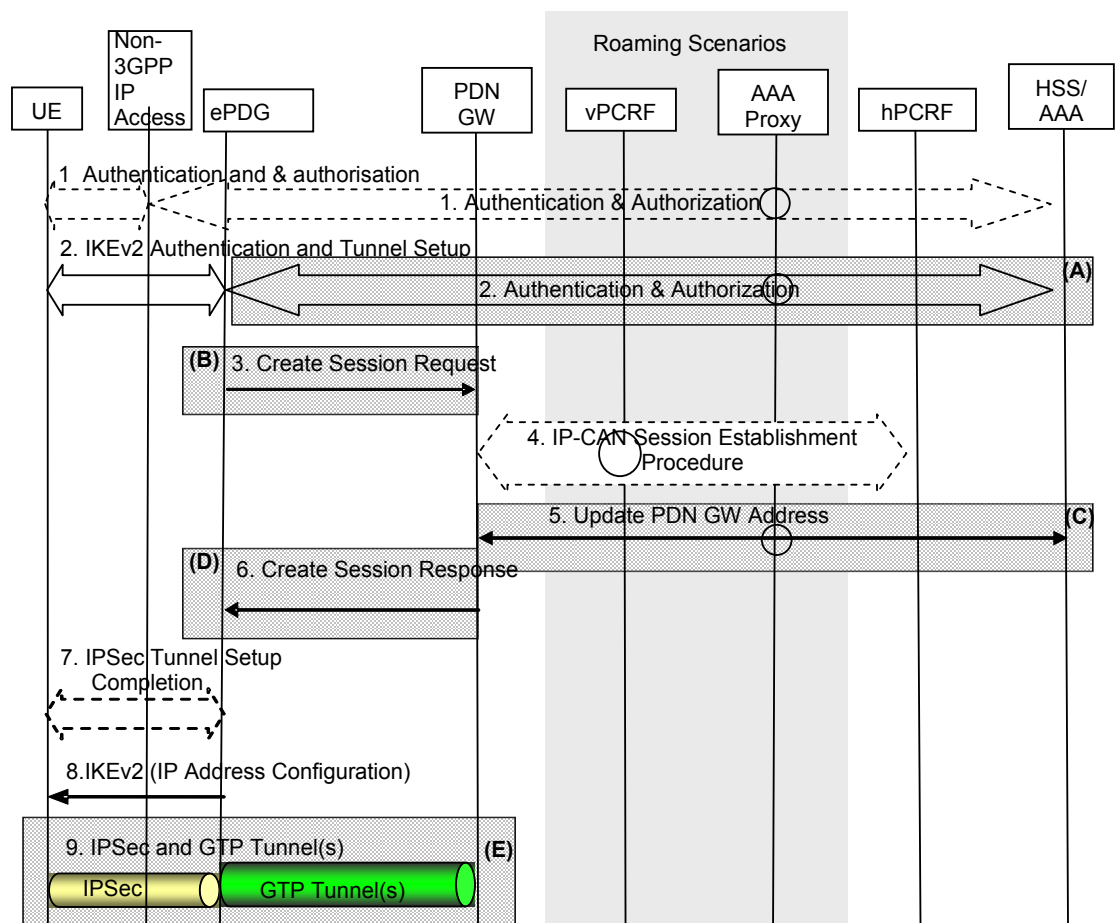


Figure 38 Initial Attachment over GTP Based S2b

Other customized access scenarios implemented by IPWorks AAA:

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

- Authentication for users want to access SES, refer to section 5.12 SES Support

5.2 ePDG Initiated Full Authentication and Authorization

This procedure is used between the ePDG and IPWorks EPC AAA server when the UE attaches to the EPC-based S2b interface.

The procedure is triggered when the UE attaches to the EPC using the s2b reference point. The authentication and authorization based on the reuse of the DER/DEA command. The traffic procedure for EAP-AKA and EAP-TLS are shown in below figure.

If the 3GPP AAA Server receives a request message not related to any existing session and recognizes that the `AAA-Failure-Indication` AVP is included in the request message, the 3GPP AAA Server will include the `AAA-Failure-Indication` AVP over the SWx interface while retrieving the access authentication and authorization data from the HSS.

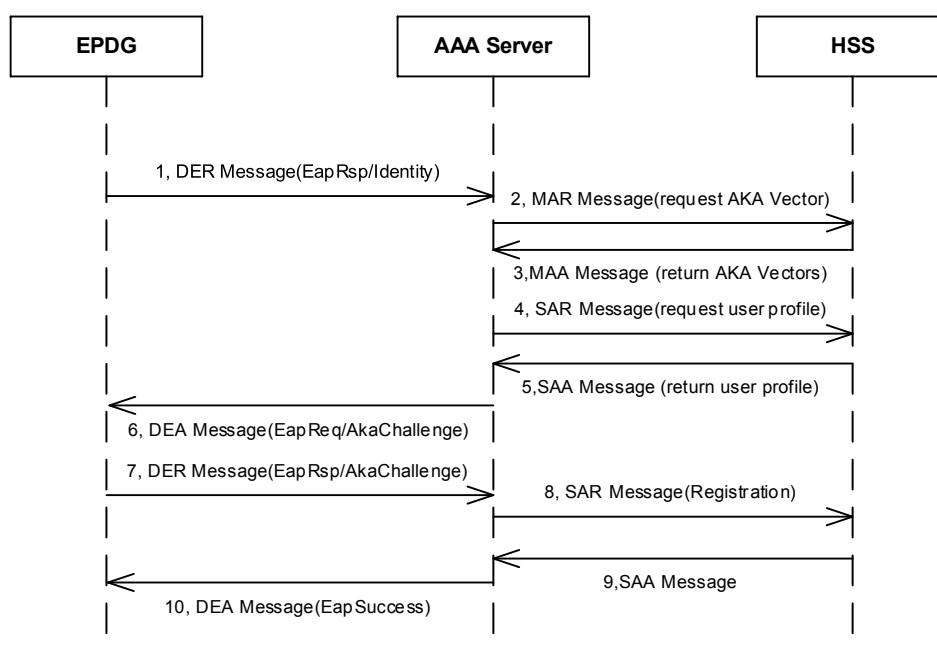


Figure 39 SWm Authentication and Authorization Using EAP-AKA Full Authentication

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

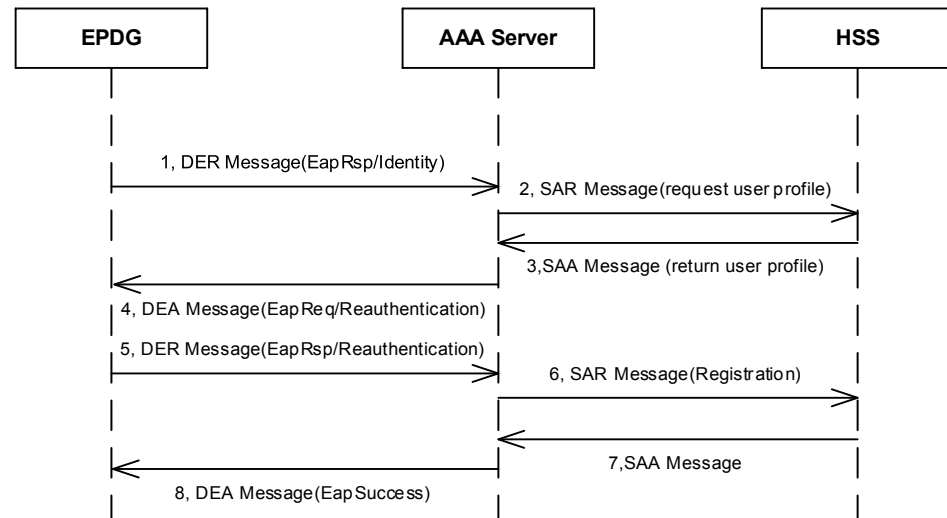


Figure 40 SWm Authentication and Authorization Using EAP-AKA Full Authentication

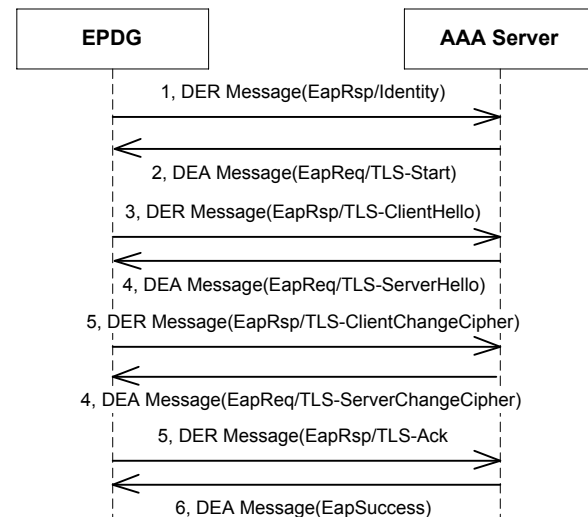


Figure 41 SWm+ Authentication and Authorization Using EAP-TLS Full Authentication

