

# ETSI TS 129 273 V11.10.0 (2015-01)



**Universal Mobile Telecommunications System (UMTS);  
LTE;  
Evolved Packet System (EPS);  
3GPP EPS AAA interfaces  
(3GPP TS 29.273 version 11.10.0 Release 11)**



---

**Reference**RTS/TSGC-0429273vba0

---

**Keywords**LTE,UMTS

---

**ETSI**

650 Route des Lucioles  
F-06921 Sophia Antipolis Cedex - FRANCE

---

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° 7803/88

---

**Important notice**

---

The present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

[http://portal.etsi.org/chaicor/ETSI\\_support.asp](http://portal.etsi.org/chaicor/ETSI_support.asp)

---

**Copyright Notification**

---

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2015.

All rights reserved.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

**GSM®** and the GSM logo are Trade Marks registered and owned by the GSM Association.

---

## Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://ipr.etsi.org>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

---

## Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under <http://webapp.etsi.org/key/queryform.asp>.

---

## Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**may not**", "**need**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

# Contents

Intellectual Property Rights .....	2
Foreword.....	2
Modal verbs terminology.....	2
Foreword.....	9
Introduction .....	9
1 Scope .....	10
2 References .....	10
3 Definitions, symbols and abbreviations .....	12
3.1 Definitions .....	12
3.1.1 General.....	12
3.1.2 Handling of Information Elements .....	12
3.2 Abbreviations .....	12
4 SWa Description .....	13
4.1 Functionality.....	13
4.1.1 General.....	13
4.1.2 Procedure Descriptions .....	13
4.1.2.1 SWa Authentication and Authorization procedure.....	13
4.1.2.1.1 General .....	13
4.1.2.1.2 3GPP AAA Server Detailed Behaviour.....	15
4.1.2.1.3 3GPP AAA Proxy Detailed Behaviour.....	15
4.1.2.2 SWa HSS/AAA Initiated Detach .....	15
4.1.2.3 SWa Non-3GPP Access Network Initiated Detach.....	15
4.1.2.4 SWa Re-Authentication and Re-Authorization Procedure.....	16
4.1.2.4.1 General .....	16
4.1.2.4.2 3GPP AAA Server Detailed Behaviour.....	17
4.1.2.4.3 3GPP AAA Proxy Detailed Behaviour.....	17
4.2 Protocol Specification .....	18
4.2.1 General.....	18
4.2.2 Commands .....	18
4.2.2.1 Commands for SWa authentication and authorization procedures.....	18
4.2.2.1.1 Diameter-EAP-Request (DER) Command .....	18
4.2.2.1.2 Diameter-EAP-Answer (DEA) Command .....	18
4.2.2.2 Commands for SWa HSS/AAA Initiated Detach.....	19
4.2.2.3 Commands for Untrusted non-3GPP Access network Initiated Session Termination .....	19
4.2.2.4 Commands for SWa Re-Authentication and Re-Authorization Procedures.....	19
4.2.2.4.1 Re-Auth-Request (RAR) Command.....	19
4.2.2.4.2 Re-Auth-Answer (RAA) Command .....	19
4.2.2.4.3 Diameter-EAP-Request (DER) Command .....	19
4.2.2.4.4 Diameter-EAP-Answer (DEA) Command .....	19
4.2.3 Information Elements .....	19
4.2.4 Session Handling .....	20
5 STa Description.....	20
5.1 Functionality.....	20
5.1.1 General.....	20
5.1.2 Procedures Description .....	20
5.1.2.1 STa Access Authentication and Authorization.....	20
5.1.2.1.1 General .....	20
5.1.2.1.2 3GPP AAA Server Detailed Behaviour.....	27
5.1.2.1.3 3GPP AAA Proxy Detailed Behaviour.....	30
5.1.2.1.4 Trusted non-3GPP access network Detailed Behaviour .....	31
5.1.2.2 HSS/AAA Initiated Detach on STa.....	32

5.1.2.2.1	General .....	32
5.1.2.2.2	3GPP AAA Server Detailed Behaviour.....	33
5.1.2.2.3	3GPP AAA Proxy Detailed Behaviour.....	34
5.1.2.3	STa Re-Authorization and Re-Authentication Procedures.....	34
5.1.2.3.1	General .....	34
5.1.2.3.2	3GPP AAA Server Detailed Behaviour.....	41
5.1.2.3.3	3GPP AAA Proxy Detailed Behaviour.....	41
5.1.2.3.4	Trusted Non-3GPP Access Network Detailed Behaviour .....	42
5.1.2.4	Non-3GPP Access Network Initiated Session Termination .....	42
5.1.2.4.1	General .....	42
5.1.2.4.2	3GPP AAA Server Detailed Behaviour.....	43
5.1.2.4.3	3GPP AAA Proxy Detailed Behaviour.....	43
5.2	Protocol Specification .....	43
5.2.1	General.....	43
5.2.2	Commands .....	44
5.2.2.1	Commands for STa PMIPv6 or GTPv2 authentication and authorization procedures.....	44
5.2.2.1.1	Diameter-EAP-Request (DER) Command .....	44
5.2.2.1.2	Diameter-EAP-Answer (DEA) Command .....	45
5.2.2.2	Commands for STa HSS/AAA Initiated Detach for Trusted non-3GPP Access .....	45
5.2.2.2.1	Abort-Session-Request (ASR) Command .....	45
5.2.2.2.2	Abort-Session-Answer (ASA) Command .....	46
5.2.2.2.3	Session-Termination-Request (STR) Command .....	46
5.2.2.2.4	Session-Termination-Answer (STA) Command .....	46
5.2.2.3	Commands for Re-Authentication and Re-Authorization Procedure .....	46
5.2.2.3.1	Re-Auth-Request (RAR) Command.....	46
5.2.2.3.2	Re-Auth-Answer (RAA) Command .....	47
5.2.2.3.3	AA-Request (AAR) Command .....	47
5.2.2.3.4	AA-Answer (AAA) Command.....	47
5.2.2.3.5	Diameter-EAP-Request (DER) Command .....	47
5.2.2.3.6	Diameter-EAP-Answer (DEA) Command .....	48
5.2.2.4	Commands for Trusted non-3GPP Access network Initiated Session Termination.....	48
5.2.2.4.1	Session-Termination-Request (STR) Command .....	48
5.2.2.4.2	Session-Termination-Answer (STA) Command .....	48
5.2.3	Information Elements .....	48
5.2.3.1	General .....	48
5.2.3.2	Mobile-Node-Identifier .....	49
5.2.3.3	MIP6-Feature-Vector .....	50
5.2.3.4	QoS Capability .....	50
5.2.3.5	Service-Selection .....	50
5.2.3.6	RAT-Type .....	50
5.2.3.7	ANID.....	51
5.2.3.8	AMBR.....	51
5.2.3.9	AN-Trusted .....	51
5.2.3.10	Feature-List-ID AVP.....	51
5.2.3.11	Feature-List AVP .....	51
5.2.3.12	MIP-FA-RK .....	51
5.2.3.13	MIP-FA-RK-SPI .....	51
5.2.3.14	Full-Network-Name .....	51
5.2.3.15	Short-Network-Name .....	51
5.2.3.16	Void.....	52
5.2.3.17	Void.....	52
5.2.3.18	WLAN-Identifier .....	52
5.2.3.19	Transport-Access-Type .....	52
5.2.3.20	DER-Flags .....	52
5.2.3.21	DEA-Flags.....	52
5.2.3.22	SSID.....	52
5.2.3.23	HESSID.....	53
5.2.4	Session Handling .....	53
6	SWd Description .....	53
6.1	Functionality.....	53
6.1.1	General.....	53

6.1.2	Procedures Description .....	53
6.1.2.1	Trusted non-3GPP Access / Access Gateway related procedures .....	53
6.1.2.1.1	Trusted Non-3GPP Access Authentication and Authorization .....	53
6.1.2.1.2	HSS/AAA Initiated Detach for Trusted non-3GPP Access .....	56
6.1.2.1.3	Access and Service Authorization information update .....	56
6.1.2.1.4	Trusted non-3GPP Access Network Initiated Session Termination .....	57
6.1.2.2	Untrusted non-3GPP Access / ePDG related procedures .....	57
6.1.2.3	PDN GW related procedures .....	57
6.2	Protocol Specification .....	58
6.2.1	General .....	58
6.2.2	Commands .....	58
6.2.2.1	Commands used in connection with the STa interface .....	58
6.2.2.1.1	Commands for STa PMIPv6 or GTPv2 authentication and authorization procedures .....	58
6.2.2.1.1.1	Diameter-EAP-Request (DER) Command .....	58
6.2.2.1.1.2	Diameter-EAP-Answer (DEA) Command .....	59
6.2.2.1.2	Commands for STa HSS/AAA Initiated Detach for Trusted non-3GPP Access .....	59
6.2.2.1.3	Commands for STa Access and Service Authorization Update Procedure .....	60
6.2.2.1.4	Commands for Trusted non-3GPP Access network Initiated Session Termination .....	60
6.2.2.2	Commands used in connection with the SWm interface .....	60
6.2.2.3	Commands used in connection with the S6b interface .....	60
6.2.3	Information Elements .....	60
6.2.3.1	General .....	60
7	SWm Description .....	61
7.1	Functionality .....	61
7.1.1	General .....	61
7.1.2	Procedures Description .....	62
7.1.2.1	Authentication and Authorization Procedures .....	62
7.1.2.1.1	General .....	62
7.1.2.1.2	3GPP AAA Server Detailed Behaviour .....	65
7.1.2.1.3	3GPP AAA Proxy Detailed Behaviour .....	67
7.1.2.1.4	ePDG Detailed Behaviour .....	67
7.1.2.2	Authorization Procedures .....	68
7.1.2.2.1	General .....	68
7.1.2.2.2	3GPP AAA Server Detailed Behaviour .....	70
7.1.2.2.3	3GPP AAA Proxy Detailed Behaviour .....	70
7.1.2.2.4	ePDG Detailed Behaviour .....	70
7.1.2.3	ePDG Initiated Session Termination Procedures .....	71
7.1.2.3.1	General .....	71
7.1.2.3.2	3GPP AAA Server Detailed Behavior .....	71
7.1.2.3.3	3GPP AAA Proxy Detailed Behavior .....	72
7.1.2.4	3GPP AAA Server Initiated Session Termination Procedures .....	72
7.1.2.4.1	General .....	72
7.1.2.4.2	3GPP AAA Server Detailed Behaviour .....	73
7.1.2.4.3	3GPP AAA Proxy Detailed Behaviour .....	73
7.1.2.5	Authorization Information Update Procedures .....	73
7.1.2.5.1	General .....	73
7.1.2.5.2	3GPP AAA Server Detailed Behaviour .....	74
7.1.2.5.3	ePDG Detailed Behaviour .....	74
7.2	Protocol Specification .....	75
7.2.1	General .....	75
7.2.2	Commands .....	75
7.2.2.1	Commands for SWm Authentication and Authorization Procedures .....	75
7.2.2.1.1	Diameter-EAP-Request (DER) Command .....	75
7.2.2.1.2	Diameter-EAP-Answer (DEA) Command .....	75
7.2.2.1.3	Diameter-AA-Request (AAR) Command .....	76
7.2.2.1.4	Diameter-AA-Answer (AAA) Command .....	76
7.2.2.2	Commands for ePDG Initiated Session Termination .....	77
7.2.2.2.1	Session-Termination-Request (STR) Command .....	77
7.2.2.2.2	Session-Termination-Answer (STA) Command .....	77
7.2.2.3	Commands for 3GPP AAA Server Initiated Session Termination .....	77
7.2.2.3.1	Abort-Session-Request (ASR) Command .....	77

7.2.2.3.2	Abort-Session-Answer (ASA) Command .....	78
7.2.2.3.3	Session-Termination-Request (STR) Command .....	78
7.2.2.3.4	Session-Termination-Answer (STA) Command .....	78
7.2.2.4	Commands for Authorization Information Update .....	78
7.2.2.4.1	Re-Auth-Request (RAR) Command.....	78
7.2.2.4.2	Re-Auth-Answer (RAA) Command.....	79
7.2.3	Information Elements .....	79
7.2.3.1	General.....	79
7.2.3.2	Feature-List-ID AVP.....	80
7.2.3.3	Feature-List AVP.....	80
7.2.4	Session Handling .....	80
8	SWx Description .....	80
8.1	Functionality.....	80
8.1.1	General.....	80
8.1.2	Procedures Description .....	81
8.1.2.1	Authentication Procedure.....	81
8.1.2.1.1	General .....	81
8.1.2.1.2	Detailed behaviour.....	83
8.1.2.2	Location Management Procedures .....	84
8.1.2.2.1	General .....	84
8.1.2.2.2	UE/PDN Registration/DeRegistration Notification.....	85
8.1.2.2.2.1	General.....	85
8.1.2.2.2.2	Detailed behaviour .....	87
8.1.2.2.3	Network Initiated De-Registration by HSS, Administrative .....	89
8.1.2.2.3.1	General.....	89
8.1.2.2.3.2	Detailed behaviour .....	90
8.1.2.3	HSS Initiated Update of User Profile .....	90
8.1.2.3.1	General .....	90
8.1.2.3.2	HSS Detailed behaviour .....	91
8.1.2.3.3	3GPP AAA Server Detailed behaviour .....	91
8.1.2.4	Fault Recovery Procedures .....	92
8.1.2.4.1	HSS Reset Indication.....	92
8.1.2.4.1.1	General.....	92
8.1.2.4.1.2	HSS Detailed behaviour .....	92
8.1.2.4.1.3	3GPP AAA Server Detailed behaviour .....	93
8.1.2.4.2	HSS Restoration .....	93
8.1.2.4.2.1	General.....	93
8.1.2.4.2.2	HSS Detailed behaviour .....	94
8.1.2.4.2.3	3GPP AAA Server Detailed behaviour .....	94
8.2	Protocol Specification .....	94
8.2.1	General.....	94
8.2.2	Commands .....	94
8.2.2.1	Authentication Procedure.....	94
8.2.2.2	HSS Initiated Update of User Profile Procedure.....	95
8.2.2.3	Non-3GPP IP Access Registration Procedure.....	96
8.2.2.4	Network Initiated De-Registration by HSS Procedure.....	97
8.2.3	Information Elements .....	97
8.2.3.0	General .....	97
8.2.3.1	Non-3GPP-User-Data .....	99
8.2.3.2	Subscription-ID .....	99
8.2.3.3	Non-3GPP-IP-Access.....	99
8.2.3.4	Non-3GPP-IP-Access-APN .....	100
8.2.3.5	RAT-Type .....	100
8.2.3.6	Session-Timeout.....	100
8.2.3.7	APN-Configuration .....	100
8.2.3.8	ANID.....	100
8.2.3.9	SIP-Auth-Data-Item .....	100
8.2.3.10	Confidentiality-Key.....	100
8.2.3.11	Integrity-Key.....	100
8.2.3.12	Server-Assignment-Type AVP .....	101
8.2.3.13	Trace-Info.....	101

