

IPWorks 3GPP AAA Server-SES SWm' Interface

INTERWORK DESCRIPTION

Copyright

© Ericsson AB 2016, 2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

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

Trademark List

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



Contents

1	Introduction	1
1.1	Prerequisites	1
1.2	Related Information	1
2	Interface Overview	3
2.1	Interface Role	3
2.2	Services	3
2.3	Encapsulation and Addressing	3
3	Procedures	5
3.1	Authentication from SES	5
4	Information Model	9
4.1	SES Initiated Authentication	9
4.2	SES Initiated Session Termination	11
5	Information Element	13
5.1	General SWm AVPs	13
6	Error Handling	15
7	Formal Syntax	17
8	Related Standards	19
	Reference List	21





1 Introduction

This document describes the SWm' interface between the IPWorks 3GPP AAA Server and SES.

Scope

The SWm' reference point is used to authenticate the User Equipment (UE).

This document covers the following topics:

- Interface Overview
- Procedures
- Information Model
- Information Elements
- Error Handling
- Formal Syntax
- Related Standards

Target Groups

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

1.1 Prerequisites

Not Applicable.

1.2 Related Information

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

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





2 Interface Overview

This section describes the interface between IPWorks 3GPP AAA Server and SES, as shown in Figure 1.

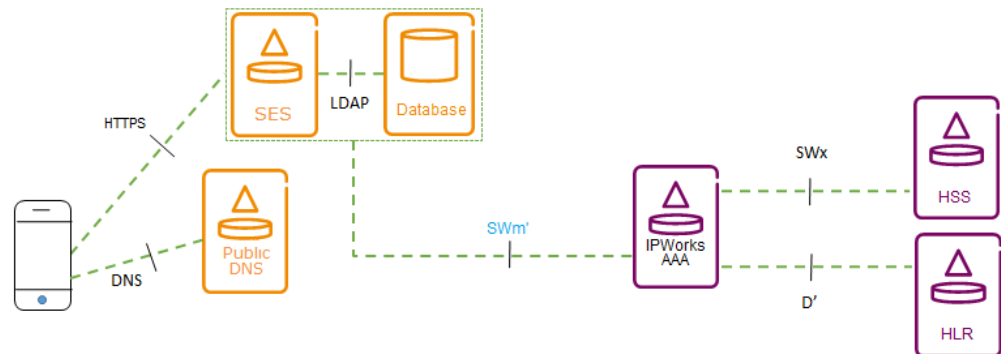


Figure 1 SWm' Interface between IPWorks 3GPP AAA Server and SES

2.1 Interface Role

This section describes the role of the SWm' interface in the EPC network.

For the SWm' interface, IPWorks AAA server acts as 3GPP AAA server in the EPC network, and also takes the role of authentication for UE who accesses to SES.

2.2 Services

This section describes the services that the SWm' interface offers.

The services offered by the SWm' interface are shown in Table 1.

Table 1 Offered Services

Offered Service	Description
Authentication Only	The 3GPP AAA Server is used to authenticate the UE to access to SES.

2.3 Encapsulation and Addressing

The following lower level protocols are used on this interface:

- SCTP
- TCP



— Diameter Base Protocol



3 Procedures

This section describes the procedures used with the offered and used interfaces of IPWorks:

- Authentication From SES

3.1 Authentication from SES

Authentication from SES includes the following three topics:

- SES Initiated Authentication for 4G subscriber
- SES Initiated Authentication for 3G subscriber
- SES Initiated Session Termination

3.1.1 **SES Initiated Authentication for 4G Subscriber**

The procedure is triggered when the 4G subscriber registers to SES.

The authentication on SWm' interface is based on EAP-AKA. The Diameter messages are DER and DEA (see Section 4.1).