5.2.1 IMSI Mask Handling Support for SWm+ Interface and SWm Interface

This feature IMSI Mask Handling is a customized feature which can be enabled by configuration.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

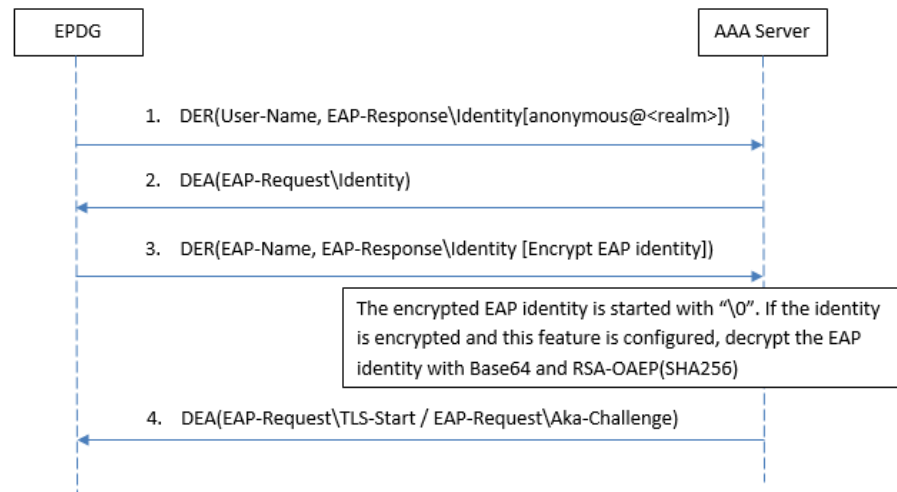


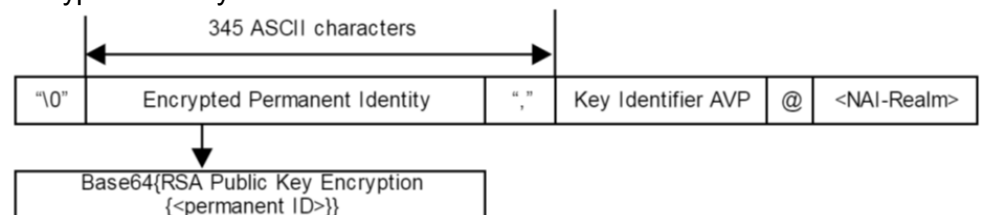
Figure 39 ePDG Initiated Anonymous and IMSI Mask Authentication and Authorization Process

For non-SIM UE and SIM UE, when AAA Server received a DER message with User-Name AVP and EAP-Response\Identity is anonymous@<realm>, AAA Server must reply DEA message with EAP-Request\Identity.

When the diameter EAP DER request is sent to the IPWorks/AAA with the encrypted identity, the IPWorks/AAA will decrypt the request with Base64 and RSA OAEP(SHA256) to obtain the native identity.

The RSA algorithm needs a private key to decrypt the request which can be got from the data base.

Encrypted Identity Format:



First ASCII character:

- "\0" (ASCII NULL character) => encrypted IMSI
- "0" (ASCII value 30 hexadecimal) => EAP-AKA IMSI
- "1" (ASCII value 31 hexadecimal) => EAP-SIM IMSI
- "6" (ASCII value 36 hexadecimal) => EAP-AKA' IMSI

Note: IPWorks AAA provides a tool to manage the private key. It can import, delete, list the private keys. For more detail, refer to Configure EPC AAA, [2].

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

5.2.2 IMEI Check Support for Untrusted Non-3GPP Access

IMEI Check is a configurable feature which can be enabled/disabled via ECLI configuration.

When IPWorks AAA receives ME identity over SWm interface, the received IMEI shall be checked towards an external Equipment Identity Register Database (EIR).

If no IMEI is received, IPWorks AAA will continue or stop the authentication and authorization procedure depending on the configuration. For more information, refer to Configure EPC AAA, [2].

EIR can return the following equipment status:

- If the IMEI is in White List, IPWorks AAA will continue the authentication/authorization procedure;
- If the IMEI is in Black List, IPWorks AAA will stop the authentication/authorization procedure;
- If the IMEI is in Grey List, IPWorks AAA will continue or stop the authentication/authorization procedure depending on the configuration. The default configuration is to continue the authentication.

If ME Identity is unknown to EIR, it returns to AAA with `DIAMETER_ERROR_EQUIPMENT_UNKNOWN`. IPWorks AAA returns to ePDG with `DIAMETER_ERROR_ILLEGAL_EQUIPMENT`.

Figure 41 shows the authentication and authorization procedure with IMEI Check.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

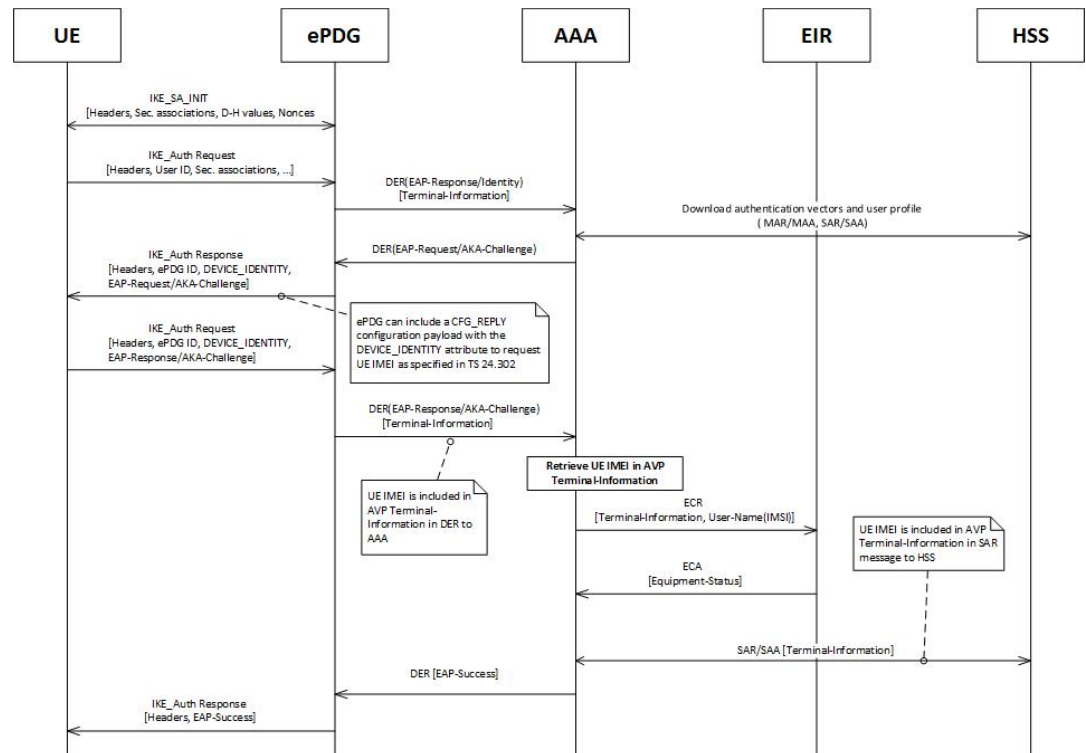


Figure 42 Authentication and Authorization Procedure with IMEI Check

5.3 ePDG Initiated Re-Authentication and Re-Authorization

The procedure is triggered when the ePDG wants to do the re-authentication and re-authorization according to local policy.

The concrete procedure of refer to Section 5.2, IPWorks takes the authentication request which has the same session-id with one existed SWm session as re-authentication request and check the related AVP value should be match with the existed session.

The Re-authentication and Re-Authorization procedure can also be triggered by HSS (not implemented yet).

5.4 ePDG Initiated Re-Authorization

The procedure is triggered by ePDG for check if there is any modification in the user authorization parameters previously provided by the 3GPP AAA server.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

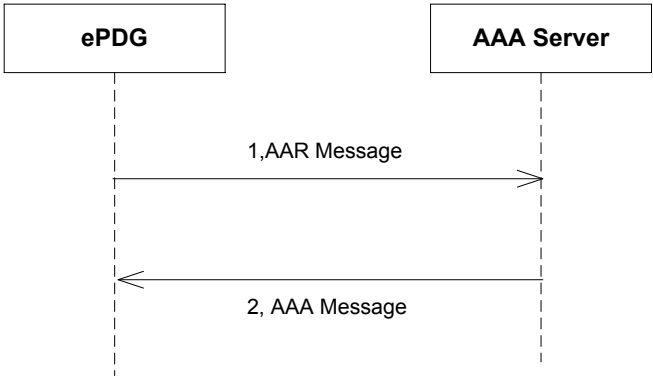


Figure 40 ePDG Initiated Re-Authorization

5.5 ePDG Initiated Session Termination

The SWm reference point allows the ePDG to inform the 3GPP AAA server about the termination of an IKE_SA between UE and ePDG, and that therefore the mobility session established on the ePDG for all associated PDN connections is to be removed.