8.2.3.14	Trace-Data.....	101
8.2.3.15	Feature-List-ID AVP.....	101
8.2.3.16	Feature-List AVP .....	101
8.2.3.17	PPR-Flags .....	102
8.2.3.18	TWAN-Default-APN-Context-Id.....	102
8.2.3.19	TWAN-Access-Info .....	102
8.2.3.20	Access-Authorization-Flags.....	103
8.2.3.21	AAA-Failure-Indication.....	103
8.2.4	Session Handling .....	103
8.3	User identity to HSS resolution.....	103
9	S6b and H2 Description .....	104
9.1	Functionality.....	104
9.1.1	General.....	104
9.1.2	Procedures Description .....	105
9.1.2.1	Authentication and Authorization Procedures when using DSMIPv6 .....	105
9.1.2.1.1	General .....	105
9.1.2.1.2	PDN GW Detailed Behaviour .....	108
9.1.2.1.3	3GPP AAA Server Detailed Behaviour.....	109
9.1.2.1.4	3GPP AAA Proxy Detailed Behaviour.....	110
9.1.2.2	Authorization Procedures when using PMIPv6 or GTPv2.....	110
9.1.2.2.1	General .....	110
9.1.2.2.2	PDN GW Detailed Behaviour .....	113
9.1.2.2.3	3GPP AAA Server Detailed Behaviour.....	113
9.1.2.2.4	3GPP AAA Proxy Detailed Behaviour.....	114
9.1.2.3	PDN GW Initiated Session Termination Procedures .....	114
9.1.2.3.1	General .....	114
9.1.2.3.2	PDN GW Detailed Behaviour .....	115
9.1.2.3.3	3GPP AAA Server Detailed Behaviour.....	115
9.1.2.3.4	3GPP AAA Proxy Detailed Behaviour.....	115
9.1.2.4	3GPP AAA Initiated Session Termination Procedures .....	116
9.1.2.4.1	General .....	116
9.1.2.4.2	PDN GW Detailed Behaviour .....	117
9.1.2.4.3	3GPP AAA Server Detailed Behaviour.....	117
9.1.2.4.4	3GPP AAA Proxy Detailed Behaviour.....	117
9.1.2.5	Service Authorization Information Update Procedures.....	118
9.1.2.5.1	General .....	118
9.1.2.5.2	Detailed Behaviour.....	121
9.1.2.6	Authorization Procedures when using MIPv4 FACoA .....	122
9.1.2.6.1	General .....	122
9.1.2.6.2	PDN GW Detailed Behaviour .....	123
9.1.2.6.3	3GPP AAA Server Detailed Behaviour.....	124
9.1.2.6.4	3GPP AAA Proxy Detailed Behaviour.....	124
9.2	Protocol Specification .....	125
9.2.1	General.....	125
9.2.2	Commands .....	125
9.2.2.1	Commands for S6b DSMIPv6 Authorization Procedures.....	125
9.2.2.1.1	Diameter-EAP-Request (DER) Command .....	125
9.2.2.1.2	Diameter-EAP-Answer (DEA) Command .....	126
9.2.2.2	Commands for S6b PMIPv6 or GTPv2 Authorization Procedures .....	126
9.2.2.2.1	AA-Request (AAR) Command .....	126
9.2.2.2.2	AA-Answer (AAA) Command.....	127
9.2.2.3	Commands for PDN GW Initiated Session Termination .....	127
9.2.2.3.1	Session-Termination-Request (STR) Command .....	127
9.2.2.3.2	Session-Termination-Answer (STA) Command .....	128
9.2.2.4	Commands for 3GPP AAA Server Initiated Session Termination.....	128
9.2.2.4.1	Abort-Session-Request (ASR) Command .....	128
9.2.2.4.2	Abort-Session-Answer (ASA) Command .....	128
9.2.2.4.3	Session-Termination-Request (STR) Command .....	129
9.2.2.4.4	Session-Termination-Answer (STA) Command .....	129
9.2.2.5	Commands for S6b MIPv4 FACoA Authorization Procedures .....	129
9.2.2.5.1	AA-Request (AAR) Command .....	129

9.2.2.5.2	AA-Answer (AAA) Command.....	129
9.2.2.6	Commands for S6b Service Authorization Information Update Procedures.....	130
9.2.2.6.1	Re-Auth-Request (RAR) Command.....	130
9.2.2.6.2	Re-Auth-Answer (RAA) Command.....	130
9.2.3	Information Elements .....	131
9.2.3.1	S6b DSMIPv6 procedures.....	131
9.2.3.1.1	General .....	131
9.2.3.1.2	Visited-Network-Identifier .....	131
9.2.3.1.3	Void.....	131
9.2.3.1.4	Void.....	131
9.2.3.1.5	RAR-Flags.....	131
9.2.3.2	S6b PMIPv6 or GTPv2 procedures.....	132
9.2.3.2.1	General .....	132
9.2.3.2.2	MIP6-Agent-Info.....	132
9.2.3.2.3	MIP6-Feature-Vector .....	132
9.2.3.2.4	QoS-Capability.....	133
9.2.3.2.5	QoS-Resources .....	133
9.2.3.3	S6b Re-used Diameter AVPs .....	133
9.2.3.4	Feature-List-ID AVP.....	133
9.2.3.5	Feature-List AVP.....	133
9.2.3.6	S6b MIPv4 FACoA procedures .....	133
9.2.3.6.1	General .....	133
9.2.3.6.2	MIP6-Agent-Info.....	133
9.2.3.6.3	MIP6-Feature-Vector .....	134
9.2.3.6.4	QoS-Capability .....	134
9.2.3.6.5	QoS-Resources .....	134
9.2.3.6.6	MIP-MN-HA-SPI.....	134
9.2.3.6.7	MIP-Session-Key .....	134
9.2.3.7	DER-S6b-Flags.....	134
9.2.4	Session Handling .....	134
10	Result-Code and Experimental-Result Values .....	135
10.1	General .....	135
10.2	Success .....	135
10.3	Permanent Failures .....	135
10.3.1	General.....	135
10.3.2	DIAMETER_ERROR_USER_UNKNOWN (5001).....	135
10.3.3	DIAMETER_ERROR_IDENTITY_NOT_REGISTERED (5003).....	135
10.3.4	DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004).....	135
10.3.5	DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED (5005).....	135
10.3.6	DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION (5450).....	135
10.3.7	DIAMETER_ERROR_USER_NO_APN_SUBSCRIPTION (5451).....	136
10.3.8	DIAMETER_ERROR_RAT_TYPE_NOT_ALLOWED (5452).....	136
10.4	Transient Failures.....	136
10.4.1	General.....	136
<b>Annex A (informative):</b>	<b>Change history .....</b>	<b>137</b>
History .....		140

---

## Foreword

This Technical Specification has been produced by the 3<sup>rd</sup> Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

---

## Introduction

The present specification details the stage 3 work related to all 3GPP AAA reference points used by the different non-3GPP accesses included in EPS; it will also cover H2 reference point defined in I-WLAN mobility.

---

# 1 Scope

The present document defines the stage-3 protocol description for several reference points for the non-3GPP access in EPS.

The present document is applicable to:

- The SWa reference point between an un-trusted non-3GPP IP access and the 3GPP AAA Server/Proxy.
- The STa reference point between a trusted non-3GPP IP access and the 3GPP AAA Server/Proxy.
- The SWd reference point between the 3GPP AAA Proxy and 3GPP AAA Server.
- The SWx reference point between the 3GPP AAA Server and the HSS.
- The S6b reference point between the 3GPP AAA Server/Proxy and the PDN GW.
- The H2 reference point between the 3GPP AAA Server and the HA.
- The SWm reference point between the 3GPP AAA Server/Proxy and the ePDG.

---

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
- [2] IETF RFC 5779: "Diameter Proxy Mobile IPv6: Mobility Access Gateway and Local Mobility Anchor Interaction with Diameter Server".
- [3] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".
- [4] IETF RFC 4005: "Diameter Network Access Server Application".
- [5] IETF RFC 4072: "Diameter Extensible Authentication Protocol (EAP) Application".
- [6] IETF RFC 5447: "Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction".
- [7] IETF RFC 3588: "Diameter Base Protocol".
- [8] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".
- [9] IETF RFC 5777: "Traffic Classification and Quality of Service (QoS) Attributes for Diameter".
- [10] 3GPP TS 33.234: "3G security; Wireless Local Area Network (WLAN) interworking security".
- [11] IETF RFC 5778: "Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction".
- [12] 3GPP TS 23.327: "Mobility between 3GPP-Wireless Local Area Network (WLAN) Interworking and 3GPP Systems".

- [13] 3GPP TS 24.303: "Mobility management based on Dual-Stack Mobile IPv6; Stage 3".
- [14] 3GPP TS 23.003: "Numbering, addressing and identification".
- [15] IETF RFC 4282: "The Network Access Identifier".
- [16] 3GPP TS 33.203: "3G security; Access security for IP-based services".
- [17] 3GPP TS 29.230: "Diameter applications; 3GPP specific codes and identifiers".
- [18] IETF RFC 4004: "Diameter Mobile IPv4 Application".
- [19] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".
- [20] IETF RFC 4006: "Diameter Credit-Control Application".
- [21] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; System description".
- [22] 3GPP TS 29.228: "IP multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and Message Elements".
- [23] 3GPP TS 29.212: "Policy and Charging Control (PCC); Reference points".
- [24] 3GPP TS 29.229: "Cx and Dx interfaces based on the Diameter protocol; Protocol details".
- [25] 3GPP2 X. S0057-B: "EUTRAN – eHRPD Connectivity and Interworking: Core Network Aspects".
- [26] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks".
- [27] IETF RFC 5448: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".
- [28] IETF RFC 6611: "Mobile IPv6 (MIPv6) Bootstrapping for the Integrated Scenario".
- [29] 3GPP TS 29.272: "Evolved Packet System; MME and SGSN Related Interfaces Based on Diameter Protocol".
- [30] 3GPP TS 32.299: "Charging management; Diameter charging applications".
- [31] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".
- [32] 3GPP TS 32.422: "Telecommunication management; Subscriber and equipment trace; Trace control and configuration management".
- [33] 3GPP TS 29.234: "3GPP System to Wireless Local Area Network (WLAN) interworking".
- [34] 3GPP TS 29.303: "Domain Name System Procedures; Stage 3".
- [35] IETF RFC 1035: "Domain Names - Implementation and Specification".
- [36] Void.
- [37] IETF RFC 5729: "Clarifications on the Routing of Diameter Requests Based on the Username and the Realm".
- [38] 3GPP TS 29.274: "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3".
- [39] 3GPP TS 23.139: "3GPP System-Fixed Broadband Access Network Interworking; Stage 2".

- [40] IEEE Std 802.11-2012: "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".
- [41] Void.
- [42] Void.
- [43] 3GPP TS 24.139: "3GPP system - fixed broadband access network interworking".

---

## 3 Definitions, symbols and abbreviations

### 3.1 Definitions

#### 3.1.1 General

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**Trusted WLAN Identifier (TWID):** Identifier of a given Trusted WLAN, a combination of, e.g., an SSID and/or an HESSID as defined in IEEE Std 802.11-2012 [40].

#### 3.1.2 Handling of Information Elements

In the tables that describe the Information Elements transported by each Diameter command, each Information Element is marked as (M) Mandatory, (C) Conditional or (O) Optional in the Category "Cat." column. For the correct handling of the Information Elements and their precedence to any included ABNF definition of the command as defined according to their category types, see the description detailed in section 6 of the 3GPP TS 29.228 [22].

### 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

AE	Authentication Extension
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
eHRPD	evolved High Rate Packet Data
FA	Foreign Agent
FACoA	FA Care-of-Address
HA	Home Agent
HBM	Host Based Mobility
HESSID	Homogenous Extended Service Set Identifier
HSGW	eHRPD Serving Gateway
LMA	Local Mobility Anchor
MAG	Mobile Access Gateway
MIPv4	Mobile IP version 4
MN	Mobile Node
NBM	Network Based Mobility
NAS	Network Access Server
PBU	Proxy Binding Update
PMIP/PMIPv6	Proxy Mobile IP version 6
RRP	MIPv4 Registration Reply
RRQ	MIPv4 Registration Request
SA	Security Association

SGW	Serving Gateway
SIPTO	Selected IP Traffic Offload
SSID	Service Set Identifier
TWAN	Trusted WLAN Access Network

---

## 4 SWa Description

### 4.1 Functionality

#### 4.1.1 General

The SWa reference point is defined between the untrusted non-3GPP IP access and the 3GPP AAA Server or Proxy. The definition of the reference point and its functionality is given in 3GPP TS 23.402 [3].

The SWa reference point is optionally used to authenticate and authorize the UE for the access to the EPS. It is up to the non-3GPP operator's policy whether this interface and the procedures defined in this section are used.

NOTE: From the EPS operator's view, the tunnel authentication and authorization procedures described in clause 7 (SWm description) and clause 9 are required to ensure the user's authentication and authorization when the UE is attached to an untrusted non-3GPP IP access.

The same procedures as defined for STa reference points are used also in the SWa, but with reduced message content. As an exception, the service authorization information update procedure is not applicable for the SWa reference point.

#### 4.1.2 Procedure Descriptions

##### 4.1.2.1 SWa Authentication and Authorization procedure

###### 4.1.2.1.1 General

This procedure follows the STa Authentication and Authorization procedure, with the following differences:

- Information elements that would reflect information about the user's service request and about the access network are not included or are optional in the authentication and authorization request.
- The information elements that describe the user's subscription profile are not downloaded to the non-3GPP access network.

NOTE: The information elements related to the IP Mobility Mode Selection function are not supported over this interface.

Table 4.1.2.1/1: SWa Authentication and Authorization Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in the IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
EAP payload	EAP-payload	M	This IE shall contain the Encapsulated EAP payload used for the UE – 3GPP AAA Server mutual authentication
Authentication Request Type	Auth-Request-Type	M	This IE shall define whether the user is to be authenticated only, authorized only or both. AUTHORIZE_AUTHENTICATE shall be used in this case.
UE Layer-2 address	Calling-Station-ID	M	This IE shall carry the Layer-2 address of the UE.
Access Type	RAT-Type	C	If present, this IE shall contain the untrusted non-3GPP access network technology type that is serving the UE.
Access Network Identity	ANID	O	If present, this IE shall contain the access network identifier used for key derivation at the HSS. (See 3GPP TS 24.302 [26] for all possible values) It shall be included if the non-3GPP access network selects the EAP-AKA' authentication method.
Full Name for Network	Full-Network-Name	O	If present, this IE shall contain the full name for network as specified in 3GPP TS 24.302 [26]. This AVP may be inserted by the non-3GPP access network depending on its local policy and only when it is not connected to the UE's Home Network
Short Name for Network	Short-Network-Name	O	If present, this IE shall contain the short name for network as specified in 3GPP TS 24.302 [26]. This AVP may be inserted by the non-3GPP access network depending on its local policy and only when it is not connected to the UE's Home Network
Transport Access Type	Transport-Access-Type	C	For interworking with Fixed Broadband access networks (see 3GPP TS 23.139 [39]), if the access network needs to receive the IMSI of the UE in the authentication response, then this information element shall be present, and it shall contain the value "BBF" (see subclause 5.2.3.19).
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.

Table 4.1.2.1/2: SWa Authentication and Authorization Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
EAP payload	EAP payload	M	This IE shall contain the Encapsulated EAP payload used for UE-3GPP AAA Server mutual authentication.
Authentication Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_AUTHENTICATE. See IETF RFC 4072 [5].
Result code	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. Result codes are as in Diameter Base Protocol (IETF RFC 3588 [7]). Experimental-Result AVP shall be used for SWa errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Session Alive Time	Session-Timeout	O	This AVP may be present if the Result-Code AVP is set to DIAMETER_SUCCESS. If present, it shall contain the maximum number of seconds the user session is allowed to remain active.
Accounting Interim Interval	Accounting Interim-Interval	O	If present, this IE shall contain the Charging duration

Pairwise Master Key	EAP-Master-Session-Key	C	This IE shall be present if the Result-Code AVP is set to DIAMETER_SUCCESS.
3GPP AAA Server Name	Redirect-Host	C	This information element shall be present if the Result-Code value is set to DIAMETER_REDIRECT_INDICATION. When the user has previously been authenticated by another 3GPP AAA Server, it shall contain the Diameter identity of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter Base Protocol (IETF RFC 3588 [7]). The command shall contain zero or one occurrence of this information element.
Trust Relationship Indicator	AN-Trusted	M	This AVP shall contain the 3GPP AAA Server's decision on handling the non-3GPP access network, i.e. trusted or untrusted. For the SWa case, the value 'UNTRUSTED' shall be used.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.
Permanent User Identity	Mobile-Node-Identifier	C	This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS and if the Transport Access Type in the request command indicated that the UE is accessing the EPC from a Fixed Broadband access network (i.e., the Transport-Access-Type AVP takes the value "BBF"); it shall contain an AAA/HSS assigned permanent user identity (i.e. an IMSI in EPC root NAI format as defined in clause 19 of 3GPP TS 23.003 [14]) to be used by the non-3GPP access network in subsequent PCC procedure for identifying the user in the EPS network. This IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.

#### 4.1.2.1.2 3GPP AAA Server Detailed Behaviour

The detailed behaviour of the 3GPP AAA Server follows the behaviour defined for the STa Authentication and Authorization procedure (refer to clause 5.1.2.1.2), with the following deviations:

- The 3GPP AAA Server shall handle the non-3GPP access network as untrusted.
- The 3GPP AAA Server marks the trust relationship as "untrusted" with the User Identity.
- The authentication method shall be selected based on the presence of the Access Network Identity: if this information element is present, EAP-AKA' method is used; otherwise, EAP-AKA method is used

#### 4.1.2.1.3 3GPP AAA Proxy Detailed Behaviour

The detailed behaviour of the 3GPP AAA Proxy follows the behaviour defined for the STa Authentication and Authorization procedure (refer to clause 5.1.2.1.3), with the following exceptions:

- The 3GPP AAA Proxy shall insert Visited-Network-Identifier AVP before forwarding the request to the 3GPP AAA Server.
- The 3GPP AAA Proxy shall handle the non-3GPP access network as untrusted and marks the trust relationship as "untrusted".