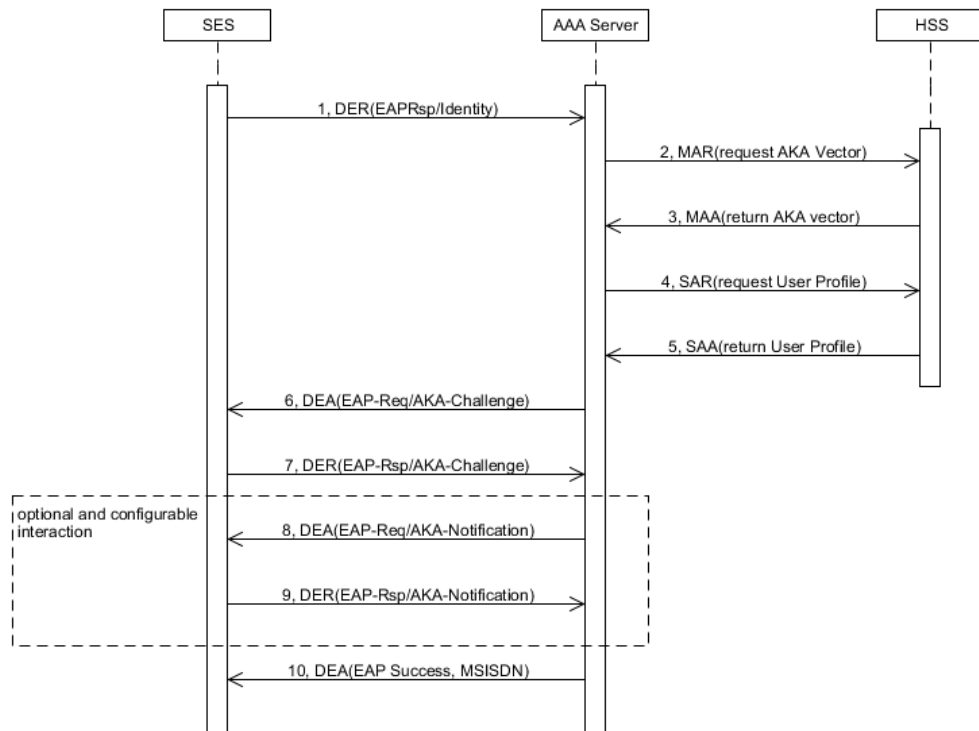


Figure 2 SES Initiated Authentication for 4G Subscriber

Note: The first DER message shall match at least one of the following conditions:

- Auth-Request-Type in DER message equals the configured special authentication request type in AAA server.
- Origin-Host in DER message is in the configured SES host list in AAA server.

3.1.2 SES Initiated Authentication for 3G UE

The procedure is triggered when the 3G subscriber registers to SES.

The authentication on SWm' interface is based on EAP-AKA. The Diameter messages are DER and DEA (see Section 4.1.1 DER Command on page 9).

AAA server requires authentication vector from HLR to complete the authentication. And AAA server will not return the MSISDN to SES after authentication completed.

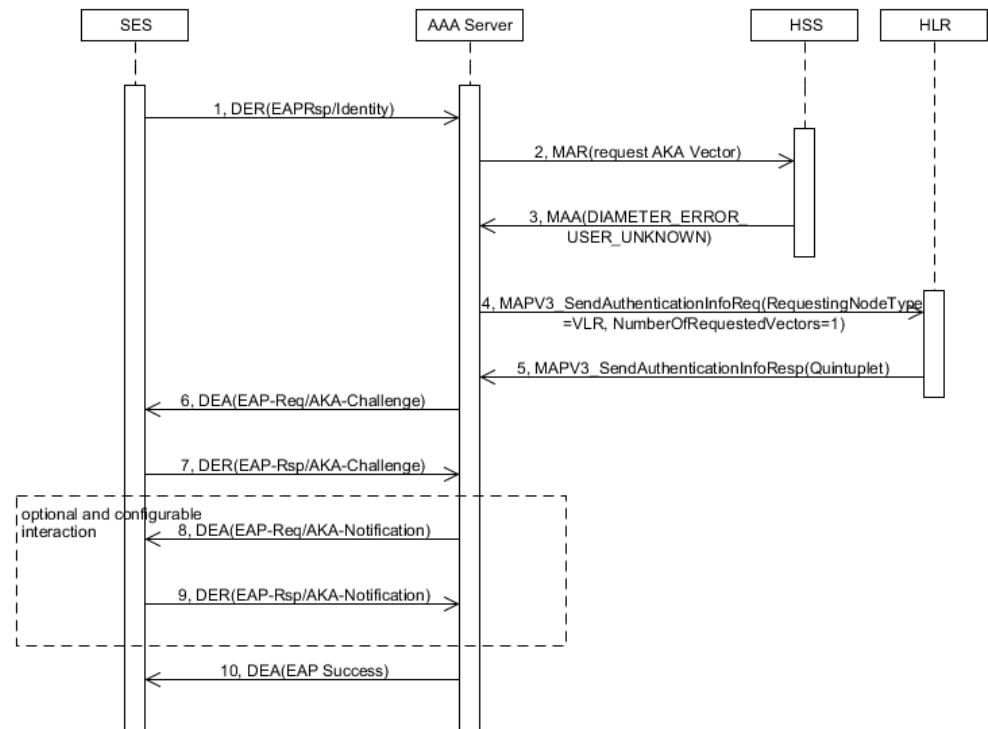


Figure 3 SES Initiated Authentication for 3G Subscriber

Note: The first DER message shall match at least one of the following conditions:

- Auth-Request-Type in DER message equals the configured special authentication request type in AAA server.
- Origin-Host in DER message is in the configured SES host list in AAA server.

3.1.3 SES Initiated Session Termination

SES does not intend to inform AAA server to remove the access information and AAA server shall not maintain the SWm' session after Authentication completed.

For compliance reason, AAA server will return STA with error code DIAMETER_UNKNOWN_SESSION_ID after receiving STR for the SWm' session.

The Diameter messages are STA and STR (see Section 4.2 SES Initiated Session Termination on page 11).

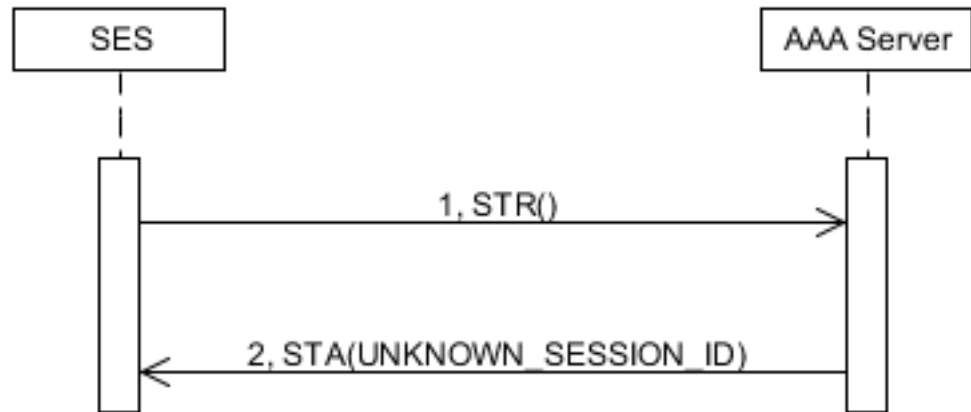


Figure 4 SES Initiated Session Termination



4 Information Model

This section describes the information model including mandatory and optional parameters of each service operation. This document only covers diameter messages and AVPs involved in the application.

Note: For the description and format of the Base Protocol, see Reference [5].

Table 2 shows the Naur Form (ABNF) format used in the commands in the subsections.

Table 2 Naur Form (ABNF) format

{ }	Mandatory
< >	Mandatory with fixed place
[]	Optional
*	Zero or more Occurrences
*n	At most
n	Occurrences

4.1 SES Initiated Authentication

4.1.1 DER Command

The Diameter-EAP-Request (DER) command is sent from SES to 3GPP AAA server. The command is set in the Command Code field (set to 268) and the "R" bit is set in the Command Flags field.

The format of this command is listed as below:

```
<Diameter-EAP-Request> ::= <Diameter Header: 268, REQ, PXY, 16777264>
<Session-Id>
{Auth-Application-Id}
{Origin-Host}
{Origin-Realm}
{Destination-Realm}
{Auth-Request-Type}
{EAP-Payload}
[User-Name]
[RAT-Type]
[Service-Selection]
[MIP6-Feature-Vector]
[QoS-Capability]
[Visited-Network-Identifier]
[UE-Local-IP-Address]
```



```
[AAA-Failure-Indication]
*[Supported-Features]...
*[Proxy-Info]
*[Route-Record]
*[AVP]
```

Note:

- The AVP is mandatory when the DER message carries the EAP-Response/Identity package:
 - User-Name
- The following AVPs must be carried in the first DER message that transfers the EAP-Response/Identity message:
 - AVPs used to fetch authentication vector and user profile from HSS.
- The 3GPP AAA server records these AVPs into the session for later re-authentication and/or re-authorization use.
 - Auth-Grace-Period and Authorization-Lifetime AVPs (if exist).
- Consult Section 5.1 General SWm AVPs on page 13 for the EAP Messages encapsulated in Diameter EAP-Payload AVP.