The SWm/SWm+ Session Termination Request procedure shall be initiated by ePDG to IPWorks AAA Server which removes associated non-3GPP Access information. The AAA server then returns the SWm Session Termination Answer containing the result of the operation.

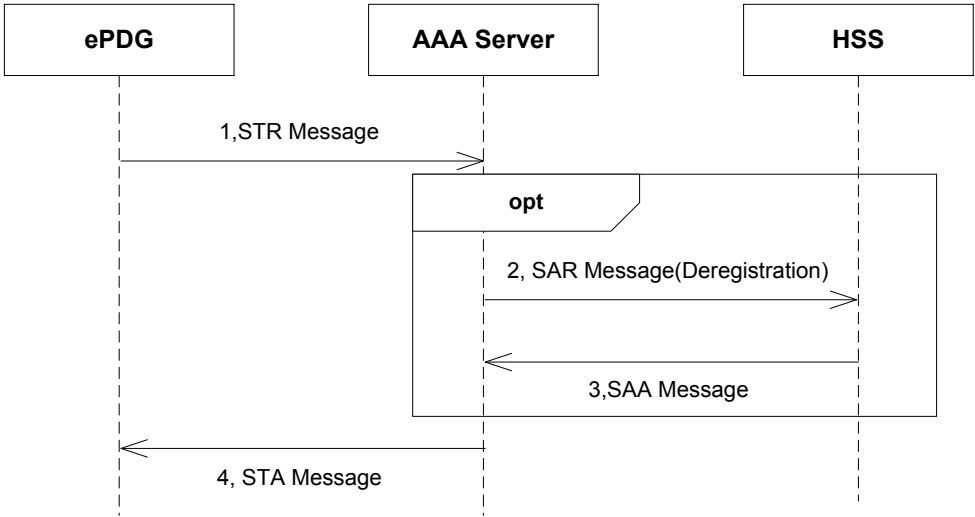


Figure 41 ePDG Initiated Session Termination for SWm sSssion

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

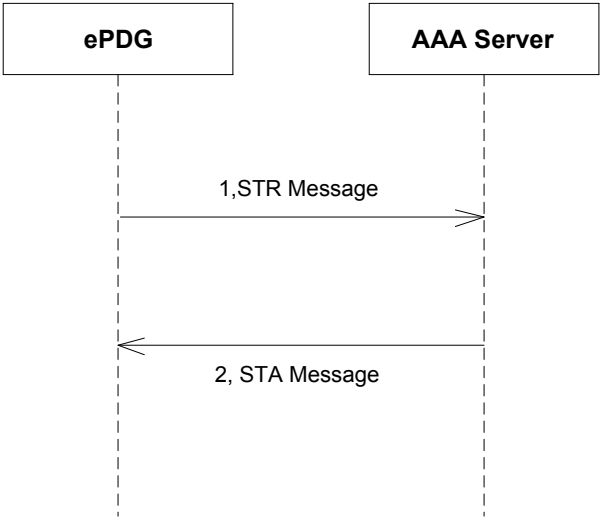


Figure 42 ePDG Initiated Session Termination for SWm+ Session

5.6 AAA Server Initiated Session Termination on SWm/SWm+ Interface

This procedure is triggered when the system administrator wants to detach the user from the 3GPP AAA server. The procedure is based on Diameter session abort messages. In EPC AAA server, the user can abort a SWm/SWm+ session using CLI which triggers the ASR message sent to the ePDG, when ePDG receive the message it sends the STR message to AAA server to terminate the session. Refer to Section 3.3.3 for more detailed information.

5.7 S6b Procedure related with SWm Session

When the UE attaches/detaches to the EPC using the S2b reference point, the S6b reference point is used to update the 3GPP AAA server with the PDN-GW address information and with the selected S2b protocol variant.

The related PDN GW initiated Authorization Procedure and Session Termination Procedure is similar with the description in Section 4.7 and 4.8.

5.8 Public Key Authentication

Non-SIM devices are supported to connect to EPC via untrusted WiFi access with authentication over SWm+ interface.

5.8.1 Authentication and Authorization over SWm+

```
sequenceDiagram
    participant EPDG
    participant AAA_Server as AAA Server
    Note over EPDG, AAA_Server: 1, DER Message(EapRsp/Identity)
    EPDG->>AAA_Server: 
    Note over EPDG, AAA_Server: 2, DEA Message(EapReq/TLS-Start)
    AAA_Server->>EPDG: 
    Note over EPDG, AAA_Server: 3, DER Message(EapRsp/TLS-ClientHello)
    EPDG->>AAA_Server: 
    Note over EPDG, AAA_Server: 4, DEA Message(EapReq/TLS-ServerHello)
    AAA_Server->>EPDG: 
    Note over EPDG, AAA_Server: 5, DER Message(EapRsp/TLS-ClientChangeCipher)
    EPDG->>AAA_Server: 
    Note over EPDG, AAA_Server: 4, DEA Message(EapReq/TLS-ServerChangeCipher)
    AAA_Server->>EPDG: 
    Note over EPDG, AAA_Server: 5, DER Message(EapRsp/TLS-Ack)
    EPDG->>AAA_Server: 
    Note over EPDG, AAA_Server: 6, DEA Message(EapSuccess)
    AAA_Server->>EPDG: 
```

Figure 44 SWm+ Authentication and Authorization using EAP-TLS Full Authentication

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

5.8.2 User Profile and Certificate Management for Non-SIM user

In Non-SIM Solution, the user profile and authentication parameter are need to be provisioned by the IPWorks CLI interface before the real traffic starting. The operators can create, delete and modify user profile by IPWorks CLI.

3GPP AAA server uses EAP-TLS, which is the certificate based authentication method, to authenticate Non-SIM user. The ca certificate and server certificate need to be pre-configured.

5.8.3 Support of AAA FE (PKI)

In Non-SIM solution, the user profile can also be stored in CUDB.

3GPP AAA server uses LDAP to access to CUDB data.

For detailed information, refer to *IPWorks AAA Front End Function Overview* [4].

5.8.4 Certificate ID Checking

IPWorks AAA supports checking certificate revocation status by binding certificate ID and issuer name with user profile.

To revoke the certificate for a user, the operator should set the corresponding ID as voided in user profile through CLI.

During the EAP-TLS authentication process, AAA will check the certificate ID and issuer name with the corresponding information in user profile. Any inconsistency will result in authentication failure for the non-SIM device.

5.8.5 OCSP Checking

IPWorks AAA supports OCSP (Online Certificate Status Protocol) interface to obtain timely information regarding the revocation status of certificate. The OCSP enables AAA to determine the revocation state of identified certificates. During the authentication procedure, IPWorks AAA issues a status request to an OCSP responder and suspends acceptance of the certificates in question until the responder provides a response.

If the response is `good`, the authentication will succeed.

If the response is `revoked` or `unknown`, the authentication will fail.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

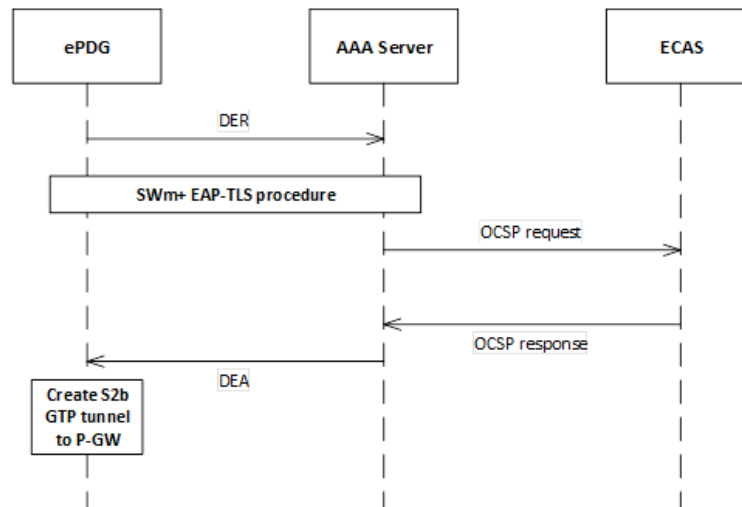


Figure 45 OCSF Checking Procedure

5.9 Network Initiated De-Registration by HSS

This procedure is triggered by HSS to remove a previous registration and all associated state. When the de-registration procedure is initiated by HSS, indicating that a subscription has to be removed, AAA Server subsequently triggers the detach procedure via the SWm interface.