On receipt of the authentication and authorization answer that completes a successful authentication, the 3GPP AAA Proxy shall record the authentication state of the user.

#### 4.1.2.2 SWa HSS/AAA Initiated Detach

This procedure equals with the STa HSS/AAA Initiated Detach procedure, refer to clause 5.1.2.2.

#### 4.1.2.3 SWa Non-3GPP Access Network Initiated Detach

This procedure equals with the STa Non-3GPP Access Network Initiated Detach procedure, refer to clause 5.1.2.4.

## 4.1.2.4 SWa Re-Authentication and Re-Authorization Procedure

### 4.1.2.4.1 General

This procedure is optional and it may be invoked by the 3GPP AAA Server, if the operator policies require that the re-authentication of the user for the SWa is to be renewed and the untrusted non-3GPP access network supports the re-authentication.

This procedure shall be performed in two steps:

- The 3GPP AAA server shall issue an unsolicited re-auth request towards the untrusted non-3GPP access, indicating that both re-authentication and re-authorization of the user is needed. Upon receipt of such a request, the untrusted non-3GPP access shall respond to the request and shall indicate the disposition of the request. This procedure is mapped to the Diameter command codes Re-Auth-Request and Re-Auth-Answer specified in IETF RFC 3588 [7]. Information element contents for these messages shall be as shown in tables 4.1.2.4.1/1 and 4.1.2.4.1/2.
- Upon receiving the re-auth request, the untrusted non-3GPP access shall immediately invoke the SWa authentication and authorization procedure requesting the identity of the user via EAP and using DER/DEA commands, with the same session-ID but the content adapted to the needs of a re-authentication. Information element contents for these messages shall be as shown in tables 4.1.2.4.1/3 and 4.1.2.4.1/4.

If the re-authentication of the user is not successful, the untrusted non-3GPP access shall detach the user.

**Table 4.1.2.4.1/1: SWa Re-auth request**

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15], and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Re-Auth Request Type	Re-Auth-Request-Type	M	This information element shall define whether the user is to be authorized only or authenticated and authorized. AUTHORIZE_AUTHENTICATE shall be used in this case.
Routing Information	Destination-Host	M	This information element shall be obtained from the Origin-Host AVP, which was included in a previous command received from the untrusted non-3GPP access.

**Table 4.1.2.4.1/2: SWa Re-auth response**

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Result	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for SWa errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP and the error code in the Experimental-Result-Code AVP.

**Table 4.1.2.4.1/3: SWa Authentication and Authorization Request**

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
EAP payload	EAP-payload	M	This IE shall contain the Encapsulated EAP payload used for the UE – 3GPP AAA Server mutual authentication.
Authentication Request Type	Auth-Request-Type	M	This IE shall define whether the user is to be authenticated only, authorized only or both. AUTHORIZE_AUTHENTICATE shall be used in this case.

**Table 4.1.2.4.1/4: SWa Authentication and Authorization Answer**

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
EAP payload	EAP payload	O	If present, this IE shall contain the Encapsulated EAP payload used for UE- 3GPP AAA Server mutual authentication.
Authentication Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_AUTHENTICATE. See IETF RFC 4072 [5].
Result code	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. Result codes are defined in the Diameter Base Protocol (IETF RFC 3588 [7]). The Experimental-Result AVP shall be used for SWa errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Session Alive Time	Session-Timeout	O	If present, this IE shall contain the maximum number of seconds the user session should remain active.
Accounting Interim Interval	Accounting Interim-Interval	O	If present, this IE shall contain the Charging duration.
Pairwise Master Key	EAP-Master-Session-Key	C	This IE shall be sent if Result-Code AVP is set to DIAMETER_SUCCESS.

#### 4.1.2.4.2 3GPP AAA Server Detailed Behaviour

The 3GPP AAA Server shall trigger this procedure according to the local policies configured by the operator.

The 3GPP AAA Server shall use the same authentication method that was used during the full authentication executed at the UE's attach. If EAP-AKA' is used, the 3GPP AAA Server shall use the ANID parameter received during the authentication and authorization executed at the UE attach (refer to clause 4.1.2.1.1).

#### 4.1.2.4.3 3GPP AAA Proxy Detailed Behaviour

The detailed behaviour of the 3GPP AAA Proxy follows the behaviour defined for the STa Re-Authorization and Re-Authentication Procedures (refer to clause 5.1.2.3.3), with the following addition:

- When forwarding the authorization answer or the authentication and authorization answer, the 3GPP AAA Proxy shall record the authentication state of the user.

## 4.2 Protocol Specification

### 4.2.1 General

The SWa reference point shall use the same Diameter application as the STa reference point. The first authentication command exchange (DER/DEA) is common between the SWa and STa reference points. During this initial exchange, the 3GPP AAA Server determines the HPLMN's trust relationship with the non-3GPP access network and communicates it to the non-3GPP access network and the UE as described in section 5.1.2.1.2. The contents of the subsequent commands are dependent on this trust relationship determination and are specific to the SWa or STa reference points.

### 4.2.2 Commands

#### 4.2.2.1 Commands for SWa authentication and authorization procedures

##### 4.2.2.1.1 Diameter-EAP-Request (DER) Command

The Diameter-EAP-Request (DER) command, indicated by the Command-Code field set to 268 and the "R" bit set in the Command Flags field, is sent from a trusted non-3GPP access network to a 3GPP AAA Server.

```

< Diameter-EAP-Request > ::=
    < Diameter Header: 268, REQ, PXY >
        < Session-Id >
        { Auth-Application-Id }
        { Origin-Host }
        { Origin-Realm }
        { Destination-Realm }
        { Auth-Request-Type }
        { EAP-Payload }
        [ User-Name ]
        [ Calling-Station-Id ]
        [ RAT-Type ]
        ...
        [ ANID ]
        [ Full-Network-Name ]
        [ Short-Network-Name ]
        *[ Supported-Features ]
        [ Transport-Access-Type ]
        ...
        *[ AVP ]

```

##### 4.2.2.1.2 Diameter-EAP-Answer (DEA) Command

The Diameter-EAP-Answer (DEA) command, indicated by the Command-Code field set to 268 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA Server to a trusted non-3GPP access network NAS.

```

< Diameter-EAP-Answer > ::=
    < Diameter Header: 268, PXY >
        < Session-Id >
        { Auth-Application-Id }
        { Result-Code }
        [ Experimental-Result ]
        { Origin-Host }
        { Origin-Realm }
        { Auth-Request-Type }
        [ EAP-Payload ]
        [ User-Name ]
        [ Session-Timeout ]
        [ Accounting-Interim-Interval ]
        [ EAP-Master-Session-Key ]

```

```

    * [ Redirect-Host ]
    [ AN-Trusted ]
    * [ Supported-Features ]
    [ Mobile-Node-Identifier ]
    ...
    * [ AVP ]

```

#### 4.2.2.2 Commands for SWa HSS/AAA Initiated Detach

Refer to clause 5.2.2.2.

#### 4.2.2.3 Commands for Untrusted non-3GPP Access network Initiated Session Termination

Refer to clause 5.2.2.4.

#### 4.2.2.4 Commands for SWa Re-Authentication and Re-Authorization Procedures

##### 4.2.2.4.1 Re-Auth-Request (RAR) Command

The Diameter Re-Auth-Request (RAR) command, indicated by the Command-Code field set to 258 and the "R" bit set in the Command Flags field, shall be sent from a 3GPP AAA server to an untrusted non-3GPP access network NAS. ABNF for the RAR command shall be as follows:

```

< Re-Auth-Request > ::= < Diameter Header: 258, REQ, PXY, 16777250 >
                        < Session-Id >
                        { Origin-Host }
                        { Origin-Realm }
                        { Destination-Realm }
                        { Destination-Host }
                        { Auth-Application-Id }
                        { Re-Auth-Request-Type }
                        [ User-Name ]
                        ...
                        * [ AVP ]

```

##### 4.2.2.4.2 Re-Auth-Answer (RAA) Command

The Diameter Re-Auth-Answer (RAA) command, indicated by the Command-Code field set to 258 and the "R" bit cleared in the Command Flags field, shall be sent from an untrusted non-3GPP access network NAS to a 3GPP AAA server. ABNF for the RAA command shall be as follows:

```

< Re-Auth-Answer > ::= < Diameter Header: 258, PXY, 16777250 >
                       < Session-Id >
                       { Result-Code }
                       { Origin-Host }
                       { Origin-Realm }
                       ...
                       * [ AVP ]

```

##### 4.2.2.4.3 Diameter-EAP-Request (DER) Command

Refer to clause 4.2.2.1.1.

##### 4.2.2.4.4 Diameter-EAP-Answer (DEA) Command

Refer to clause 4.2.2.1.2

### 4.2.3 Information Elements

The information elements of SWa are the same as the IEs defined for the STa interface described in the clause 5.2.3.

## 4.2.4 Session Handling

The session handling for the SWa interface is the same as the STa session handling described in the clause 5.2.4.

---

# 5 STa Description

## 5.1 Functionality

### 5.1.1 General

The STa reference point is defined between a non-3GPP access network and the 3GPP AAA Server or between a non-3GPP access network and the 3GPP AAA Proxy. The definition of the reference point and its functionality is given in 3GPP TS 23.402 [3].

Whether a Non-3GPP access network is Trusted or Untrusted is not a characteristic of the access network; this decision shall be made during the access authentication and authorization procedure executed between the non-3GPP access network and the 3GPP AAA Server. This is implemented by the STa and SWa reference points sharing the same Diameter application and partly sharing the same authentication and authorization procedure. The STa and SWa reference points are clearly distinguished after the exchange of the first authentication and authorization messages, during which trusted/untrusted decision is made by the 3GPP AAA server and this decision is communicated to the non-3GPP access network. The other procedures are specific to the STa and SWa reference points.

The STa reference point shall be used to authenticate and authorize the UE.

The STa reference point may also be used to transport PMIPv6, GTPv2, or MIPv4 FA-CoA mode related mobility parameters in a case the UE attaches to the EPC using the S2a reference point. The procedures specified for EPC access via GTP based S2a are only applicable to trusted WLAN access networks (see clause 16 of 3GPP TS 23.402 [3]).

Additionally the STa reference point may also be used to transport DSMIPv6 related mobility parameters in case the UE attaches to the EPC using the S2c reference point. In particular, in this case the STa reference point may be used for conveying the Home Agent IP address or FQDN from the AAA server to the gateway of the trusted non-3GPP access for Home Agent discovery based on DHCPv6 (see TS 24.303 [13]).

This reference point shall be also used to transport charging-related information and optionally information about IP Mobility Mode Selection.

### 5.1.2 Procedures Description

#### 5.1.2.1 STa Access Authentication and Authorization

##### 5.1.2.1.1 General

These procedures are transported over Diameter, the Access (Re-)Authentication and Authorization between the trusted non-3GPP access network and the 3GPP AAA Proxy or Server. The STa interface and Diameter application shall be used for authenticating and authorizing the UE for EPC access in PMIPv6, GTPv2, MIPv4 FA-CoA mode or for TWAN access without EPC S2a access (i.e. non-seamless WLAN offload) via trusted non-3GPP accesses and non-3GPP accesses that are decided to be untrusted during the authentication and authorization procedure.

When EAP-AKA' is used in the STa access authentication and either EPC access in NBM (PMIPv6 or GTPv2) or TWAN access without EPC S2a access (i.e. non-seamless WLAN offload) is used, the trusted non-3GPP access network shall support also the role of the NAS. Specifically in the case where PMIPv6 is used, the network element of the non-3GPP access network acting as a MAG shall have also the role of the NAS. During the STa access authentication the NAS shall serve as pass-through EAP authenticator.

Diameter usage over the STa interface:

- When EAP is used, the trusted non-3GPP access authentication and authorization procedure shall be mapped to the Diameter-EAP-Request and Diameter-EAP-Answer command codes specified in IETF RFC 4072 [5].

- For (re)authentication procedures, the messaging described below shall be reused.

During the STa Access Authentication and Authorization procedure the non-3GPP access network may provide information on its PMIPv6 or GTPv2 capabilities to the 3GPP AAA Server.

During the STa Access Authentication and Authorization procedure the trusted non-3GPP access network shall provide information on the Access Network Identity (ANID) to the 3GPP AAA Server. Specifically the TWAN shall set the Access Network Identity as specified in subclause 8.1.1.2 of 3GPP TS 24.302 [26] for a WLAN access network.

For a trusted non-3GPP access, the 3GPP AAA Server may perform IP mobility mode selection between NBM and HBM. The 3GPP AAA Server may provide to the trusted non-3GPP access network an indication if either NBM or local IP address assignment (for HBM) shall be used.

For a trusted WLAN access, if the user is successfully authenticated and authorized for this access, the 3GPP AAA Server may either only authorize the user to access to EPC via S2a (i.e. EPC-routed service only), or only authorize the user to access the TWAN without granting access to EPC via S2a (i.e. non-seamless WLAN offload service only), or authorize both EPC-routed and non-seamless WLAN offload services. The TWAN decides the S2a protocol variant to use if access to EPC is authorized and the TWAN decides to establish S2a.

When authorizing NBM to be used, the 3GPP AAA server shall return NBM related information back to the trusted non-3GPP access network.

During the STa Access Authentication and Authorization procedure, when DSMIPv6 is used, the 3GPP AAA Server may provide a Home Agent IPv6 address (and optionally IPv4 address) or FQDN to the trusted non-3GPP access network. This is needed if the DHCPv6 option for Home Agent address discovery is chosen (see TS 24.303 [13] and IETF RFC 6611 [28]). If the Home Agent IPv6 address or FQDN is not included in the final Authentication and Authorization Answer by the 3GPP AAA server, the trusted non-3GPP access network shall not assign the Home Agent via DHCPv6.

During the STa Access Authentication and Authorization procedure for MIPv4 FA-CoA mode using trusted non-3GPP access, the 3GPP AAA Server may provide the mobility security parameters FA-RK and FA-RK-SPI to the trusted non-3GPP access network.

The User-Name AVP may contain a decorated NAI (as defined in clause 19 of 3GPP TS 23.003 [14]) in a roaming case. In this case the 3GPP AAA Proxy shall process the decorated NAI and support routing of the Diameter request messages based on the decorated NAI as described in IETF RFC 5729 [37].

For UEs where the IMSI is not available, the Authentication and Authorization procedures shall not be used over the STa interface. For UEs receiving emergency services, where the IMSI is available, the Authentication and Authorization procedures shall be used, but if they fail, the procedures shall proceed as if they succeeded on the non-3GPP access network.

For PMIPv6, GTPv2 and MIPv4 FA-CoA mode trusted non-3GPP accesses, upon mobility between 3GPP and non-3GPP accesses, for the PDNs the UE is already connected, the PDN Gateway identity for each of the already allocated PDN Gateway(s) with the corresponding PDN information is provided to the trusted non-3GPP system. The PDN Gateway identity is a FQDN and/or IP address of the PDN GW. The non-3GPP access network shall use the received PDN Gateway identity for mobility with IP address preservation or in case of static PDN Gateway assignment. If a FQDN is provided, the trusted non-3GPP system shall then derive it to IP address according to the selected mobility management protocol.

NOTE: Mobility with IP address preservation is not supported between TWAN and 3GPP access in this release of the specification.