4.1.2**DEA Command**

The Diameter-EAP-Answer (DEA) command is sent from 3GPP AAA server to SES. The command is set in the Command Code field (set to 268) and the "R" bit is cleared in the Command Flags field.

The format of this command is listed as below:

```
<Diameter-EAP-Request>::=<Diameter Header: 268, REQ, PXY, 16777264>
<Session-Id>
{Auth-Application-Id}
{Auth-Request-Type}
{Result-Code}
{Origin-Host}
{Origin-Realm}
{EAP-Payload}
[EAP-Master-Session-Key]
[APN-OI-Replacement]
[APN-Configuration]
[MIP6-Feature-Vector]
[Mobile-Node-Identifier]
[Trace-Info]
[Subscription-ID]
[Session-Timeout]
[MIP6-Agent-Info]
```



```
[3GPP-Charging-Characteristics]
[Visited-Network-Identifier]
*[Redirect-Host]
[Redirect-Host-Usage]
[Redirect-Max-Cache-Time]
*[Supported-Features]
...
*[Proxy-Info]
*[AVP]
```

4.2 SES Initiated Session Termination

4.2.1 STR Command

The Session-Termination-Request (STR) command is sent from SES to 3GPP AAA server.

This command is set in the Command-Code field (set to 275) and the "R" bit set in the Command Flags field.

Note: The Command Code value and Augmented Backus-Naur Form (ABNF) follows the format defined in the IETF RFC 3588, see Reference [5].

The format of this command is listed as below:

```
<Session-Termination-Request>::<Diameter Header: 275,REQ,PXY,16777264>
<Session-Id>
{Origin-Host}
{Origin-Realm}
{Destination-Realm}
{Auth-Application-Id}
[User-Name]
...
*[Proxy-Info]
*[Route-Record]
*[AVP]
```

Note: The AVP User-Name is mandatory for the STR message.

4.2.2 STA Command

The Session-Termination-Answer (STR) command is sent from 3GPP AAA server to SES.

This command is set in the Command-Code field (set to 275) and the "R" bit cleared in the Command Flags field.



Note: The IETF RFC 3588 Session-Termination-Request command reuses this Command Code value and Augmented Backus-Naur Form (ABNF), see Reference [5].

The format of this command is listed as below:

```
<Session-Termination-Answer>::=<Diameter Header: 275, PXY, 16777264>
<Session-Id>
{Result-Code}
{Origin-Host}
{Origin-Realm}
[Redirect-Host-Usage]
[Redirect-Max-Cache-Time]
...
*[Proxy-Info]
*[AVP]
```




5 Information Element

The IE definition of SWm' interface is almost the same as SWm interface. The SWm' specific AVPs are list in the following section.

5.1 General SWm AVPs

For general SWm AVPs, refer to section Information Element in document IPWorks 3GPP AAA Server-ePDG SWm and SWm+ Interface.





6 Error Handling

The error handling of SWm' interface is the same as SWm interface.

For more detail, refer to section Error Handling in document IPWorks 3GPP AAA Server-ePDG SWm and SWm+ Interface.





7 Formal Syntax

Not Applicable.





8 Related Standards

- 3GPP EPS AAA interfaces 3GPP TS 29.273 version 12.5.0
- Diameter Base Protocol RFC 3588
- Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) RFC 4187
- Extensible Authentication Protocol (EAP) RFC 3748 Diameter
- Extensible Authentication Protocol (EAP) Application RFC 4072
- 3GPP MAP





Reference List

IPWorks Library Documents

- [1] Glossary of Terms and Acronyms
- [2] Trademark Information
- [3] Typographic Conventions
- [4] IPWorks 3GPP AAA Server-ePDG SWm and SWm+ Interface

Standards

- [5] [Diameter Base Protocol RFC 3588](#)
- [6] [Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement \(EAP-AKA\) RFC 4187](#)
- [7] [Extensible Authentication Protocol \(EAP\) RFC 3748](#)
- [8] [Diameter Extensible Authentication Protocol \(EAP\) Application RFC 4072](#)
- [9] [Universal Mobile Telecommunications System \(UMTS\); LTE3GPP EPS AAA interfaces; Evolved Packet System \(EPS\); \(3GPP TS 29.273 version 12.5.0 Release 12\)](#)
- [10] [EAP-TLS Authentication Protocol RFC 5216.](#)