The HSS shall send the Deregistration-Reason AVP indicating the reason for the de-registration, the possible reason codes are listed as follow:

- **NEW_SERVER_ASSIGNED:** The HSS indicates to the AAA Server that a new AAA Server has been allocated to the user. The AAA Server shall not send ASR message to ePDG.
- **PERMANENT_TERMINATION:** The Non-3GPP subscription or service profile(s) has been permanently terminated. AAA Server should clean up user data and related sessions from local repository, and send ASR to ePDG for each active session. STR message is not required in this case, so the Auth-Session-State AVP in ASR message is set to the value **NO_STATE_MAINTAINED**.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

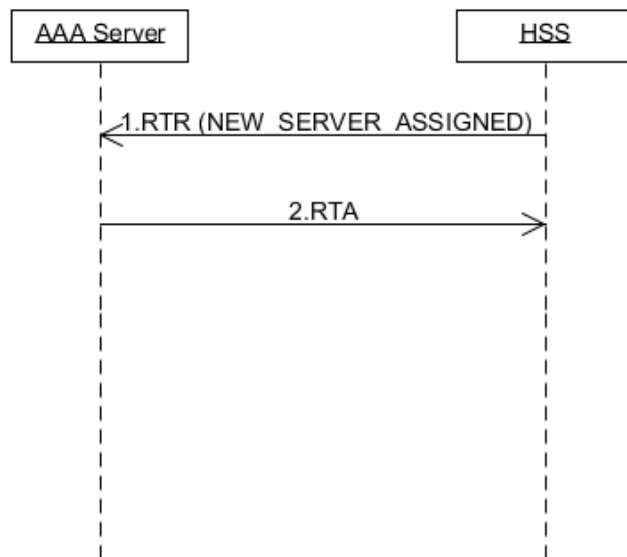


Figure 43 De-Registration with Reason Code NEW_SERVER_ASSIGNED

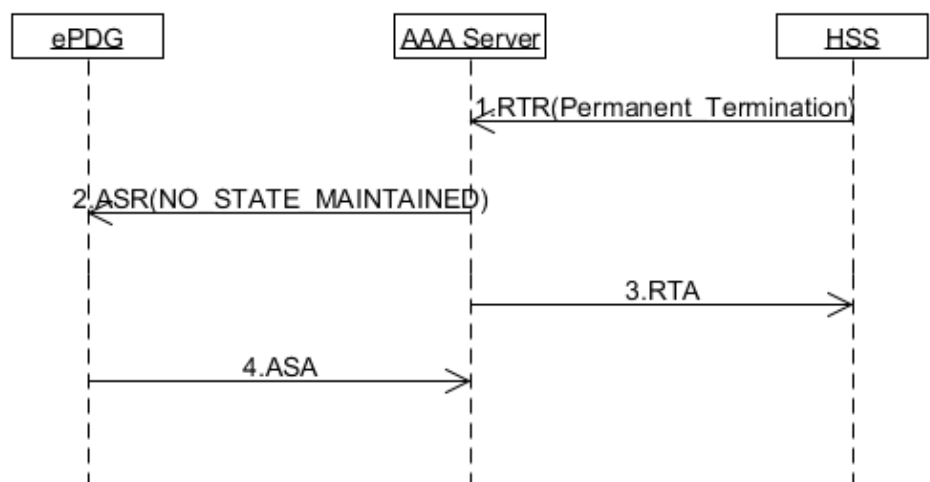


Figure 44 De-Registration with Reason Code PERMANENT_TERMINATION

5.10 HSS Initiated Update of User Profile

The procedure is invoked by the HSS in the following case:

- Indication to AAA Server of change of Non-3GPP subscriber profile within HSS. AAA Server shall update user profile in local repository, and then send RAR to ePDG with the Re-Auth-Request-Type AVP set to AUTHORIZE_ONLY. AAA Server shall also send RAR to PDN_GW if the "Support RAR in S6b" feature is enabled.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

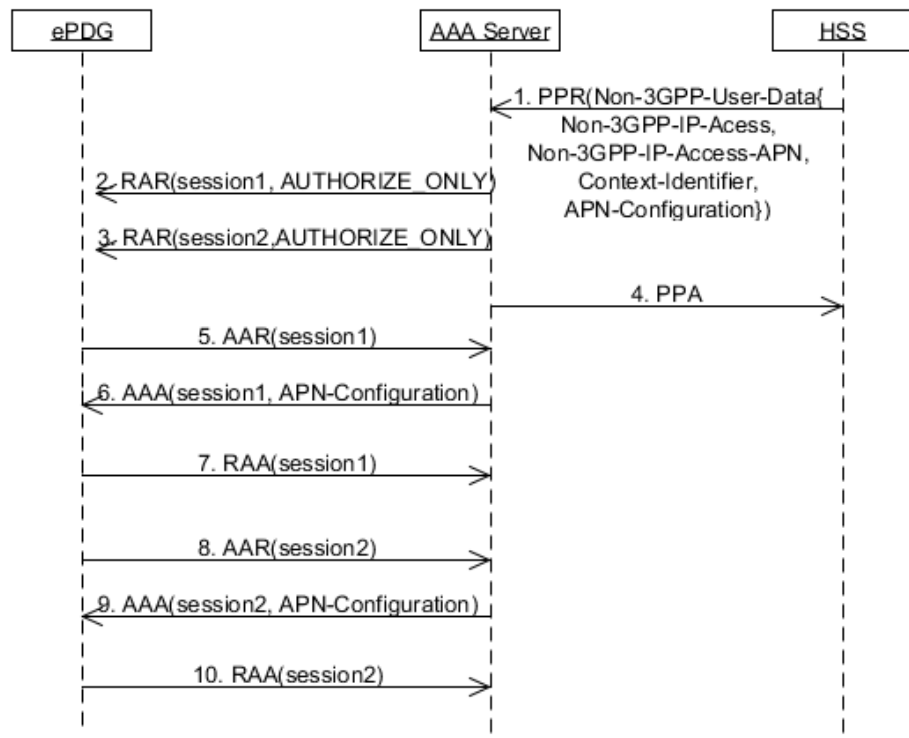


Figure 45 HSS Initiated Update of User Profile

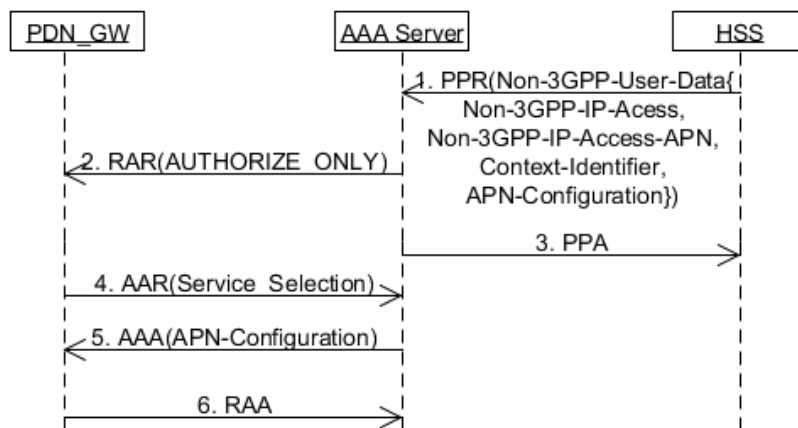


Figure 46 HSS Initiated Update of User Profile with Supporting RAR in S6b

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

5.11 HSS Initiated P-CSCF Restoration

For more information, refer to **4.11 HSS Initiated P-CSCF Restoration**.

5.12 WiFi Mobility Management

This section describes the WiFi Mobility Management (WiFiMM) function. The description is focus on the following two parts:

- The interrogation among network nodes
- The internal behavior of AAA Server to get the user location

WiFiMM is an enhancement of “ePDG Initiated Full Authentication and Authorization” and “ePDG Initiated Re-Authentication and Re-Authorization”. With WiFiMM function, AAA server provides the current user location, in form of `VisitedNetworkId` AVP, to HSS for roaming restriction and to ePDG for charging.