Table 5.1.2.1/1: STa Access Authentication and Authorization Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
EAP payload	EAP-payload	O	If present, this IE shall contain the Encapsulated EAP payload used for the UE – 3GPP AAA Server mutual authentication
Authentication Request Type	Auth-Request-Type	M	This IE shall define whether the user is to be authenticated only, authorized only or both. AUTHORIZE_AUTHENTICATE shall be used in this case.
UE Layer-2 address	Calling-Station-ID	M	This IE shall contain the Layer-2 address of the UE.
Supported 3GPP QoS profile	QoS-Capability	O	If the non-3GPP access network supports QoS mechanisms, this information element may be included to contain the access network's QoS capabilities as defined in IETF RFC 5777 [9].
Mobility Capabilities	MIP6-Feature-Vector	C	This information element shall contain the mobility capabilities of the non-3GPP access network. This information shall be utilized if dynamic mobility mode selection is executed. This information may also be used to decide whether to authorize access to EPC to a user accessing a TWAN.  The PMIP6_SUPPORTED flag and/or the GTPv2 SUPPORTED flag shall be set if the non-3GPP access supports PMIPv6 and/or GTPv2. PMIP6_SUPPORTED flag is defined in IETF RFC 5779 [2].  The flag MIP6_INTEGRATED shall be set if DHCPv6 based Home Agent address discovery is supported as defined in IETF RFC 5447 [6].  The MIP4_SUPPORTED flag shall be set if the non-3GPP access supports MIPv4 FA-CoA mode.
Access Type	RAT-Type	M	This IE shall contain the non-3GPP access network technology type that is serving the UE. The TWAN shall set the Access Type value to "WLAN".
Access Network Identity	ANID	M	This IE shall contain the access network identifier used for key derivation at the HSS. (See 3GPP TS 24.302 [26] for all possible values)
Full Name for Network	Full-Network-Name	O	If present, this IE shall contain the full name for network as specified in 3GPP TS 24.302 [26]. This AVP may be inserted by the non-3GPP access network depending on its local policy and only when it is not connected to the UE's Home Network. If the Visited Network Identifier is present, this AVP shall be set.
Short Name for Network	Short-Network-Name	O	If present, this IE shall contain the short name for network as specified in 3GPP TS 24.302 [26]. This AVP may be inserted by the non-3GPP access network depending on its local policy and only when it is not connected to the UE's Home Network. If the Visited Network Identifier is present, this AVP shall be set.
Visited Network Identifier	Visited-Network-Identifier	O	If present, this IE shall contain the Identifier that allows the home network to identify the Visited Network. This AVP may be inserted by the non-3GPP access network depending on its local policy and only when it is not connected to the UE's Home Network.
APN Id	Service-Selection	O	If present, this information element shall contain the Network Identifier part of the APN the user wants to connect to (if available).
Terminal Information	Terminal-Information	O	If present, this information element shall contain information about the user's mobile equipment. The type of identity carried depends on the access technology type. For an HRPD access network, the 3GPP2-MEID AVP shall be included in this grouped AVP.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.

Selected Trusted WLAN Identifier	WLAN-Identifier	O	If present, this IE shall contain the WLAN Identifier selected by the UE to access the Trusted WLAN Access Network (see clause 16 of 3GPP TS 23.402 [3]).
AAA Failure Indication	AAA-Failure-Indication	O	If present, this information element shall indicate that the request is sent after the non-3GPP access network has determined that a previously assigned 3GPP AAA Server is unavailable.
DER Flags	DER-Flags	O	This Information Element contains a bit mask. See 5.2.3.20 for the meaning of the bits.
Transport Access Type	Transport-Access-Type	C	For interworking with Fixed Broadband access networks (see 3GPP TS 23.139 [39]), if the access network needs to receive the IMSI of the UE in the authentication response, then this information element shall be present, and it shall contain the value "BBF" (see subclause 5.2.3.19).

Table 5.1.2.1/2: Trusted non-3GPP Access Authentication and Authorization Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
EAP payload	EAP payload	M	This IE shall contain the Encapsulated EAP payload used for UE-3GPP AAA Server mutual authentication.
Authentication Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_AUTHENTICATE. See IETF RFC 4072 [5].
Result code	Result-Code / Experimental Result Code	M	This IE shall contain the result of the operation. Result codes are as in Diameter Base Protocol (IETF RFC 3588 [7]). Experimental-Result AVP shall be used for STa errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Session Alive Time	Session-Timeout	O	This AVP may be present if the Result-Code AVP is set to DIAMETER_SUCCESS; if present, it contains the maximum number of seconds the session is allowed to remain active.
Accounting Interim Interval	Accounting Interim-Interval	O	If present, this IE shall contain the Charging duration.
Pairwise Master Key	EAP-Master-Session-Key	C	This IE shall be present if Result-Code AVP is set to DIAMETER_SUCCESS.
Default APN	Context-Identifier	C	This AVP shall indicate the default APN for the user. If the Access Network Identity received in the Authentication and Authorization Request indicates WLAN (see subclause 8.1.1.2 of 3GPP TS 24.302 [26]), this AVP shall be set to the Default APN for Trusted WLAN if received from the HSS; otherwise this AVP shall be set to the subscriber's Default APN for 3GPP and other non-3GPP accesses. It shall only be included if NBM is authorized for use, the non-3GPP access network was decided to be trusted and the Result-Code AVP is set to DIAMETER_SUCCESS.
APN-OI replacement	APN-OI-Replacement	C	This AVP shall indicate the domain name to replace the APN-OI in the non-roaming case or in the home routed roaming case when constructing the PDN GW FQDN upon which a DNS resolution needs to be performed. See 3GPP TS 23.003 [3]. It shall only be included if NBM is authorized for use and the Result-Code AVP is set to DIAMETER_SUCCESS.

APN and PGW Data	APN-Configuration	C	<p>This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS.</p> <p>When NBM is authorized for use, this AVP shall contain the default APN, the list of authorized APNs, user profile information and PDN GW information.</p> <p>When local IP address assignment is used (for HBM), this AVP shall only be present if DHCP based Home Agent discovery is used and contain the Home Agent Information for discovery purposes.</p> <p>The trusted non-3gpp access network knows if NBM is authorized for use or if a local IP address (for HBM) is assigned based on the flags in the MIP6-Feature-Vector.</p> <p>APN-Configuration is a grouped AVP, defined in 3GPP TS 29.272 [29]. When NBM is authorized for use, the following information elements per APN may be included:</p> <ul style="list-style-type: none"> <li>- APN</li> <li>- Authorized 3GPP QoS profile</li> <li>- Statically allocated User IP Address (IPv4 and/or IPv6)</li> <li>- Allowed PDN types</li> <li>- PDN GW identity</li> <li>- PDN GW allocation type</li> <li>- VPLMN Dynamic Address Allowed</li> <li>- APN-AMBR</li> <li>- Visited Network Identifier (see subclause 5.1.2.1.4)</li> <li>- SIPTO permission</li> </ul> <p>When DSMIPv6 with HA discovery based on DHCPv6 is used, the following information elements per Home Agent may be included:</p> <ul style="list-style-type: none"> <li>- HA-APN (Home Agent APN as defined in 3GPP TS 23.003 [14])</li> <li>- Authorized 3GPP QoS profile</li> <li>- PDN GW identity</li> </ul> <p>When MIPv4 FACoA is used, the following information elements per APN may be included:</p> <ul style="list-style-type: none"> <li>- APN</li> <li>- Allowed PDN types</li> </ul>
Serving GW Address	MIP6-Agent-Info	O	<p>This AVP shall be used only in chained S2a-S8 cases and it shall be sent only if the Result-Code AVP is set to DIAMETER_SUCCESS.</p>
Mobility Capabilities	MIP6-Feature-Vector	C	<p>This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS.</p> <p>It shall contain a AAA/HSS authorized set of mobility capabilities to the trusted non-3GPP access network, if dynamic mobility mode selection between NBM and HBM is done. It shall also be sent when authorizing access to EPC to a user accessing a TWAN.</p> <p>The PMIP6_SUPPORTED and/or the GTPv2_SUPPORTED shall be set to indicate that NBM (PMIPv6 or GTPv2) is authorized for use.</p> <p>Otherwise, ASSIGN_LOCAL_IP or MIP4_SUPPORTED flag shall be set by the 3GPP AAA Server to mandate which HBM mobility protocol is used.</p> <p>The MIP6_INTEGRATED flag shall be set if a Home Agent address is provided for DHCPv6 based Home Agent address discovery. In the latter case HA information for DHCPv6 discovery is provided via the APN-Configuration AVP.</p>

Permanent User Identity	Mobile-Node-Identifier	C	<p>This information element shall be sent if NBM or MIPv4 is authorized for use, or when authorizing the user to access the TWAN without granting access to EPC S2a (i.e. non-seamless WLAN offload), and the Result-Code AVP is set to DIAMETER_SUCCESS and shall contain an AAA/HSS assigned permanent user identity (i.e. an IMSI in EPC root NAI format as defined in clause 19 of 3GPP TS 23.003 [14]) to be used:</p> <ul style="list-style-type: none"> <li>- by the MAG in subsequent PBUs as the MN-ID identifying the user in the EPS network, or</li> <li>- by the trusted non-3GPP access network in subsequent MIPv4 RRs as the MN-NAI identifying the user in the EPS network, or</li> <li>- by the trusted non-3GPP access network to derive the IMSI to be sent in subsequent Create Session Request on GTP S2a.</li> </ul> <p>This information element shall also be sent if DSMIP is authorized for use and if the Transport Access Type in the request command indicated that the UE is accessing the EPC from a Fixed Broadband access network (i.e., the Transport-Access-Type AVP takes the value "BBF"); it shall contain an AAA/HSS assigned permanent user identity (i.e. an IMSI in EPC root NAI format as defined in clause 19 of 3GPP TS 23.003 [14]) to be used:</p> <ul style="list-style-type: none"> <li>- by the non-3GPP access network in subsequent PCC procedure for identifying the user in the EPS network.</li> </ul> <p>This IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.</p>
3GPP AAA Server Name	Redirect-Host	C	<p>This information element shall be sent if the Result-Code value is set to DIAMETER_REDIRECT_INDICATION. When the user has previously been authenticated by another 3GPP AAA Server, it shall contain the Diameter identity of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter Base Protocol (IETF RFC 3588 [7]). The command shall contain zero or more occurrences of this information element. When choosing a destination for the redirected message from multiple Redirect-Host AVPs, the receiver shall send the Diameter request to the first 3GPP AAA Server in the ordered list received in the Diameter response. If no successful response to the Diameter request is received, the receiver shall send the Diameter request to the next 3GPP AAA Server in the ordered list. This procedure shall be repeated until a successful response is received from a 3GPP AAA Server.</p>
UE Charging Data	3GPP-Charging-Characteristics	O	<p>If present this information element shall contain the type of charging method to be applied to the user (see 3GPP TS 29.061 [31]).</p>
UE AMBR	AMBR	C	<p>This Information Element shall contain the UE AMBR of the user. It shall be present only if the non-3GPP access network was decided to be trusted, the Result-Code AVP is set to DIAMETER_SUCCESS and ANID is "HRPD".</p>
Trust Relationship Indicator	AN-Trusted	C	<p>This AVP shall be included only in the first authentication and authorization response. If present, it shall contain the 3GPP AAA Server's decision on handling the non-3GPP access network trusted or untrusted.</p>
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	<p>If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.</p>
FA-RK	MIP-FA-RK	C	<p>This AVP shall be present if MIPv4 FA-CoA mode is used, the MN-FA authentication extension is supported and the Result-Code AVP is set to DIAMETER_SUCCESS.</p>
FA-RK-SPI	MIP-FA-RK-SPI	C	<p>This AVP shall be present if MIP-FA-RK is present</p>

Trace information	Trace-Info	C	This AVP shall be included if the subscriber and equipment trace has been activated for the user in the HSS and signalling based activation is used to download the trace activation from the HSS to the non-3GPP access network. Only the Trace-Data AVP shall be included to the Trace-Info AVP and shall contain the following AVPs: - Trace-Reference - Trace-Depth-List - Trace-Event-List, for PGW - Trace-Collection-Entity The following AVPs may also be included in the Trace-Data AVP: - Trace-Interface-List, for PGW, if this AVP is not present, trace report generation is requested for all interfaces for PGW listed in 3GPP TS 32.422 [32] - Trace-NE-Type-List, with the only allowed value being "PDN GW". If this AVP is not included, trace activation in PDN GW is required.
MSISDN	Subscription-ID	C	This AVP shall contain the MSISDN of the UE and shall be sent if it is available and the non-3GPP access network is trusted and the Result-Code AVP is set to DIAMETER_SUCCESS.
DEA Flags	DEA-Flags	O	This Information Element contains a bit mask. See 5.2.3.21 for the meaning of the bits.

#### 5.1.2.1.2 3GPP AAA Server Detailed Behaviour

On receipt of the first DER message, the 3GPP AAA Server shall check the validity of the ANID AVP and whether the non-3GPP access network is entitled to use the included value. The correct syntax of the ANID is checked as follows:

- In a non-roaming case, i.e. when the 3GPP AAA Server receives the request directly and not via the 3GPP AAA Proxy, checking ANID is mandatory;
- In a roaming case when the request is received via an 3GPP AAA proxy, checking ANID is optional. The 3GPP AAA Server may decide to check ANID based on local configuration, e.g. depending on the received visited network identifier.
- If the checking result shows that the included ANID value is not valid (not defined by 3GPP) or that the requesting entity is not entitled to use the received ANID value, the Result-Code shall be set to DIAMETER\_UNABLE\_TO\_COMPLY.

The 3GPP AAA Server shall check if user data exists in the 3GPP AAA Server (containing valid authentication information for the current access network identity). If not, the 3GPP AAA Server shall use the procedures defined in SWx interface to obtain access authentication and authorization data.

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

If SWx authentication response indicates that:

- The user does not exist, then the 3GPP AAA Server shall respond the non-3GPP access network with Experimental-Result-Code DIAMETER\_ERROR\_USER\_UNKNOWN.
- The user does not have non-3GPP access subscription, then 3GPP AAA Server shall respond the non-3GPP access network with Experimental-Result-Code DIAMETER\_ERROR\_USER\_NO\_NON\_3GPP\_SUBSCRIPTION.
- The user is not allowed to roam in the visited network, then 3GPP AAA Server shall respond the non-3GPP access network with Experimental-Result-Code DIAMETER\_ERROR\_ROAMING\_NOT\_ALLOWED.
- The user is currently being served by a different 3GPP AAA Server, then the 3GPP AAA Server shall respond to the non-3GPP access network with the Result-Code set to DIAMETER\_REDIRECT\_INDICATION and the Redirect-Host set to the Diameter identity of the 3GPP AAA Server currently serving the user (as indicated in the 3GPP-AAA-Server-Name AVP returned in the SWx authentication response from the HSS).

- Any other error occurred, then the error code `DIAMETER_UNABLE_TO_COMPLY` shall be returned to the non-3GPP access network.

When SWx authentication response includes the requested authentication information, the 3GPP AAA Server shall proceed with the authentication and authorization procedure. The 3GPP AAA Server shall use the procedures defined in SWx interface to obtain the user's subscription profile from HSS.

Before sending out the authentication challenge, the 3GPP AAA Server shall decide, whether the access network is handled as Trusted or Untrusted. The 3GPP AAA Server shall make the decision based on the Access Network Identifier and Visited Network Identity information elements, according to its local policies. The local policies of the 3GPP AAA Server shall be based on the security criteria described in 3GPP TS 33.402 [19].

NOTE 1: The network operator can configure this e.g. according to the roaming agreements with the non-3GPP AN operator or with VPLMN operator.

In a roaming case, if the 3GPP AAA Server has received the trust relationship indicator from the VPLMN (AN-Trusted AVP), the 3GPP AAA Server may use this information as input parameter to the trusted/untrusted evaluation.

The VPLMN trust relationship indicator may be utilized only if the appropriate trust relationship exists between the HPLMN and VPLMN operators.

If the 3GPP AAA Server has decided to take the received trust relationship indicator into account, it shall combine its own decision (taken as described above) with the received trust relationship indicator in a way that the final decision shall be "trusted" only if both initial decisions were "trusted"; otherwise, the final decision shall be "untrusted".

Based on the trusted/untrusted decision, the 3GPP AAA Server may send a trust relationship indication to the UE, as described in 3GPP TS 24.302 [26].

The 3GPP AAA Server shall indicate the trust relationship assessment of the non-3GPP access network to the UE in the `AT_TRUST_IND` attribute (in the EAP-Request/AKA'-Challenge) as defined in 3GPP TS 24.302 [26]. The 3GPP AAA Server shall also indicate the trust relationship assessment to the non-3GPP access network using AN-Trusted AVP in the DEA command.

If the decision is "Trusted", the STa authentication and authorization procedure is executed as described here, in clause 5.1.2.1 and its subclauses. Otherwise, the SWa authentication and authorization procedure is executed as described in clause 4.1.2.1.