5.12.1 Full Authentication and Authorization with WiFiMM

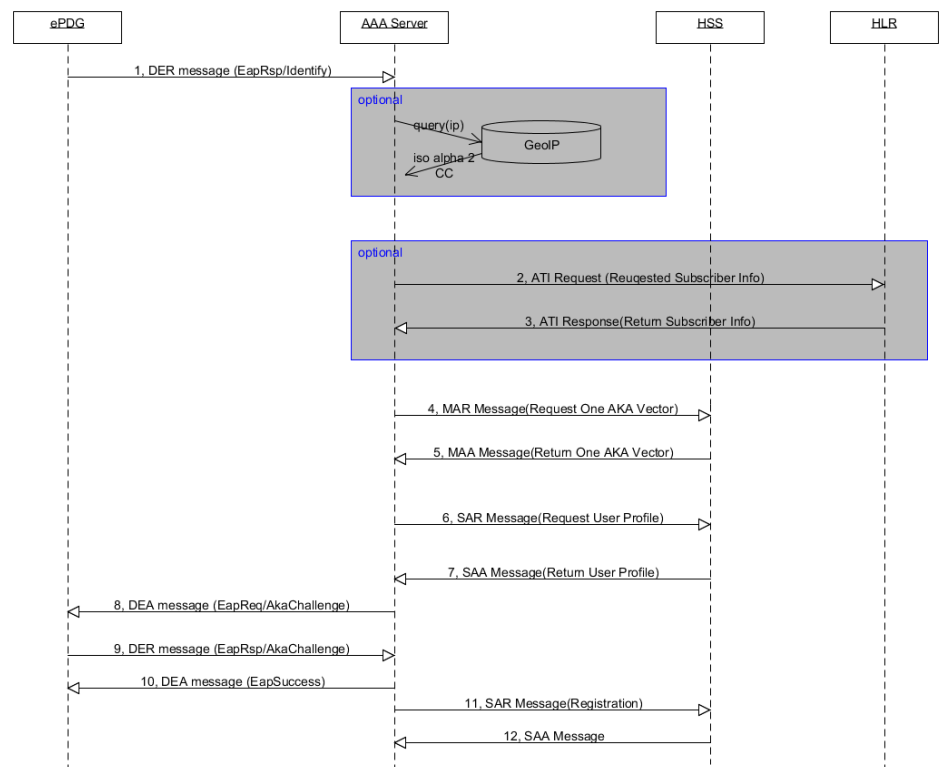


Figure 47 SWm Authentication and Authorization with WiFiMM

Compared with the original “ePDG Initiated Full Authentication and Authorization” and “ePDG Initiated Re-Authentication and Re-Authorization”, the differences are listed as below:

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

1. ePDG provides an `UELocalIPAddress` AVP in the first DER message. Then, AAA server gets the user location through Geography IP Query. Geography IP Query is optional.
2. AAA Server triggers 3GPP CS location lookup through MAPV3 ATI (Any Time Interrogation) with HLR. Then, AAA Server extracts user location from VLR number in the received subscriber information. 3GPP CS Location Lookup is also optional.
3. Controlled by the WiFi Mobility Management option, AAA Server gets the proper MCC (Mobile Country Code) from the result of Geography IP Query and 3GPP CS Location Lookup. Then, AAA Server sends MAR to HSS with a `VisitedNetworkId` AVP. This AVP is `mnc<WiFIMM_MNC>.mcc<USER_MCC>.3gppnetwork.org`, where `WiFIMM_MNC` is a configurable parameter and `USER_MCC` is the MCC selected by AAA Server. For selecting MCC, refer to section 5.11.3.3.
4. HSS checks the `VisitedNetworkId` AVP with its predefined rule, and HSS continues the authentication when no rule violation occurs.
5. AAA Server provides the `VisitedNetworkId` AVP in DEA message to ePDG.

Compared with the Figure , HSS checks the received `VisitedNetworkId` AVP and rejects the authentication here as shown in Figure 44 because user is not allowed roaming to this location.

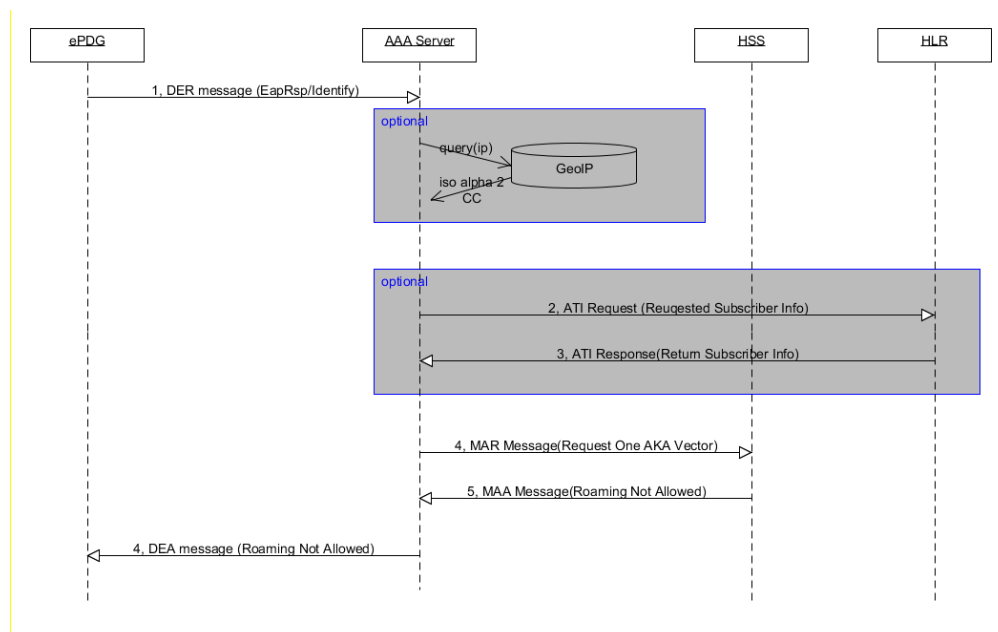


Figure 48 SWm Authentication and Authorization - Roaming Not Allowed

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

HSS sends MAA to AAA Server with result code as DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004). AAA Server aborts the authentication and relays the result code to ePDG. No VisitedNetworkId AVP is sent to ePDG in this case.

5.12.2 Re-Authentication

AAA Server sends MAR to HSS in Re-Authentication case if WiFi Mobility Management function is enabled. If there are caching EAP AKA authentication vectors, AAA Server does not send MAR to HSS for Authentication.

So, with enabled WiFi Mobility Management function, AAA Server asks for only one EAP AKA authentication vector from HSS in both Authentication case and Re-Authentication case.

5.12.3 Getting User Location

AAA Server can get raw user location information through two methods:

- Geography IP Database Query
- 3GPP CS Location Lookup

AAA Server calculates the mobile country code by the procedure shown in the following diagram.

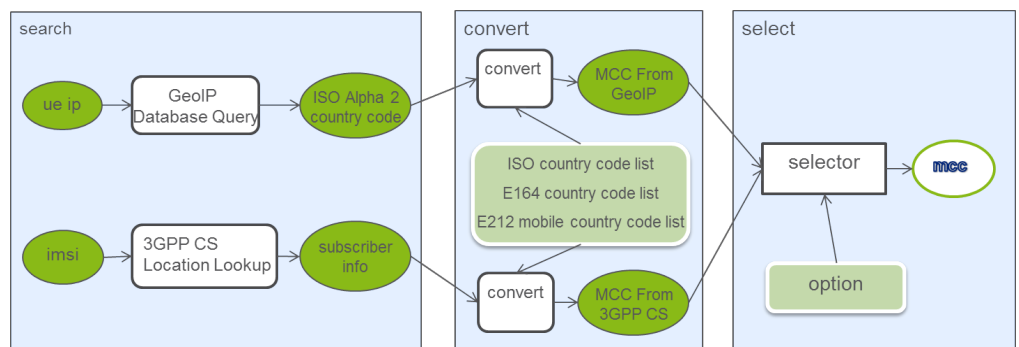


Figure 49 Calculating MCC Procedure

AAA Server supports five exclusive WiFiMM options:

- Disable WiFi Mobility Management
- Get user location from Geography IP Database only
- Get user location from 3GPP CS Network only
- Prefer user location from Geography IP Database

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

- Prefer user location from 3GPP CS Network

5.12.3.1 Geography IP Query

Geography IP Query method is triggered if the option is one of the following:

- Get user location from Geography IP Database only
- Prefer user location from Geography IP Database
- Prefer user location from 3GPP CS Network

AAA Server searches the local Geography IP Database with the input UE local IP address. An ISO Alpha 2 country code is returned if query succeeded, for example, SE for Sweden. A dictionary file maps the ISO country code to mobile country code (MCC). This MCC is saved as `mccFromGeoIP`. If query failed, the `mccFromGeoIP` is empty.

Through checking the Anonymous Proxy list, AAA Server can find out whether the input UE local IP address is anonymous proxy or not. If the IP address belongs to an anonymous proxy, AAA Server assigns `mccFromGeoIP` as the configured special MCC for anonymous proxy.

Geography IP data and Anonymous Proxy list can be gotten from third party data provider, for example, MaxMind GeoIP2. Customer needs to get license from the third party provider. AAA Server defines Geography IP data format, and offers tool to import/update Geography IP data of such format. Only IPv4 data is supported by AAA Server.

5.12.3.2 3GPP CS Location Lookup

3GPP CS Location Lookup method is triggered if the option is one of following:

- Get user location from 3GPP CS Network only
- Prefer user location from Geography IP Database
- Prefer user location from 3GPP CS Network

AAA Server uses MAP J' interface to do ATI with HLR. From the ATI response, AAA Server will get the VLR number where user locates, and extract the MCC as follow:

- If VLR number is international format, AAA Server gets the E164 country code through digital tree search. Then, AAA Server converts the E164 country code into MCC.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

Note: The digital tree is built with all valid E164 country codes; and the longest prefix of the VLR number is the target E164 country code.