The 3GPP AAA Server marks the trust relationship as "trusted" with the User Identity. If the 3GPP AAA Server detects that an S6b session already exists for the corresponding UE and the S6b session was established as a result of an authentication request for DSMIPv6, the 3GPP AAA Server shall send the trust relationship to the PDN GW as specified in clause 9.1.2.5.

The 3GPP AAA Server shall run EAP-AKA' authentication as specified in 3GPP TS 33.402 [19]. Exceptions shall be treated as error situations and the result code shall be set to `DIAMETER_UNABLE_TO_COMPLY`.

Once authentication is successfully completed, the 3GPP AAA Server shall perform the following authorization checking (if there is an error in any of the steps, the 3GPP AAA Server shall stop processing and return the corresponding error):

- 1) Check if the user is barred to use the non 3GPP Access. If it is so, then the Result-Code shall be set to `DIAMETER_AUTHORIZATION_REJECTED`
- 2) Check RAT-Type AVP. If
  - the access type indicates any value not described in 3GPP TS 29.212 [23] or
  - the received RAT-Type is listed in the user's disallowed RAT-Types,this shall be treated as error and the Result-Code `DIAMETER_UNABLE_TO_COMPLY` shall be returned.

The following steps are only executed if the non-3GPP access network was decided to be Trusted.

- 3) Check if the user has a subscription for the requested APN if present, or for the wildcard APN. If not, Experimental-Result-Code shall be set to `DIAMETER_ERROR_USER_NO_APN_SUBSCRIPTION`

4) for a trusted WLAN access (i.e. ANID in the request indicates WLAN, see subclause 8.1.1.2 of 3GPP TS 24.302 [26]), check if the user is authorized to access to EPC via S2a and/or non-seamless WLAN offload via the selected WLAN:

- if no TWAN-Access-Info AVP was received from the HSS in the user's subscription, the 3GPP AAA Server shall consider that access to EPC and non-seamless WLAN Offload is authorized;
- if one or more TWAN-Access-Info AVP(s) was received from the HSS in the user's subscription:
  - if the TWAN has signalled the selected Trusted WLAN in the request and the selected Trusted WLAN identifier contains only the SSID of the selected WLAN, the 3GPP AAA Server shall authorize the access methods allowed by the TWAN-Access-Info AVP explicitly matching the selected trusted WLAN (i.e. including a WLAN-Identifier AVP with the same SSID and without HESSID information) if any;

NOTE 2: When the TWAN does not include the HESSID in the request, the authorization information in the 3GPP AAA Server containing both SSID and HESSID is not applicable; therefore, in order to get specific authorization of the UE in this case, the operator needs to define authorization information for the SSID in question (without HESSID), or to rely on the "wildcard" authorization (i.e., a TWAN-Access-Info AVP not including a WLAN-Identifier AVP).

- if the TWAN has signalled the selected Trusted WLAN in the request and the selected Trusted WLAN identifier contains both the SSID and the HESSID of the selected WLAN, the 3GPP AAA Server shall authorize the access methods allowed by the TWAN-Access-Info AVP explicitly matching the selected trusted WLAN (i.e. including a WLAN-Identifier AVP with the same SSID and same HESSID);

Else, if no match is found, the 3GPP AAA Server shall authorize the access methods allowed by the TWAN-Access-Info AVP explicitly matching the HESSID of the selected Trusted WLAN identifier (i.e. TWAN-Access-Info including a WLAN-Identifier AVP with the same HESSID and without SSID information);

Else, if no match is found, the 3GPP AAA Server shall authorize the access methods allowed by the TWAN-Access-Info AVP explicitly matching the SSID of the selected Trusted WLAN identifier (i.e. TWAN-Access-Info including a WLAN-Identifier AVP with the same SSID and without HESSID information) ;

- otherwise, if the selected Trusted WLAN does not match explicitly any of the TWAN-Access-Info or if TWAN has not signalled the selected Trusted WLAN Identifier, the 3GPP AAA Server shall apply the access methods allowed by the "wildcard" TWAN-Access-Info AVP (i.e. TWAN-Access-Info AVP not including a WLAN-Identifier AVP) if any;
- otherwise, if the "wildcard" TWAN-Access-Info is not present, the 3GPP AAA Server shall consider that access to EPC and non-seamless WLAN Offload is not authorized.

5) Check if the user is not authorized to perform non-seamless WLAN Offload and, if the user is also barred from using the subscribed APNs, then the Result-Code shall be set to DIAMETER\_AUTHORIZATION\_REJECTED.

6) If present, check the flags of the received MIP6-Feature-Vector AVP:

- If the MIP6-INTEGRATED flag is set and the 3GPP AAA Server has authorized DHCP Home Agent assignment, the 3GPP AAA Server shall include the Home Agent addresses in the APN-Configuration AVP in the response and the MIP6-Feature-Vector AVP with the MIP6-INTEGRATED flag set. If the HA assignment via DHCPv6 is not used, the MIP6-Feature-Vector AVP with the MIP6-INTEGRATED flag not set shall be sent.
- The PMIP6\_SUPPORTED and/or GTPv2 SUPPORTED flag indicates to the 3GPP AAA Server whether the trusted non-3GPP access network supports NBM or not.

As specified in 3GPP TS 23.402 [3], based on the information it has regarding the UE (see 3GPP TS 24.302 [26]), local/home network capabilities and local/home network policies, the 3GPP AAA Server may perform mobility mode selection between NBM and HBM.

For a trusted WLAN access, if the user is successfully authenticated and authorized for this access, the 3GPP AAA Server may either only authorize the user to access to EPC via S2a (i.e. EPC-routed service only), or only authorize the user to access the TWAN without granting access to EPC via S2a (i.e. non-seamless WLAN offload service only), or authorize both EPC-routed and non-seamless WLAN offload services,

taking also into account the subscriber profile, access network, the selected WLAN identifier if present, and the TWAN's non-seamless WLAN offload capability if present. The 3GPP AAA Server may authorize both EPC-routed and non-seamless WLAN offload services only in non-roaming scenarios; the 3GPP AAA Server shall not authorize both EPC-routed and non-seamless WLAN offload services in roaming scenarios.

If the 3GPP AAA Server decides that access to EPC is authorized and NBM should be used for such access, the PMIP6\_SUPPORTED and GTPv2\_SUPPORTED flags shall be set in the response to indicate that NBM is authorized for use for the UE by the trusted non 3GPP access network. If only the PMIPv6\_SUPPORTED or the GTPv2\_SUPPORTED flag is present in the response, the trusted non-3GPP access network shall assume that this also indicates that NBM is authorized for use. In addition, for a trusted WLAN access, the Non-seamless WLAN offload Authorization flag shall be set in the DEA-Flags AVP in the response if the non-seamless WLAN offload is authorized.

If the 3GPP AAA Server decides to only authorize the user to access the TWAN without granting access to EPC S2a (i.e. non-seamless WLAN offload service only), none of the flags (PMIP6\_SUPPORTED, GTPv2\_SUPPORTED, MIP4\_SUPPORTED, MIP6-INTEGRATED, ASSIGN\_LOCAL\_IP) shall be set in the response, i.e. the Mobility Capabilities IE is not sent in the response, and the Non-seamless WLAN offload Authorization flag shall be set in the DEA-Flags AVP in the response.

If the 3GPP AAA Server decides that a local IP address should be assigned for HBM, the ASSIGN\_LOCAL\_IP flag shall be set in the response to indicate to the trusted non 3GPP access network that a local IP address (for HBM) should be assigned.

The 3GPP AAA Server shall not set the PMIP6\_SUPPORTED/GTPv2\_SUPPORTED and ASSIGN\_LOCAL\_IP flags both at the same time in the response.

- The MIP4\_SUPPORTED flag indicates to the 3GPP AAA Server whether the trusted non-3GPP access network supports MIPv4 FA-CoA mode or not. As specified in 3GPP TS 23.402 [3], based on the information it has regarding the UE (see 3GPP TS 24.302 [26]), local/home network capabilities and local/home network policies, the 3GPP AAA Server may perform mobility mode selection. If the 3GPP AAA Server decides that MIPv4 FA-CoA mode should be used, the MIP4\_SUPPORTED flag shall be set in the response.

NOTE 3: When selecting DSMIPv6 the AAA server assumes that the trusted non 3GPP access gateway has the capability to assign a local IP address to the UE.

Once the Authentication and Authorization procedure successfully finishes, the 3GPP AAA Server shall download, together with authentication data, the list of authorized APN's and the authorized mobility protocols in the authentication and authorization response from the HSS (see SWx procedure in Section 8.1.2.1). If the Access Network Identity received in the Authentication and Authorization Request indicates WLAN (see subclause 8.1.1.2 of 3GPP TS 24.302 [26]), the 3GPP AAA Server shall set the Default APN in the Authentication and Authorization Answer to the Default APN for Trusted WLAN if received from the HSS, otherwise to the subscriber's Default APN for 3GPP and other non-3GPP accesses.

Once the Authentication and Authorization procedures successfully finish and if MIPv4 FACoA mode is used the 3GPP AAA Server shall calculate the MIPv4 FACoA mobility security parameters as defined in 3GPP TS 33.402 [19] and include these in the authentication and authorization response to the trusted non 3GPP access network.

Exceptions to the cases specified here shall be treated by 3GPP AAA Server as error situations, the Result-Code shall be set to DIAMETER\_UNABLE\_TO\_COMPLY and, therefore, no authorization information shall be returned.

### 5.1.2.1.3 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy is required to handle roaming cases in which the non-3GPP access network is connected to a VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy, with the following additions.

On receipt of an authentication and authorization request, the 3GPP AAA Proxy

- shall check the Visited-Network-Identifier AVP,
- If the AVP is not present, the 3GPP AAA Proxy shall insert it before forwarding the request to the 3GPP AAA Server.

- If the AVP is present, the 3GPP AAA Proxy may check and overwrite its value, depending on its local policy, e.g. the trusted non-3GPP access network being operated by the VPLMN operator or by a third party.
- shall check the ANID AVP. If the result of the checking shows that the included ANID value is not valid (not defined by 3GPP) or that the requesting entity is not entitled to use the received value, the Result-Code shall be set to DIAMETER\_UNABLE\_TO\_COMPLY and the authentication response shall be sent to the trusted non-3GPP access network.
- may take a decision about the trustworthiness of the non-3GPP access from VPLMN's point of view. If such decision is taken, it shall be based on the Access Network Identifier and optionally, on further information about the non-3GPP access network, according to the 3GPP AAA Proxy's local policies. These local policies shall reflect the security criteria described in 3GPP TS 33.402 [19], with the assumption that the PDN GW will be allocated in the VPLMN.

NOTE: For example, if hop-by-hop security relationship exists between the NAS and the 3GPP AAA Proxy, the 3GPP AAA Proxy may use the Origin-Host AVP to uniquely identify the NAS and the access network.

The decision about the trustworthiness of the non-3GPP access network is encoded to the VPLMN trust relationship indicator that is inserted to the authentication and authorization request.

On receipt of the first authentication and authorization request, the 3GPP AAA Proxy shall check locally configured information whether users from the HPLMN are allowed to activate a PDN connection from the non-3GPP access network via this (V)PLMN. If not, the Experimental-Result-Code shall be set to DIAMETER\_ERROR\_ROAMING\_NOT\_ALLOWED and the authentication and authorization response shall be sent to the non-3GPP access network.

On receipt of the authentication and authorization answer that completes a successful authentication, the 3GPP AAA Proxy

- may check locally configured information about using the chained S8-S2a option towards the given HPLMN. If chaining is required, the 3GPP AAA Proxy shall select a Serving GW from its network configuration database and shall include the Serving GW address in the answer.
- shall check locally configured information for the maximum allowed static QoS parameters valid for visitors from the given HPLMN and modify the QoS parameters received from the 3GPP AAA Server, to enforce the policy limitations.
- shall record the state of the connection (i.e. Authentication and Authorization Successful).

#### 5.1.2.1.4 Trusted non-3GPP access network Detailed Behaviour

The Trusted non-3GPP access network shall initiate the Trusted non-3GPP Access Authentication and Authorization procedure when the user attaches to the access network. During the authentication, it shall act as a pass-through EAP authenticator.

If PMIPv6, GTPv2 or MIPv4 FCoA is used, at successful completion of the procedure, the trusted non-3GPP access network shall store the non-3GPP user data received from the 3GPP AAA Server. The trusted non-3GPP access network shall utilize these data

- To authorize the APNs received in PDN connection creation request from the UE;
- To authorize the requested home address types: IPv4 home address and/or IPv6 home network prefix.

NOTE: The user will be allowed to create PDN connections only to the subscribed APNs and use the address types that are allowed by the subscribed PDN types.

If DSMIPv6 is used and if the trusted non-3GPP access network has received the PGW identity in form of the FQDN from the 3GPP AAA Server, then the trusted non-3GPP access network may obtain the IP address of the Home Agent functionality of that PGW as described in 3GPP TS 29.303 [34].

If MIPv4 FCoA is used and if the non-3GPP access network has received FA-RK-SPI and FA-RK from the 3GPP AAA Server, the trusted non-3GPP access network will use FA-RK key and FA-RK-SPI to further derive MN-FA shared key and MN-FA-SPI, as defined in 3GPP TS 33.402 [19]. These are used to process the MN-FA Authentication Extension in the RRQ/RRP messages if the extension is present.

If the subscriber is not roaming and the SIPTO-Permission information for an APN is present, the HSGW shall allow SIPTO for that APN only if the SIPTO-Permission information indicates so. If the subscriber is not roaming and the SIPTO-Permission information for an APN is not present, the HSGW may allow SIPTO for that APN. If the subscriber is roaming and the SIPTO-Permission information for an APN is present, the HSGW shall allow SIPTO for that APN only if the SIPTO-Permission information indicates so and the VPLMN Dynamic Address is allowed and the HSGW selects a PDN GW in the VPLMN. For the requested APN allowed for SIPTO, the trusted non-3GPP access network may use the 3GPP DNS mechanism to select a PGW which is close to the HSGW. Detailed behaviour is specified in 3GPP2 X.S0057 [25], 3GPP TS 23.402 [3] and 3GPP TS 29.303 [34].

For optimized handover of an emergency session from E-UTRAN to an S2a based cdma2000<sup>®</sup> HRPD access network, if the trusted non-3GPP access network supports Emergency services for users in limited service state, then the trusted non-3GPP access network shall skip the authentication procedure (for users without an IMSI or with an IMSI marked as unauthenticated); or if the trusted non-3GPP access network accepts that the authentication may fail (for users with an IMSI), it shall continue with the procedure. For these cases, the Trusted non-3GPP access network shall release any non-emergency PDN connections.

The TWAN decides the S2a protocol variant to use if access to EPC is authorized and the TWAN decides to establish S2a. The TWAN may be configured with the S2a protocol variant(s) on a per PLMN granularity, or may retrieve information regarding the S2a protocol variants supported by the PDN GW (PMIPv6 or/and GTPv2) from the Domain Name Service Function as described in 3GPP TS 29.303[34]. For static PDN Gateway assignment, in order to determine the PLMN of the PDN GW, the TWAN may use the Visited Network Identifier, if received from the 3GPP AAA Server, or the FQDN of the PDN GW, if included in the MIP6-Agent-Info AVP of the APN in use; if none of them are available, it may use the PLMN where the 3GPP AAA Server is located.

If GTPv2 is used on S2a and if the Trace-Info AVP including Trace-Data has been received in the authorization response, the trusted non-3GPP access network shall send a GTPv2 Trace Session Activation message (see 3GPP TS 29.274 [38]) to the PGW to start a trace session for the user.

If the Trusted non-3GPP access network determines that a previously assigned 3GPP AAA Server is unavailable, it may attempt to send a new authentication and authorization request to an alternate 3GPP AAA Server. If the Trusted non-3GPP access network receives from this new server a redirect indication towards the former server (due to the HSS having stored the former 3GPP AAA Server identity), it shall terminate all previously existing sessions and PDN connections for that user, and it shall re-send again the request towards the new server, but it shall include the AAA-Failure-Indication AVP in the new request.

## 5.1.2.2 HSS/AAA Initiated Detach on STa

### 5.1.2.2.1 General

This procedure is used between the 3GPP AAA/HSS and the trusted non-3GPP access network to instruct the non-3GPP access network to detach a specific user from the access network. The procedure is based on Diameter session abort messages.