- If VLR number is national format, use configurable HPLMN MCC.

The MCC is saved as `mccFromCS`. The `mccFromCS` is empty in the following exceptional cases:

- AAA server does not receive the ATI response before the guard timer expired.
- Age Of Location in ATI response is greater than the threshold (default threshold 120 minutes).

Note:

1. Age Of Location indicates the elapsed time since the last access to the network. It needs to configure the threshold with a proper value to avoid using out-of-date user location.
2. The interrogation with HLR will introduce additional latency to the overall authentication procedure. The latency comes from both network latency and SS7 stack processing cost.

5.12.3.3 Selecting Mobile Country Code

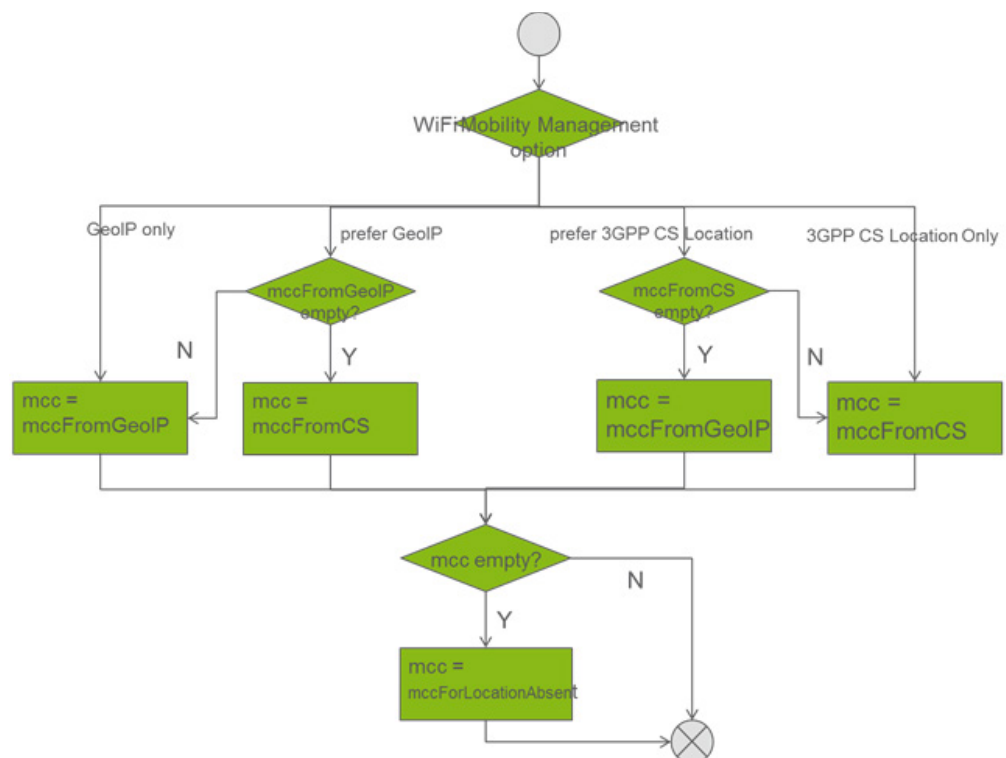


Figure 50 Selecting MCC from Search Results

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

AAA Server checks the WiFi Mobility Management option, and selects mobile country code according to the result of section 5.11.3.1 and section 5.11.3.2.

- **mccFromGeoIP:** It is the result of Geography IP Query.
- **mccFromCS:** It is the result of 3GPP CS Location Lookup.
- **mccForLocationAbsent:** It is a configurable parameter that is used when both **mccFromGeoIP** and **mccFromCS** are empty.

5.13 SES Support

SWm' interface is an extension of 3GPP SWm' interface. This interface is used between IPWorks AAA server and SES for user authentication.

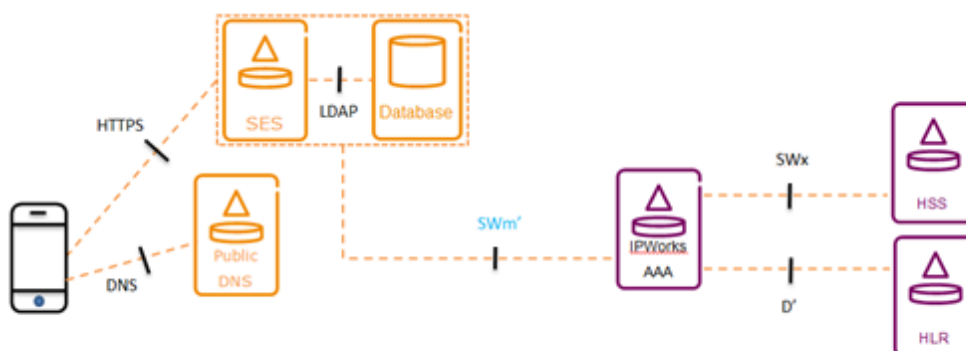


Figure 51 User Authentication for SES

The Secure Entitlement Server (SES) is used to control mobile service delivered to the end users. User devices are equipped with entitlement clients, which query SES periodically to determine, for which services each subscriber is entitled. At first, the entitlement client in the device sends authentication vector stored in the SIM card via HTTPS to SES. The SES delegates the authentication to AAA server over SWm' interface. Once the user is authenticated, a token is returned in the authentication response. The subsequent entitlement related requests carry this token to SES to reduce the signaling towards the AAA server.

SWm' interface uses the same Diameter dictionary as SWm interface. And DER of SWm' interface shall match at least one of the following conditions:

- 1) Auth-Request-Type in DER message equals the configured special authentication request type in AAA server.
- 2) Origin-Host in DER message equals one of the configured SES origin host in AAA server.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

SES and AAA Server support both authentication for both 4G and 3G subscriber, where the authentication method is SIM based EAP AKA. No service authorization is required.

2G subscriber uses EAP-SIM authentication method and AAA Server does not support it.

5.13.1 SES Initiated Authentication for 4G Subscriber

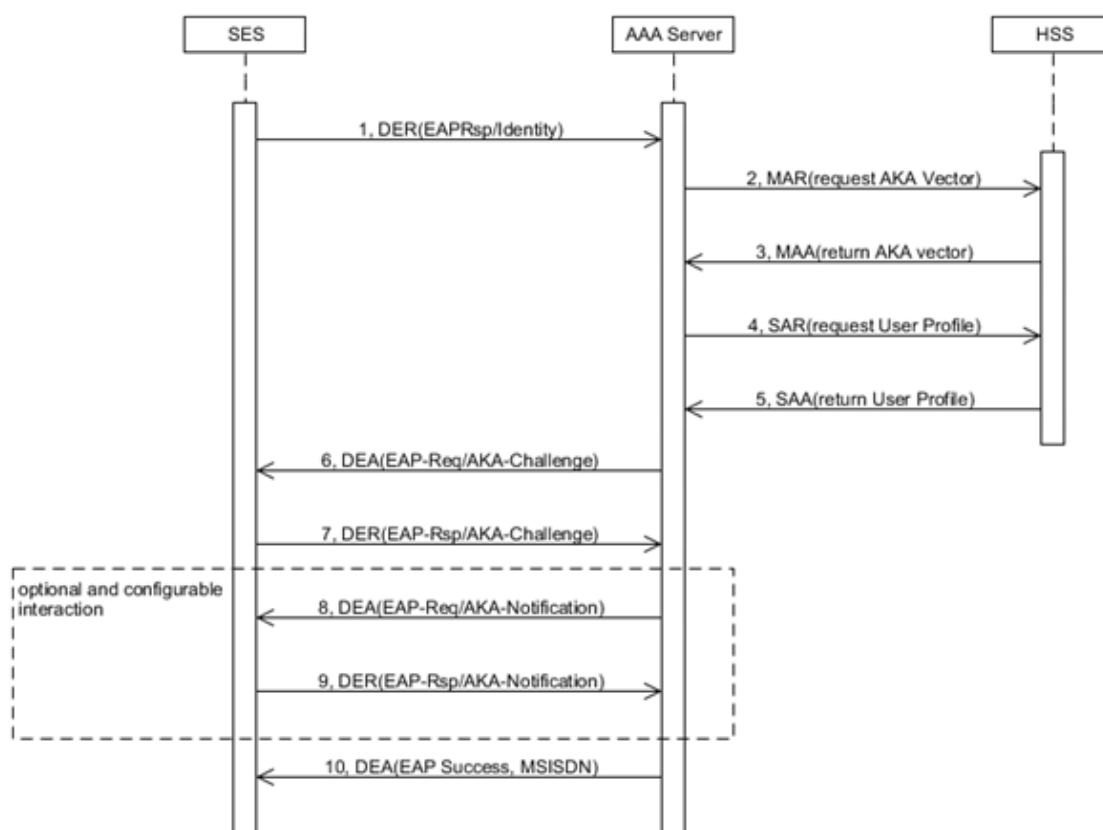


Figure 52 SES Initiated Authentication for 4G Subscriber

AAA Server replies the MSISDN within Mobile-Node-Identifier AVP after authentication completed. And AAA server does not save user profile or SWm' session into DB.