Diameter usage over the STa interface:

- This procedure is mapped to the Diameter command codes Diameter-Abort-Session-Request (ASR), Diameter-Abort-Session-Answer (ASA), Diameter-Session-Termination-Request (STR) and Diameter-Session-Termination-Answer (STA) specified in RFC 3588 [7]. Information element contents for these messages are shown in tables 5.1.2.2.1/1 and 5.1.2.2.1/2.
- The STa application id value of 16777250 shall be used as the Application Id in ASR/ASA/STR/STA commands.

**Table 5.1.2.2.1/1: Information Elements passed in ASR message**

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15], and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Auth-Session-State	Auth-Session-State	O	If present this information element shall indicate to the Non-3GPP access network whether the 3GPP AAA Server requires an STR message.

**Table 5.1.2.2.1/2: Information Elements passed in ASA message**

Information element name	Mapping to Diameter AVP	Cat.	Description
Result-Code	Result-Code	M	This IE shall indicate the result of the operation.

**Table 5.1.2.2.1/3: Information Elements passed in STR message**

Information element name	Mapping to Diameter AVP	Cat.	Description
Termination-Cause	Termination-Cause	M	This information element shall contain the reason why the session was terminated. It shall be set to "DIAMETER_ADMINISTRATIVE" to indicate that the session was terminated in response to an ASR message.

**Table 5.1.2.2.1/4: Information Elements passed in STA message**

Information element name	Mapping to Diameter AVP	Cat.	Description
Result-Code	Result-Code	M	This IE shall contain the result of the operation.

#### 5.1.2.2.2 3GPP AAA Server Detailed Behaviour

The 3GPP AAA Server shall make use of this procedure to instruct the Non-3GPP access network to detach a specific user from the access network.

In the DSMIPv6 case, the 3GPP AAA Server shall initiate first the detach procedure over the S6b reference point towards the PDN GW. When this process has finalized, the 3GPP AAA Server can initiate the detach procedure of the UE from the non-3GPP access network.

The 3GPP AAA Server shall include the Auth-Session-State AVP in the ASR command with a value of NO\_STATE\_MAINTAINED if it does not require a STR from the Non-3GPP access network. If it does require a STR from the Non-3GPP access network, the 3GPP AAA Server shall either omit the Auth-Session-State AVP from the ASR command or include the Auth-Session-State AVP in the ASR command with a value of STATE\_MAINTAINED.

On receipt of the ASR command, the Non-3GPP access network shall check if the user is known in the Non-3GPP access network. If not, Experimental-Result-Code shall be set to DIAMETER\_ERROR\_USER\_UNKNOWN.

If the user is known, the Non-3GPP access network shall perform the disconnection of all the PDN connections active for this user and remove any stored user information, except for emergency PDN connections which shall remain active, if the trusted Non-3GPP access supports Emergency services for users in limited service state.

The Non-3GPP access network shall set the Result-Code to DIAMETER\_SUCCESS and send back the ASA command to the 3GPP AAA Server, which shall update the status of the subscriber on the detached access network.

If required by the 3GPP AAA Server, the Non-3GPP access network shall send an STR with the Termination-Cause set to DIAMETER\_ADMINISTRATIVE. The 3GPP AAA Server shall set the Result-Code to DIAMETER\_SUCCESS and return the STA command to the Non-3GPP access network.

#### 5.1.2.2.3 3GPP AAA Proxy Detailed Behaviour

When the 3GPP AAA Proxy receives the ASR from the 3GPP AAA Server it shall route the request to the non-3GPP access network.

If the 3GPP AAA Proxy requires an STR but the 3GPP AAA Server does not, the 3GPP AAA Proxy may override the value of the Auth-Session-State AVP in the ASR and set it to STATE\_MAINTAINED. In this case, the 3GPP AAA Proxy shall not forward the STR received from the non-3GPP access network onto the 3GPP AAA Server and shall return an STA command to the non-3GPP access network with the Result-Code set to DIAMETER\_SUCCESS. The 3GPP AAA Proxy shall not override the value of the Auth-Session-State AVP under any other circumstances.

On receipt of the ASA message with Diameter Result Code set to DIAMETER\_SUCCESS, the 3GPP AAA Proxy shall route the successful response to the 3GPP AAA Server and shall release the resources associated with the session.

When the 3GPP AAA Proxy receives the STR from the Non-3GPP access network, it shall route the request to the 3GPP AAA Server. On receipt of the STA message, the 3GPP AAA Proxy shall route the response to the Non-3GPP access network.

### 5.1.2.3 STa Re-Authorization and Re-Authentication Procedures

#### 5.1.2.3.1 General

The STa Re-Authorization procedure shall be used between the 3GPP AAA Server and the trusted non-3GPP access network for enabling:

- the 3GPP AAA Server to modify the previously provided authorization parameters. This may happen due to a modification of the subscriber profile in the HSS (for example, removal of a specific APN associated with the subscriber, or change of the identity of a dynamically allocated PDN GW, see subclause 8.1.2.3). In this case, this procedure is performed in two steps:
  - The 3GPP AAA server shall issue an STa Re-Auth request towards the trusted non-3GPP access network. Upon receipt of such a request, the trusted non-3GPP access network shall respond to the request and shall indicate the disposition of the request. This procedure is mapped to the Diameter command Re-Auth-Request and Re-Auth-Answer specified in IETF RFC 3588 [7]. Information element contents for these messages are shown in tables 5.1.2.3.1/1 and 5.1.2.3.1/2.
  - Upon receiving the STa Re-Auth request, the non-3GPP access network shall immediately invoke the STa access authorization procedure, based on the reuse of the Diameter command codes AA-Request and AA-Answer commands specified in IETF RFC 4005 [4]. Information element contents for these messages are shown in tables 5.1.2.3.1/3 and 5.1.2.3.1/4.
- the trusted non-3GPP access network to retrieve the subscriber profile from the HSS. This procedure may be initiated at any time by the Trusted non-3GPP access network for check if there is any modification in the user authorization parameters previously provided by the 3GPP AAA Server. In this one-step procedure, the trusted non-3GPP access network shall invoke the STa access authorization procedure, based on the reuse of the Diameter commands AA-Request and AA-Answer commands IETF RFC 4005 [4]. Information element contents for these messages are shown in tables 5.1.2.3.1/3 and 5.1.2.3.1/4.

After receiving the authorization answer, the trusted non-3GPP access network will release the active PDN connections, for which the authorization has been revoked. If the authorization was rejected by the 3GPP AAA server (e.g. because the user's subscription for non-3GPP accesses has been terminated), the non-3GPP access network shall detach the user from the non-3GPP access network and release all resources. If an emergency PDN connection is active and the trusted non-3GPP access supports emergency services for users in limited service state, the non-3GPP access network shall keep the user attached in the non-3GPP access and the emergency PDN connection active. The non-emergency resources shall be released.

The STa Re-Authentication procedure shall be used between the 3GPP AAA Server and the trusted non-3GPP access network for re-authenticating the user. This procedure may be initiated at any time by the 3GPP AAA Server based on HPLMN operator policies configured in the 3GPP AAA server. This procedure is performed in two steps:

- The 3GPP AAA server issues an STa Re-Auth request towards the trusted non-3GPP access. Upon receipt of such a request, the trusted non-3GPP access network shall respond to the request and indicate the disposition of the request. This procedure is mapped to the Diameter command Re-Auth-Request and Re-Auth-Answer specified in IETF RFC 3588 [7]. Information element contents for these messages are shown in tables 5.1.2.3.1/1 and 5.1.2.3.1/2.
- Upon receiving the STa Re-Auth request, the trusted non-3GPP access network shall immediately invoke the STa Access Authentication and Authorization procedure, based on the Re-Auth Request Type provided by the 3GPP AAA server. This procedure is mapped to the Diameter command codes based on the reuse of the Diameter commands Diameter-EAP-Request and Diameter-EAP-Answer specified in IETF RFC 4072 [5]. Information element contents for these messages are shown in tables 5.1.2.3.1/5 and 5.1.2.3.1/6.

If the re-authentication of the user is not successful, the trusted non-3GPP access network will release all the active PDN connections of the user, except for emergency PDN connections which shall remain active if the trusted non-3GPP access network supports Emergency services for users in limited service state. After a successful authentication and authorization procedure, the trusted non-3GPP access network shall release the active PDN connections for which the authorization has been revoked.

**Table 5.1.2.3.1/1: STa Re-Auth request**

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Re-Auth Request Type	Re-Auth-Request-Type	M	This IE shall define whether the user is to be authorized only or authenticated and authorized. In this case, the following values shall be used: AUTHORIZE_AUTHENTICATE if the re-authentication of the user is requested; AUTHORIZE_ONLY if the update of the previously provided user authorization parameters is requested.
Routing Information	Destination-Host	M	This information element shall be obtained from the Origin-Host AVP, which was included in a previous command received from the trusted non-3GPP access.

**Table 5.1.2.3.1/2: STa Re-Auth response**

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Result	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for STa errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

Table 5.1.2.3.1/3: STa Authorization Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Request-Type	Auth-Request-Type	M	This IE shall define whether the user is to be authenticated only, authorized only or both. In this case, it shall have the value: AUTHORIZE_ONLY
Mobility Capabilities	MIP6-Feature-Vector	C	This information element shall contain the mobility capabilities of the non-3GPP access network. This AVP shall be included only if optimized idle mode mobility from E-UTRAN to HRPD access is executed. When included, the PMIP_SUPPORTED and the OPTIMIZED_IDLE_MODE_MOBILITY flags shall be set.
Routing Information	Destination-Host	M	The 3GPP AAA Server name shall be obtained from the Origin-Host AVP of a previously received message.

Table 5.1.2.3.1/4: STa Authorization response

Information element name	Mapping to Diameter AVP	Cat.	Description
Registration Result	Result Code/ Experimental Result Code	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for STa errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP
Request-Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_ONLY. See IETF RFC 4072 [5].
Session Alive Time	Session-Timeout	O	This AVP may be present if the Result-Code AVP is set to DIAMETER_SUCCESS; if present, it shall contain the maximum number of seconds the user session is allowed to remain active. This AVP is defined in IETF RFC 3588 [7].
Accounting Interim Interval	Acct-Interim-Interval	O	If present, this IE shall contain the Charging duration.
Default APN	Context-Identifier	C	This AVP shall indicate the default APN for the user. It shall only be included if NBM is authorized for use and the Result-Code AVP is set to DIAMETER_SUCCESS.
APN-OI replacement	APN-OI-Replacement	C	This AVP shall indicate the domain name to replace the APN-OI in the non-roaming case or in the home routed roaming case when constructing the PDN GW FQDN upon which it needs to perform a DNS resolution. See 3GPP TS 23.003 [3]. It shall only be included if NBM is authorized for use and the Result-Code AVP is set to DIAMETER_SUCCESS.
APN and PGW Data	APN-Configuration	C	This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS. When NBM is authorized for use, this AVP shall contain the default APN, the list of authorized APNs, user profile information and PDN GW information. When local IP address assignment is used (for HBM), this AVP shall only be present if DHCP based Home Agent discovery is used and contain the Home Agent Information for discovery purposes. The Trusted Non-3GPP access network knows if NBM is authorized for use or if a local IP address (for HBM) is assigned based on the flags in the MIP6-Feature-Vector received during the STa access authentication and authorization procedure. APN-Configuration is a grouped AVP, defined in 3GPP TS 29.272 [29]. When NBM is authorized for use, the following information elements per APN may be included: - APN - APN-AMBR - Authorized 3GPP QoS profile - Statically allocated User IP Address (IPv4 and/or IPv6) - Allowed PDN types (IPv4, IPv6, IPv4v6, IPv4_OR_IPv6) - PDN GW identity - PDN GW allocation type - VPLMN Dynamic Address Allowed - Visited Network Identifier (see subclause 5.1.2.1.4)  When DSMIPv6 with HA discovery based on DHCPv6 is used, the following information elements per Home Agent may be included: - HA-APN (Home Agent APN as defined in 3GPP TS 23.003 [14]) - Authorized 3GPP QoS profile - PDN GW identity
UE Charging Data	3GPP-Charging-Characteristics	O	If present, this information element shall contain the type of charging method to be applied to the user (see 3GPP TS 29.061 [31]).
UE AMBR	AMBR	C	This Information Element shall contain the modified UE AMBR of the user. It shall be present if the Result-Code AVP is set to DIAMETER_SUCCESS and ANID is "HRPD".
Mobility Capabilities	MIP6-Feature-Vector	C	This information element shall only be sent if it has been received in the corresponding authorization request and the Result-Code AVP is set to DIAMETER_SUCCESS. When included, the PMIP_SUPPORTED and the OPTIMIZED_IDLE_MODE_MOBILITY flags shall be set.
Trace information	Trace-Info	C	This AVP shall be included if the subscriber and equipment trace has been activated for the user in the HSS and signalling based activation is used to

			<p>download the trace activation from the HSS to the trusted non-3GPP access network.</p> <p>Only the Trace-Data AVP shall be included to the Trace-Info AVP and shall contain the following AVPs:</p> <ul style="list-style-type: none"> <li>- Trace-Reference</li> <li>- Trace-Depth-List</li> <li>- Trace-Event-List, for PGW</li> <li>- Trace-Collection-Entity</li> </ul> <p>The following AVPs may also be included in the Trace-Data AVP:</p> <ul style="list-style-type: none"> <li>- Trace-Interface-List, for PGW, if this AVP is not present, trace report generation is requested for all interfaces for PGW listed in 3GPP TS 32.422 [32]</li> <li>- Trace-NE-Type-List, with the only allowed value being "PDN GW". If this AVP is not included, trace activation in PDN GW is required.</li> </ul>
MSISDN	Subscription-ID	C	This AVP shall contain the MSISDN of the UE and shall be sent if it is available and the Result-Code AVP is set to DIAMETER_SUCCESS.

**Table 5.1.2.3.1/5: STa Access Authentication and Authorization Request**

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
EAP payload	EAP-payload	M	This IE shall contain the Encapsulated EAP payload used for the UE – 3GPP AAA Server mutual authentication
Authentication Request Type	Auth-Request-Type	M	This IE shall define whether the user is to be authenticated only, authorized only or both. In this case, it shall have the value AUTHORIZE_AUTHENTICATE.

Table 5.1.2.3.1/6: Trusted non-3GPP Access Authentication and Authorization Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and it shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
EAP payload	EAP payload	M	This IE shall contain the Encapsulated EAP payload used for UE-3GPP AAA Server mutual authentication.
Authentication Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_AUTHENTICATE. See IETF RFC 4072 [5].
Result code	Result-Code / Experimental Result Code	M	This IE shall contain the result of the operation. Result codes are as in Diameter Base Protocol (IETF RFC 3588 [7]). Experimental-Result AVP shall be used for STa errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Session Alive Time	Session-Timeout	O	This AVP may be present if the Result-Code AVP is set to DIAMETER_SUCCESS; if present, it contains the maximum number of seconds the user session is allowed to remain active. This AVP is defined in IETF RFC 3588 [7].
Accounting Interim Interval	Accounting Interim-Interval	O	If present, this IE shall contain the Charging duration.
Pairwise Master Key	EAP-Master-Session-Key	C	This IE shall be sent if Result-Code AVP is set to DIAMETER_SUCCESS.
Default APN	Context-Identifier	C	This AVP shall indicate the default APN for the user. It shall only be included if NBM is authorized for use and the Result-Code AVP is set to DIAMETER_SUCCESS.
APN-OI replacement	APN-OI-Replacement	C	This AVP shall indicate the domain name to replace the APN-OI in the non-roaming case or in the home routed roaming case when constructing the PDN GW FQDN upon which it needs to perform a DNS resolution. See 3GPP TS 23.003 [3]. It shall only be included if NBM is authorized for use and the Result-Code AVP is set to DIAMETER_SUCCESS.