SES will not send STR message to AAA server.

5.13.2 SES Initiated Authentication for 3G Subscriber

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

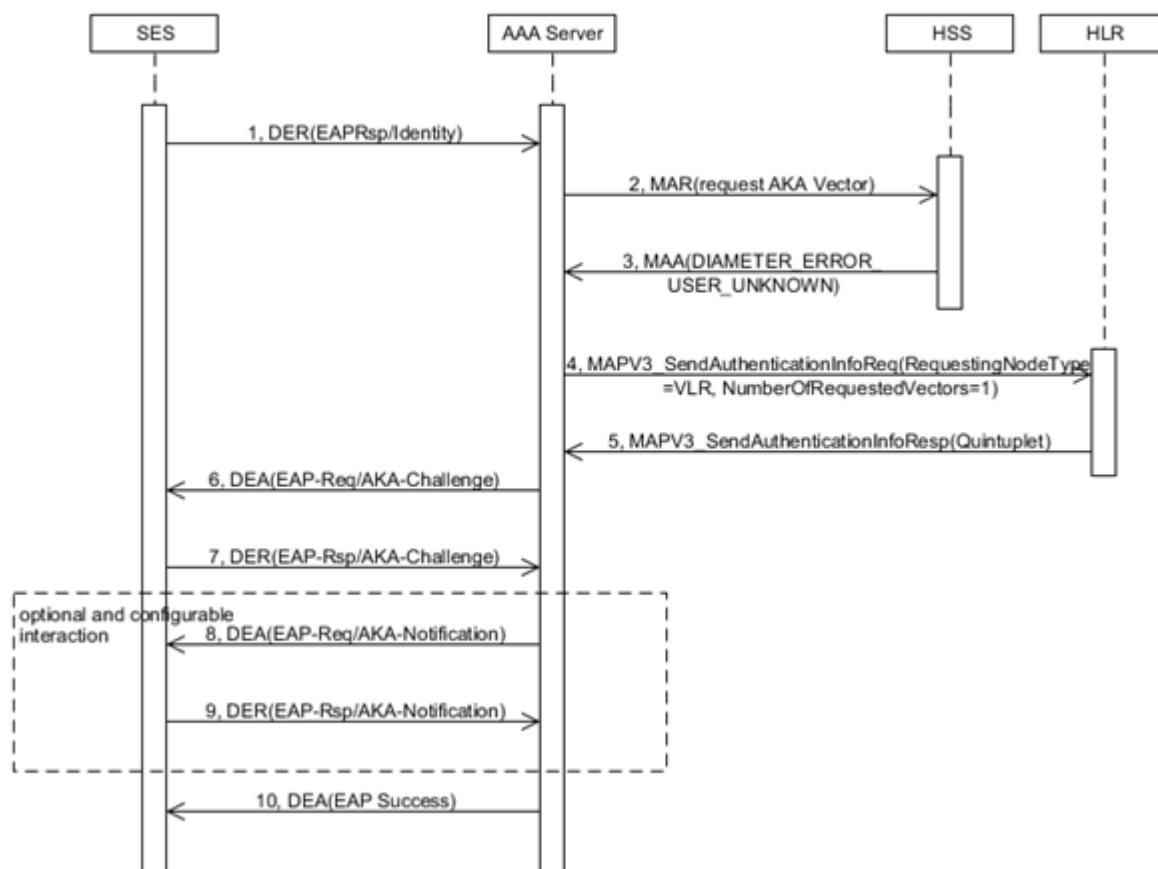


Figure 53 SES Initiated Authentication for 3G Subscriber

HSS notices AAA Server it is not a 4G subscriber. Then AAA Server tries to get one authentication vector from HLR through MAPV3 Send-Authentication-Info procedure. HLR return authentication vector (quintuplet) for the 3G subscriber.

AAA Server does not provide MSISDN to SES for the 3G subscriber. SES will get the MSISDN through query third-party DB.

AAA server does not save user profile or SWm' session into DB. SES will not send STR message to AAA server.

5.14 Emergency Service Control

This section describes the emergency service control function which complies with 3GPP R13 specifications.

AAA supports EPC access for emergency services over an untrusted WLAN access for UEs with valid EPC subscription. AAA supports emergency service

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

control for both SIM-based UE (SWm interface) and non-SIM UE (SWm+ interface).

For emergency service related to Authentication and Authorization message, IPWorks will handle it with high priority, it will not reject it because of overload control function or SWx throttling function.

5.14.1

SWm+S6b Full Authentication and Authorization with Emergency Service

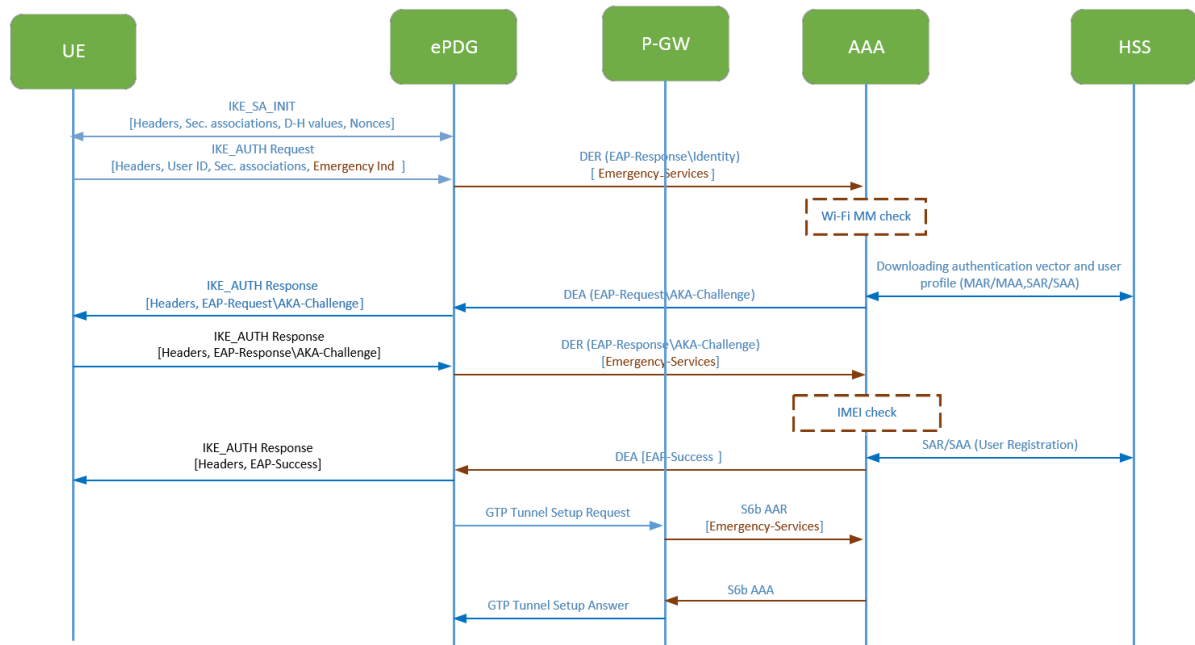


Figure 54 SWm Authentication and Authorization with Emergency Service

Compared with the original “ePDG Initiated Full Authentication and Authorization” and “ePDG Initiated Re-Authentication and Re-Authorization”, the differences are listed as below:

- ePDG provides an Emergency- Services AVP with the Emergency-Indication bit set in the first DER message. Then, AAA server treats this UE requests to access the EPC for emergency services, AAA skips APN authorization and does not send APN-Configuration AVP in the Authentication and Authorization Answer.
- For S6b authorization procedure (AAR/AAA), if `enableS6bAuthzWithoutProfile` is set to true, and the Emergency-Indication bit of the Emergency-Services AVP is set in the Authorization Request, after IPWorks get user profile from HSS via SAA message, IPWorks will response DEA with `DIAMETER_SUCCESS` result code.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

- If IMEI check function is enabled, and `skipIMEICheckForEC` flag value is false, AAA will skip the IMEI check function for emergency service and continue the authentication and authorization procedure.