APN and PGW Data	APN-Configuration	C	<p>This information element shall only be sent if the non-3GPP access network was decided to be trusted and the Result-Code AVP is set to DIAMETER_SUCCESS.</p> <p>When NBM is authorized for use this AVP shall contain the default APN, the list of authorized APNs, user profile information and PDN GW information.</p> <p>When local IP address assignment is used (for HBM), this AVP shall only be present if DHCP based Home Agent discovery is used and contain the Home Agent Information for discovery purposes.</p> <p>The trusted non-3GPP access network knows if NBM is authorized for use or if a local IP address (for HBM) is assigned based on the flags in the MIP6-Feature-Vector.</p> <p>APN-Configuration is a grouped AVP, defined in 3GPP TS 29.272 [29]. When NBM is authorized for use, the following information elements per APN may be included:</p> <ul style="list-style-type: none"> <li>- APN</li> <li>- APN-AMBR</li> <li>- Authorized 3GPP QoS profile</li> <li>- User IP Address (IPv4 and/or IPv6)</li> <li>- Allowed PDN types (IPv4, IPv6, IPv4v6, IPv4_OR_IPv6)</li> <li>- PDN GW identity</li> <li>- PDN GW allocation type</li> <li>- VPLMN Dynamic Address Allowed</li> <li>- APN-AMBR</li> <li>- Visited Network Identifier (see subclause 5.1.2.1.4)</li> </ul> <p>When DSMIPv6 with HA discovery based on DHCPv6 is used, the following information elements per Home Agent may be included:</p> <ul style="list-style-type: none"> <li>- HA-APN (Home Agent APN as defined in 3GPP TS 23.003 [14])</li> <li>- Authorized 3GPP QoS profile</li> <li>- PDN GW identity</li> </ul>
UE Charging Data	3GPP-Charging-Characteristics	O	If present, this information element shall contain the type of charging method to be applied to the user (see 3GPP TS 29.061 [31]).
UE AMBR	AMBR	C	This Information Element shall contain the UE AMBR of the user. It shall be present only if the non-3GPP access network was decided to be trusted, the Result-Code AVP is set to DIAMETER_SUCCESS and ANID is "HRPD".
FA-RK	MIP-FA-RK	C	This AVP shall be present if MIPv4 is used, MN-FA authentication extension is supported and the Result-Code AVP is set to DIAMETER_SUCCESS.
FA-RK-SPI	MIP-FA-RK-SPI	C	This AVP shall be present if MIP-FA-RK is present
Trace information	Trace-Info	C	<p>This AVP shall be included if the subscriber and equipment trace has been activated for the user in the HSS and signalling based activation is used to download the trace activation from the HSS to the trusted non-3GPP access network.</p> <p>Only the Trace-Data AVP shall be included to the Trace-Info AVP and shall contain the following AVPs:</p> <ul style="list-style-type: none"> <li>- Trace-Reference</li> <li>- Trace-Depth-List</li> <li>- Trace-Event-List, for PGW</li> <li>- Trace-Collection-Entity</li> </ul> <p>The following AVPs may also be included in the Trace-Data AVP:</p> <ul style="list-style-type: none"> <li>- Trace-Interface-List, for PGW, if this AVP is not present, trace report generation is requested for all interfaces for PGW listed in 3GPP TS 32.422 [32]</li> <li>- Trace-NE-Type-List, with the only allowed value being "PDN GW". If this AVP is not included, trace activation in PDN GW is required.</li> </ul>
MSISDN	Subscription-ID	C	This AVP shall contain the MSISDN of the UE and shall be sent if it is available and the Result-Code AVP is set to DIAMETER_SUCCESS.

### 5.1.2.3.2 3GPP AAA Server Detailed Behaviour

#### Handling of Re-Auth Request:

The 3GPP AAA Server shall make use of this procedure to indicate the following:

- If the relevant service authorization information shall be updated in the Trusted non-3GPP access network, the Re-Auth-Request-Type shall be set to AUTHORIZE\_ONLY. This procedure may be triggered by the HSS sending a subscription data update (refer to clause 8.1.2.3) or by local policies, e.g. periodic re-authorization configured by the operator. As for the STa reference point, only a single Diameter authorization session is used for a user, this procedure is initiated for all the PDN connections of this user, i.e. a single instance of Re-authorization Request shall be used per user.
- If the re-authentication and re-authorization of the user shall be executed, the Re-Auth-Request-Type shall be set to AUTHORIZE\_AUTHENTICATE. This procedure may be triggered e.g. by the expiration of a timer started at the successful completion of the last (re-)authentication of the user, depending on the local policies configured in the 3GPP AAA Server.

#### Handling of Authorization Request:

The 3GPP AAA Server shall check that the user exists in the 3GPP AAA Server. The check shall be based on Diameter Session-Id. If not, Experimental-Result-Code shall be set to DIAMETER\_ERROR\_USER\_UNKNOWN. If the user exists, the 3GPP AAA Server shall perform the authorization checking described in chapter 5.1.2.1.2.

If the Authorization request contained the MIP6-Feature-Vector with the OPTIMIZED\_IDLE\_MODE\_MOBILITY flag set, the 3GPP AAA server shall request the user data from the HSS, in order to retrieve up-to-date PDN GW information.

#### Handling of Authentication and Authorization Requests:

The 3GPP AAA Server shall execute the re-authentication of the user, using a full authentication or fast re-authentication, as described in 3GPP TS 33.402 [19], clause 6.2 and 6.3. If full authentication is executed and there are no valid authentication vectors for the given non-3GPP access network available in the 3GPP AAA Server, it shall fetch authentication vectors from the HSS. A combined authentication and authorization shall be executed, with reduced message content described in Tables 5.1.2.3.1/5 and 5.1.2.3.1/6. The QoS-Capability, Access Network Identity, Access Type, Visited Network Identifier, Terminal Information elements received during the initial authentication and authorization procedure as well as the trustworthiness of the non-3GPP AN and the IP mobility mode selected during that procedure shall be considered as valid. If re-authentication of the user is successful and MIPv4 FACoA mode is used the 3GPP AAA Server shall create the MIPv4 FACoA security parameters as defined in 3GPP TS 33.402 [19].

If the re-authentication of the user is unsuccessful, the 3GPP AAA Server shall:

- Terminate all S6b authorization sessions connected to the user, as described in clause 9.1.2.4
- Remove all APN-PDN GW bindings from the HSS, as described in subclauses 8.1.2.2.2.1 and 8.1.2.2.2.2.
- De-register the user from the HSS, as described in subclauses 8.1.2.2.2.1 and 8.1.2.2.2.2. Depending on the cause of the re-authentication being unsuccessful, the Server Assignment Type shall be set to AUTHENTICATION\_FAILURE or AUTHENTICATION\_TIMEOUT.
- Release all resources connected to the user.

### 5.1.2.3.3 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy is required to handle roaming cases in which the Non-3GPP access network is in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy, with the following additions.

When forwarding the authorization answer or the authentication and authorization answer, the 3GPP AAA Proxy

- shall check locally configured information for the maximum allowed static QoS parameters valid for visitors from the given HPLMN and modify the QoS parameters received from the 3GPP AAA Server, to enforce the policy limitations.
- shall record the state of the connection (i.e. Authentication and Authorization Successful).

#### 5.1.2.3.4 Trusted Non-3GPP Access Network Detailed Behaviour

Upon receiving the re-auth request, the Trusted non-3GPP access network shall perform the following checks and if an error is detected, the non-3GPP access network shall stop processing the request and return the corresponding error code.

Check the Re-Auth-Request-Type AVP:

- 1) If it indicates AUTHENTICATE\_ONLY, Result-Code shall be set to DIAMETER\_INVALID\_AVP\_VALUE.
- 2) If it indicates AUTHORIZE\_AUTHENTICATE, the authentication and authorization of the user is initiated, as defined in 3GPP TS 33.402, with the Diameter message contents described by Tables 5.1.2.3.1/5 and 5.1.2.3.1/6.
- 3) If it indicates AUTHORIZE\_ONLY, the non-3GPP access network shall just perform an authorization procedure as described by Tables 5.1.2.3.1/3 and 5.1.2.3.1/4.

After successful authorization or authentication and authorization procedure, the trusted non-3GPP access network shall overwrite, for the subscriber identity indicated in the request and the received session, the current authorization information with the information received from the 3GPP AAA Server.

For the TWAN access, if the TWAN receives the PDN GW Identity from 3GPP AAA Server which is different from the currently selected PDN GW for the same APN, the TWAN shall not tear down the existing PDN connection.

The release of a PDN connection shall be initiated if the user's subscription for the APN belonging to an active PDN connection has been terminated.

If the authorization or authentication and authorization procedure was unsuccessful, the non-3GPP access network shall detach the user from the non-3GPP access and release all resources. If the trusted non-3GPP access supports emergency services for users in limited service state, and there is an emergency PDN connection active for such user, the non-3GPP access network shall keep the user attached in the non-3GPP access and the emergency PDN connection active. The non-emergency resources shall be released.

The Trusted Non-3GPP access network shall initiate the re-authorization of the user in a one-step procedure (i.e. without receiving a re-authorization request from the AAA Server) if the PDN GW information needs to be updated for optimized idle mode mobility from E-UTRAN to HRPD access.

If GTPv2 is used on S2a and if the Trace-Info AVP including Trace-Data has been received in the authorization response, the trusted non-3GPP access network shall send a GTPv2 Trace Session Activation message (see 3GPP TS 29.274 [38]) to the PGW to start a trace session for the user. If the Trace-Info AVP including Trace-Reference (directly under the Trace-Info) has been received in the authorization response, the trusted non-3GPP access network shall send a GTPv2 Trace Session Deactivation message to the PGW to stop the ongoing trace session, identified by the Trace-Reference. For details, see 3GPP TS 32.422 [32].

#### 5.1.2.4 Non-3GPP Access Network Initiated Session Termination

##### 5.1.2.4.1 General

The STa reference point allows the non-3GPP access network to inform the 3GPP AAA server that the session resources of the non-3GPP access network assigned to a given user are being released.

The procedure shall be initiated by the non-3GPP access network and removes non-3GPP access information from the 3GPP AAA Server. These procedures are based on the reuse of Diameter Base IETF RFC 3588[7] STR and STA commands

**Table 5.1.2.4.1/1: STa Session Termination Request**

Information Element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user (i.e. an IMSI in EPC root NAI format as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes).
Termination Cause	Termination-Cause	M	This IE shall contain the reason for the disconnection.

**Table 5.1.2.4.1/2: STa Session Termination Answer**

Information Element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors as defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for STa errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

#### 5.1.2.4.2 3GPP AAA Server Detailed Behaviour

Upon reception of the Session Termination Request message from the non-3GPP access network, the 3GPP AAA Server shall check that there is an ongoing session associated to the two parameters received (Session-Id and User-Name).

If an active session is found and it belongs to the user identified by the User-Name parameter, the 3GPP AAA Server shall deregister itself as the managing 3GPP AAA Server for the subscriber following the procedures listed in 8.1.2.2.2. In case of a deregistration success, the 3GPP AAA Server shall release the session resources associated to the specified session and a Session Termination Response shall be sent to the non-3GPP access network, indicating DIAMETER\_SUCCESS. If deregistration from the HSS fails, the 3GPP AAA Server shall return a Session-Termination Response with the Diameter Error DIAMETER\_UNABLE\_TO\_COMPLY.

Otherwise, the 3GPP AAA Server returns a Session Termination Response with the Diameter Error DIAMETER\_UNKNOWN\_SESSION\_ID

#### 5.1.2.4.3 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy is required to handle roaming cases in which the non-3GPP access network is located in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy.

On receipt of the Session Termination Request message from the non-3GPP access network, the 3GPP AAA Proxy shall route the message to the 3GPP AAA Server.

On receipt of the Session Termination Answer message from the 3GPP AAA Server, the 3GPP AAA Proxy shall route the message to the non-3GPP access network and it shall release any local resources associated to the specified session only if the result code is set to DIAMETER\_SUCCESS.

## 5.2 Protocol Specification

### 5.2.1 General

The STa reference point shall be based on Diameter, as defined in IETF RFC 3588 [7] and contain the following additions and extensions:

- IETF RFC 4005 [4], which defines a Diameter protocol application used for Authentication, Authorization and Accounting (AAA) services in the Network Access Server (NAS) environment.

- IETF RFC 4072 [5], which provides a Diameter application to support the transport of EAP (IETF RFC 3748 [8]) frames over Diameter.
- IETF RFC 5779 [2], which defines a Diameter extensions and application for PMIPv6 MAG to AAA and LMA to AAA interfaces.
- IETF RFC 5447 [6], which defines Diameter extensions for Mobile IPv6 NAS to AAA interface.

In the case of a trusted non-3GPP IP access where PMIPv6 is used as mobility protocol, the MAG to 3GPP AAA server or the MAG to 3GPP AAA proxy communication shall use the MAG to AAA interface functionality defined in IETF RFC 5779 [2] and the NAS to AAA interface functionality defined in IETF RFC 5447 [6].

The trusted non-3GPP access network to AAA interface functionality over the STa reference defines a new Application Id:

- "STa" with value 16777250.

The STa application reuses existing EAP (IETF RFC 4072 [5]) application commands, command ABNFs, and application logic and procedures.

## 5.2.2 Commands

### 5.2.2.1 Commands for STa PMIPv6 or GTPv2 authentication and authorization procedures

#### 5.2.2.1.1 Diameter-EAP-Request (DER) Command

The Diameter-EAP-Request (DER) command, indicated by the Command-Code field set to 268 and the "R" bit set in the Command Flags field, is sent from a non-3GPP access network NAS to a 3GPP AAA server. The ABNF is re-used from the IETF RFC 5779 [2].

```

< Diameter-EAP-Request > ::= < Diameter Header: 268, REQ, PXY, 16777250 >
    < Session-Id >
    { Auth-Application-Id }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    { Auth-Request-Type }
    { EAP-Payload }
    [ User-Name ]
    [ Calling-Station-Id ]
    ...
    [ RAT-Type ]
    [ ANID ]
    [ Full-Network-Name ]
    [ Short-Network-Name ]
    [ QoS-Capability ]
    [ MIP6-Feature-Vector ]
    [ Visited-Network-Identifier ]
    [ Service-Selection ]
    [ Terminal-Information ]
    *[ Supported-Features ]
    [ WLAN-Identifier ]
    [ DER-Flags ]
    ...
    *[ AVP ]

```

### 5.2.2.1.2 Diameter-EAP-Answer (DEA) Command

The Diameter-EAP-Answer (DEA) command, indicated by the Command-Code field set to 268 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA Server to a non-3GPP access network NAS. The ABNF is reused from the IETF RFC 5779 [2]. The ABNF also contains AVPs that are reused from IETF RFC 4072 [5].

```

< Diameter-EAP-Answer > ::= < Diameter Header: 268, PXY, 16777250 >
    < Session-Id >
    { Auth-Application-Id }
    { Result-Code }
    [ Experimental-Result ]
    { Origin-Host }
    { Origin-Realm }
    { Auth-Request-Type }
    [ EAP-Payload ]
    [ User-Name ]
    [ Session-Timeout ]
    [ Accounting-Interim-Interval ]
    [ EAP-Master-Session-Key ]
    [ Context-Identifier ]
    [ APN-OI-Replacement ]
    *[ APN-Configuration ]
    [MIP6-Agent-Info ]
    [ MIP6-Feature-Vector ]
    [ Mobile-Node-Identifier ]
    [ 3GPP-Charging-Characteristics ]
    [ AMBR ]
    *[ Redirect-Host ]
    [ AN-Trusted ]
    [ Trace-Info ]
    [ Subscription-ID ]
    *[ Supported-Features ]
    [ MIP-FA-RK ]
    [ MIP-FA-RK-SPI ]
    [ NSWO-Authorization ]
    [ DEA-Flags ]
    ...
    *[ AVP ]

```

### 5.2.2.2 Commands for STa HSS/AAA Initiated Detach for Trusted non-3GPP Access

#### 5.2.2.2.1 Abort-Session-Request (ASR) Command

The Abort-Session-Request (ASR) command, indicated by the Command-Code field set to 274 and the "R" bit set in the Command Flags field, is sent from a 3GPP AAA Server/Proxy to a non-3GPP access network NAS. ABNF for the ASR commands is as follows:

```

< Abort-Session-Request > ::= < Diameter Header: 274, REQ, PXY, 16777250 >
    < Session-Id >
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    { Destination-Host }
    { Auth-Application-Id }
    [ User-Name ]
    [ Auth-Session-State ]
    ...
    *[ AVP ]

```

### 5.2.2.2.2 Abort-Session-Answer (ASA) Command

The Abort-Session-Answer (ASA) command, indicated by the Command-Code field set to 274 and the "R" bit cleared in the Command Flags field, is sent from a non-3GPP access network NAS to a 3GPP AAA Server/Proxy. ABNF for the ASA commands is as follows:

```
< Abort-Session-Answer > ::= < Diameter Header: 274, PXY, 16777250 >
                               < Session-Id >
                               { Result-Code }
                               { Origin-Host }
                               { Origin-Realm }
                               ...
                               *[ AVP ]
```