5.14.2 SWm Re-Authorization with Emergency Service

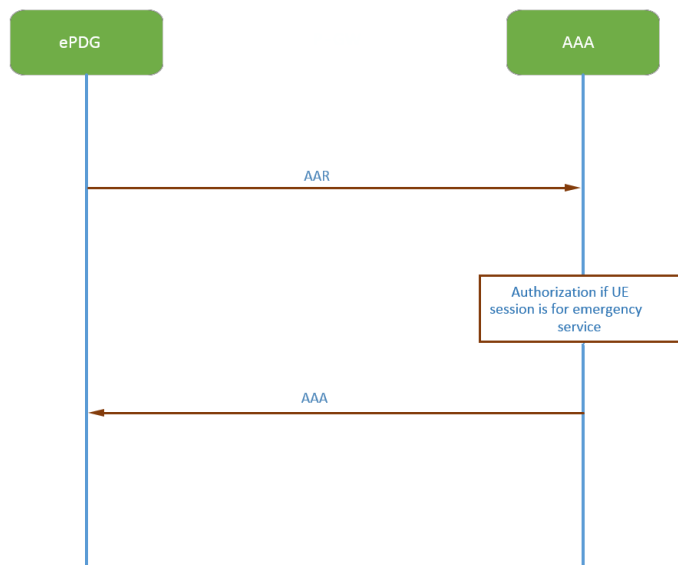


Figure 55 SWm Re-Authorization with Emergency Service

Compared with the original “ePDG Initiated Re-Authorization”, the difference is listed as below:

- For authorization procedure (AAR/AAA), if the Emergency-Indication bit of the Emergency-Services AVP is set in the initial Authentication and Authorization Request, AAA will skip APN authorization and not send APN-Configuration AVP in the Authorization Answer.

5.14.3 SWm+ Authentication and Authorization with Emergency Service

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

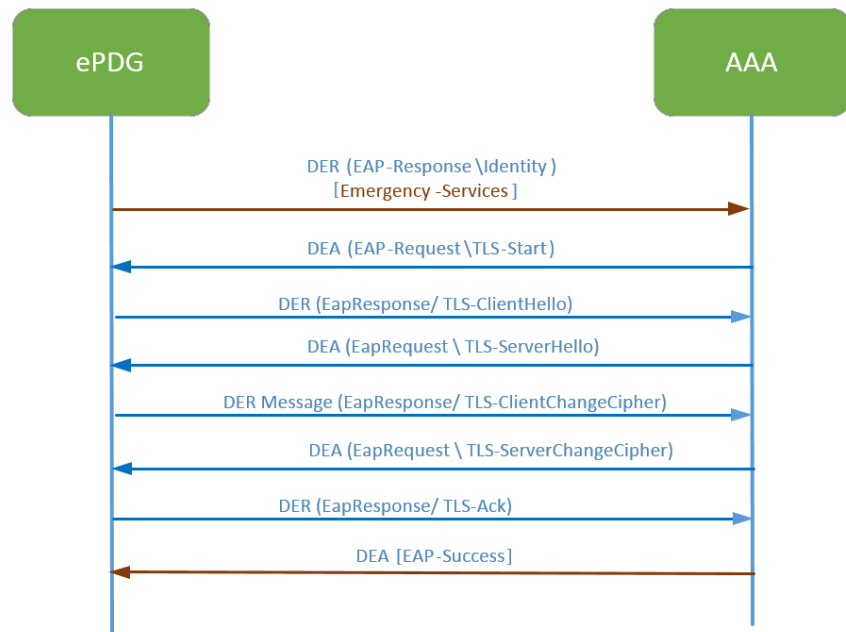


Figure 56 SWm+ Authentication and Authorization with EmergencyService

Compared with the original “SWm+ Authentication and Authorization using EAP-TLS Full Authentication”, the difference is listed as below:

- ePDG provides an Emergency- Services AVP with the Emergency-Indication bit set in the first DER message. Then, AAA server treats this UE requests to access the EPC for emergency services, AAA skips APN authorization and not send APN-Configuration AVP in the Authentication and Authorization Answer.

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

5.14.4 Roaming Check for Emergency Service

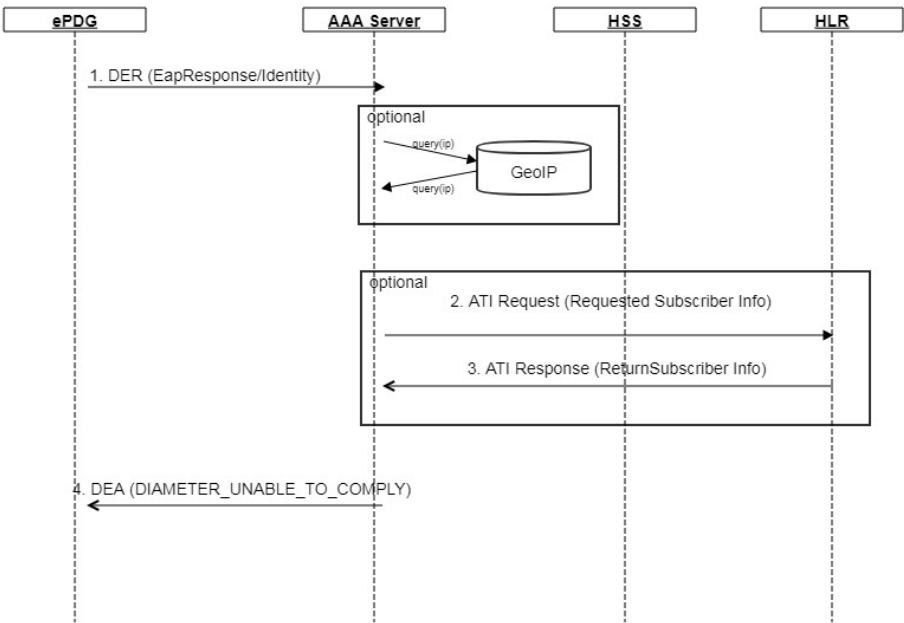


Figure 57 SWm Reject Roaming Authentication

If Wi-Fi mobility management is activated and AAA determines UE requesting emergency services is located outside its home country, AAA rejects the request with DIAMETER_UNABLE_TO_COMPLY when skipRoamingCheck4EC flag is false.

If the UE which requesting emergency service is located within home country, AAA will follow the basic emergency service process.

For more information about skipRoamingCheck4EC, refer to the document **Configure EPC AAA 72[2]**.

6 Standard Compliance Statement

RFC 4187	Reference [10]
3GPP TS 29.273 v12.5.0	Reference [11]
RFC 5448	Reference [12]
RFC 3588	Reference [13]
RFC 4072	Reference [14]
RFC 5216	Reference [15]
RFC 6960	Reference [16]
3GPP TS 23.078 v6.0.0	Reference [17]

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

3GPP TS 29.002 v6.0.0 Reference [18]

7 Terminology

7.1 Abbreviations

AAA	Authentication, Authorization, Accounting
APN	Access Point Name
ABNF	Augmented Backus-Naur Form
AKA	Authentication and Key Agreement
AMBR	Aggregate Maximum Bit Rate
AUTN	Authentication Token
AUTS	Authentication Token for re-synchronization
AV	Authentication Vector
AVP	Attribute-Value Pair
EPC	Evolved Packet Core
MM	Mobility Management
SLF	Subscription Locator Function

7.2 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.
Non-Sim Solution	The solution that can provide authentication, authorization and accounting service for Non-SIM user.

8 References

- [1] IPWorks Configuration Management 6/1551-AVA 901 33/2
- [2] Configure EPC AAA 38/1543-AVA 901 33/2
- [3] Diameter Stack Configuration Guide 8/1553-AVA 901 33/2
- [4] IPWorks AAA Front End Function Overview 61/155 17-AVA 901 6
- [5] Diameter Base Protocol RFC 3588
- [6] Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) RFC 4187
- [7] Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA') RFC 5448
- [8] Extensible Authentication Protocol (EAP) RFC 3748

Prepared (also subject responsible if other) EZAIYUA		No. 57/155 17-AVA 901 16 Uen		
Approved	Checked	Date 2018-06-19	Rev PH1	Reference

- [9] Diameter Extensible Authentication Protocol (EAP) Application RFC 4072
- [10] Universal Mobile Telecommunications System (UMTS); LTE3GPP EPS AAA interfaces; Evolved Packet System (EPS); (3GPP TS 29.273 version 12.5.0 Release 9)
- [11] Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements for non-3GPP accesses (3GPP TS 23.402 version 9.6.0 Release 9)
- [12] IPWorks Statement of Compliance – Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) (RFC 4187)
- [13] IPWorks Statement of Compliance – Universal Mobile Telecommunications System (UMTS); LTE; Evolved Packet System (EPS); 3GPP EPS AAA interfaces (3GPP TS 29.273 v12.5.0)
- [14] IPWorks Statement of Compliance – Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA') (RFC 5448)
- [15] IPWorks Statement of Compliance – Diameter Base Protocol (RFC 3588) 34/174 02-AVA 901 16
- [16] IPWorks Statement of Compliance - RFC 4072
- [17] The EAP-TLS Authentication Protocol – RFC 5216
- [18] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP RFC 6960