### 5.2.2.2.3 Session-Termination-Request (STR) Command

The Session-Termination-Request (STR) command, indicated by the Command-Code field set to 275 and the "R" bit set in the Command Flags field, is sent from a trusted non-3GPP access network to a 3GPP AAA Server/Proxy. The Command Code value and ABNF are re-used from the IETF RFC 3588 [7] Session-Termination-Request command.

```
<Session-Termination-Request> ::= < Diameter Header: 275, REQ, PXY, 16777250 >
                                   < Session-Id >
                                   { Origin-Host }
                                   { Origin-Realm }
                                   { Destination-Realm }
                                   { Auth-Application-Id }
                                   { Termination-Cause }
                                   [ User-Name ]
                                   ...
                                   *[ AVP ]
```

### 5.2.2.2.4 Session-Termination-Answer (STA) Command

The Session-Termination-Answer (STA) command, indicated by the Command-Code field set to 275 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA Server/Proxy to a trusted non-3GPP access network. The Command Code value and ABNF are re-used from the IETF RFC 3588 [7] Session-Termination-Answer command.

```
<Session-Termination-Answer> ::= < Diameter Header: 275, PXY, 16777250 >
                                   < Session-Id >
                                   { Result-Code }
                                   { Origin-Host }
                                   { Origin-Realm }
                                   *[ AVP ]
```

## 5.2.2.3 Commands for Re-Authentication and Re-Authorization Procedure

### 5.2.2.3.1 Re-Auth-Request (RAR) Command

The Diameter Re-Auth-Request (RAR) command, indicated by the Command-Code field set to 258 and the "R" bit set in the Command Flags field, is sent from a 3GPP AAA Server to a Trusted Non-3GPP access network. ABNF for the RAR command is as follows:

```
< Re-Auth-Request > ::= < Diameter Header: 258, REQ, PXY, 16777250 >
                          < Session-Id >
                          { Origin-Host }
                          { Origin-Realm }
                          { Destination-Realm }
                          { Destination-Host }
                          { Auth-Application-Id }
                          { Re-Auth-Request-Type }
                          [ User-Name ]
                          ...
                          *[ AVP ]
```

### 5.2.2.3.2 Re-Auth-Answer (RAA) Command

The Diameter Re-Auth-Answer (ASA) command, indicated by the Command-Code field set to 258 and the "R" bit cleared in the Command Flags field, is sent from a Trusted Non-3GPP access network to a 3GPP AAA Server/Proxy. ABNF for the RAA commands is as follows:

```
< Re-Auth-Answer > ::=
    < Diameter Header: 258, PXY, 16777250 >
    < Session-Id >
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    ...
    *[ AVP ]
```

### 5.2.2.3.3 AA-Request (AAR) Command

The AA-Request (AAR) command, indicated by the Command-Code field set to 265 and the "R" bit set in the Command Flags field, is sent from a Trusted Non-3GPP access network to a 3GPP AAA Server/Proxy. The ABNF is re-used from IETF RFC 4005 [4], adding AVPs from IETF RFC 5779 [2].

```
< AA-Request > ::=
    < Diameter Header: 265, REQ, PXY, 16777250 >
    < Session-Id >
    { Auth-Application-Id }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    { Auth-Request-Type }
    [ Destination-Host ]
    [ User-Name ]

    [ MIP6-Feature-Vector ]
    ...
    *[ AVP ]
```

### 5.2.2.3.4 AA-Answer (AAA) Command

The AA-Answer (AAA) command, indicated by the Command-Code field set to 265 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA Server/Proxy to a Trusted Non-3GPP access network. The ABNF is re-used from IETF RFC 4005 [4], adding AVPs from IETF RFC 5779 [2].

```
< AA-Answer > ::=
    < Diameter Header: 265, PXY, 16777250 >
    < Session-Id >
    { Auth-Application-Id }
    { Auth-Request-Type }
    { Result-Code }
    [ Experimental-Result ]
    { Origin-Host }
    { Origin-Realm }
    [ Session-Timeout ]
    [ Accounting-Interim-Interval ]
    [ Context-Identifier ]
    [ APN-OI-Replacement ]
    *[ APN-Configuration ]
    [ 3GPP-Charging-Characteristics ]
    [ Trace-Info ]
    [ Subscription-ID ]
    ...
    *[ AVP ]
```

### 5.2.2.3.5 Diameter-EAP-Request (DER) Command

Refer to clause 5.2.2.1.1

### 5.2.2.3.6 Diameter-EAP-Answer (DEA) Command

Refer to clause 5.2.2.1.2

## 5.2.2.4 Commands for Trusted non-3GPP Access network Initiated Session Termination

### 5.2.2.4.1 Session-Termination-Request (STR) Command

The Session-Termination-Request (STR) command, indicated by the Command-Code field set to 275 and the "R" bit set in the Command Flags field, is sent from a non-3GPP access network to a 3GPP AAA server. The Command Code value and ABNF are re-used from the IETF RFC 3588 [7] Session-Termination-Request command.

```
<Session-Termination-Request> ::= < Diameter Header: 275, REQ, PXY, 16777250 >
                                < Session-Id >
                                { Origin-Host }
                                { Origin-Realm }
                                { Destination-Realm }
                                { Auth-Application-Id }
                                { Termination-Cause }
                                [ User-Name ]
                                ...
                                *[ AVP ]
```

### 5.2.2.4.2 Session-Termination-Answer (STA) Command

The Session-Termination-Answer (STA) command, indicated by the Command-Code field set to 275 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA server to a non-3GPP access network. The Command Code value and ABNF are re-used from the IETF RFC 3588 [7] Session-Termination-Answer command.

```
<Session-Termination-Answer> ::= < Diameter Header: 275, PXY, 16777250 >
                                < Session-Id >
                                { Result-Code }
                                { Origin-Host }
                                { Origin-Realm }
                                *[ AVP ]
```

## 5.2.3 Information Elements

### 5.2.3.1 General

The following table describes the Diameter AVPs defined for the STa interface protocol in NBM mode, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted.

**Table 5.2.3.1/1: Diameter STa AVPs**

	AVP Flag rules
--	----------------

Attribute Name	AVP Code	Section defined	Value Type	Must	May	Should not	Must not
MIP6-Feature-Vector	124	5.2.3.3	Unsigned64	M			V,P
QoS-Capability	578	5.2.3.4	Grouped	M			V,P
Service-Selection	493	5.2.3.5	UTF8String	M			V,P
RAT-Type	1032	5.2.3.6	Enumerated	M,V			P
ANID	1504	5.2.3.7	UTF8String	M,V			P
AN-Trusted	1503	5.2.3.9	Enumerated	M,V			P
MIP-FA-RK	1506	5.2.3.12	OctetString	M,V			P
MIP-FA-RK-SPI	1507	5.2.3.13	Unsigned32	M,V			P
Full-Network-Name	1516	5.2.3.14	OctetString	V			M,P
Short-Network-Name	1517	5.2.3.15	OctetString	V			M,P
WLAN-Identifier	1509	5.2.3.18	Grouped	V			M,P
Mobile-Node-Identifier	506	5.2.3.2	UTF8String	M			V,P
Transport-Access-Type	1519	5.2.3.19	Enumerated	V			M,P
APN-Configuration	1430	8.2.3.7	Grouped	M,V			P
Visited-Network-Identifier	600	9.2.3.1.2	OctetString	M,V			P
DER-Flags	1520	5.2.3.20	Unsigned32	V			M,P
DEA-Flags	1521	5.2.3.21	Unsigned32	V			M,P
SSID	1524	5.2.3.22	UTF8String	V			M,P
HESSID	1525	5.2.3.23	UTF8String	V			M,P

The following table describes the Diameter AVPs re-used by the STa interface protocol from existing Diameter Applications, including a reference to their respective specifications and when needed, a short description of their use within STa. Other AVPs from existing Diameter Applications, except for the AVPs from Diameter Base Protocol, do not need to be supported.

**Table 5.2.3.1/2: STa re-used Diameter AVPs**

Attribute Name	Reference	Comments	M-bit
Accounting-Interim-Interval	IETF RFC 3588 [7]		
Auth-Request-Type	IETF RFC 3588 [7]		
Calling-Station-Id	IETF RFC 4005 [4]		
Subscription-ID	IETF RFC 4006 [20]		Must not set
EAP-Master-Session-Key	IETF RFC 4072 [5]		
EAP-Payload	IETF RFC 4072 [5]		
RAT-Type	3GPP TS 29.212 [23]		
Re-Auth-Request-Type	IETF RFC 3588 [7]		
Session-Timeout	IETF RFC 3588 [7]		
User-Name	IETF RFC 3588 [7]		
Terminal-Information	3GPP TS 29.272 [29]		
MIP6-Agent-Info	IETF RFC 5447 [6]		
APN-OI-Replacement	3GPP TS 29.272 [29]		
Supported-Features	3GPP TS 29.229 [24]		
Feature-List-ID	3GPP TS 29.229 [24]	See section 5.2.3.10	
Feature-List	3GPP TS 29.229 [24]	See section 5.2.3.11	
NOTE: The M-bit settings for re-used AVPs override those of the defining specifications that are referenced. Values include: "Must set", "Must not set". If the M-bit setting is blank, then the defining specification applies.			

Only those AVP initially defined in this reference point or AVP with values initially defined in this reference point and for this procedure are described in the following subchapters.

### 5.2.3.2 Mobile-Node-Identifier

The Mobile-Node-Identifier AVP (AVP Code 506) is of type UTF8String.

The Mobile-Node-Identifier AVP is returned in an answer message that ends a successful authentication (and possibly an authorization) exchange between the AAA client and the AAA server. The returned Mobile Node Identifier may be used as the PMIPv6 MN-ID or as the MIPv4 MN-NAI or to derive the IMSI to be sent in GTPv2 signalling.

The Mobile-Node-Identifier is defined on IETF RFC 5779 [2].

### 5.2.3.3 MIP6-Feature-Vector

The MIP6-Feature-Vector AVP (AVP Code 124) is of type Unsigned64 and contains a 64 bit flags field of supported mobile IP capabilities of the non-3GPP access network (when this AVP is used in the request commands) and the mobile IP capabilities the 3GPP AAA Server has authorized (when this AVP is used in the response commands).

The following capabilities are defined for STa interface:

- MIP6\_INTEGRATED (0x0000000000000001)  
This flag is set by the non-3GPP access network and the 3GPP AAA Server. It means that the Mobile IPv6 integrated scenario bootstrapping functionality is supported.
- PMIP6\_SUPPORTED (0x0000010000000000)  
When this flag is set by the non-3GPP access network it indicates to the 3GPP AAA Server that it supports PMIPv6.  
When this flag is set by the 3GPP AAA Server it indicates to the non-3GPP access network that NBM shall be used.
- ASSIGN\_LOCAL\_IP (0x0000080000000000)  
This flag is set by the 3GPP AAA Server.  
When this flag is set by the 3GPP AAA Server it indicates to the non-3GPP access network that the non-3GPP access network shall assign to the user a local IP address (for HBM).
- MIP4\_SUPPORTED (0x0000100000000000)  
This flag is set by the non-3GPP access network, the PDN GW and the 3GPP AAA Server. When this flag is set by the non-3GPP access network it indicates to the 3GPP AAA Server that it supports MIPv4 FA-CoA mode.  
When this flag is set by the 3GPP AAA Server it indicates to the non-3GPP access network that MIPv4 FA-CoA mode shall be used. When this flag is set by the PDN GW and 3GPP AAA Server over the S6b interface, it shows that MIPv4 mobility protocol is used on the S2a interface.
- OPTIMIZED\_IDLE\_MODE\_MOBILITY (0x0000200000000000)  
This flag is set by the Trusted Non-3GPP access network if the PDN GW information needs to be updated for the case of idle mode mobility from E-UTRAN to HRPD access.
- GTPv2\_SUPPORTED (0x0000400000000000)  
When this flag is set by the non-3GPP access network it indicates to the 3GPP AAA Server that it supports GTPv2.  
When this flag is set by the 3GPP AAA Server it indicates to the non-3GPP access network that NBM shall be used.

### 5.2.3.4 QoS Capability

This AVP is FFS

### 5.2.3.5 Service-Selection

The Service-Selection AVP is of type of UTF8String. This AVP contains an APN Network Identifier (i.e., an APN without the Operator Identifier), and it shall consist of one or more labels according to DNS naming conventions (IETF RFC 1035 [35]) describing the access point to the packet data network.

The contents of the Service-Selection AVP shall be formatted as a character string composed of one or more labels separated by dots (".").

The Service-Selection AVP is defined in IETF RFC 5778 [11].

### 5.2.3.6 RAT-Type

The RAT-Type AVP (AVP code 1032) is of type Enumerated and is used to identify the radio access technology that is serving the UE. It follows the specification described in TS 29.212 [23].

### 5.2.3.7 ANID

The ANID AVP is of type UTF8String; this AVP contains the Access Network Identity; see 3GPP TS 24.302 [26] for defined values.

### 5.2.3.8 AMBR

Please refer to 3GPP TS 29.272 [29] for the encoding of this AVP.

### 5.2.3.9 AN-Trusted

The AN-Trusted AVP (AVP Code 1503) is of type Enumerated.

The AN-Trusted AVP sent from the 3GPP AAA Server to the Non-3GPP access network conveys the decision about the access network being trusted or untrusted by the HPLMN.

The following values are defined:

TRUSTED (0)

This value is used when the non-3GPP access network is to be handled as trusted.

UNTRUSTED (1)

This value is used when the non-3GPP access network is to be handled as untrusted.

### 5.2.3.10 Feature-List-ID AVP

The syntax of this AVP is defined in 3GPP TS 29.229 [24]. For this release, the Feature-List-ID AVP value shall be set to 1 for the STa/SWa application.

### 5.2.3.11 Feature-List AVP

The syntax of this AVP is defined in 3GPP TS 29.229 [24]. A null value indicates that there is no feature used by the STa/SWa application.

NOTE: There are no STa/SWa features defined for this release.

### 5.2.3.12 MIP-FA-RK

The MIP-FA-RK AVP is of type OctetString; this AVP contains the FA-RK used to calculate the security parameters needed for the MN-FA authentication extension as defined by 3GPP TS 33.402 [19].

### 5.2.3.13 MIP-FA-RK-SPI

The MIP-FA-RK-SPI AVP is of type Unsigned32; this AVP contains the security index used in identifying the security context for the FA-RK as defined by 3GPP TS 33.402 [19].

### 5.2.3.14 Full-Network-Name

The Full-Network-Name AVP is of type OctetString; this AVP contains the Full Network Name; see 3GPP TS 24.302 [26] for defined values.

### 5.2.3.15 Short-Network-Name

The Short-Network-Name AVP is of type OctetString; this AVP contains the Short Network Name; see 3GPP TS 24.302 [26] for defined values.

5.2.3.16 Void

5.2.3.17 Void

5.2.3.18 WLAN-Identifier

The WLAN-Identifier AVP is of type Grouped. It contains the type and value of an IEEE 802.11 identifier of a Trusted WLAN.

AVP Format:

```
WLAN-Identifier ::= < AVP Header: 1509 10415 >
                    [SSID ]
                    [HESSID ]
                    *[ AVP ]
```

5.2.3.19 Transport-Access-Type

The Transport-Access-Type AVP (AVP code 1519) is of type Enumerated and is used to identify the transport access technology that is serving the UE.

The following values are defined:

BBF (0)

This value shall be used to indicate a BBF transport access network.

5.2.3.20 DER-Flags

The DER-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 5.2.3.20/1:

**Table 5.2.3.20/1: DER-Flags**

Bit	Name	Description
0	NSWO-Capability-Indication	This bit, when set, indicates to the 3GPP AAA proxy/server that the TWAN supports non-seamless WLAN offload service (see clause 16 of 3GPP TS 23.402 [3]).
NOTE: Bits not defined in this table shall be cleared by the sender and discarded by the receiver of the command.		

5.2.3.21 DEA-Flags

The DEA-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 5.2.3.21/1:

**Table 5.2.3.21/1: DEA-Flags**

Bit	Name	Description
0	NSWO-Authorization	This bit, when set, indicates to the TWAN that the non-seamless WLAN offload service is authorized (see clause 16 of 3GPP TS 23.402 [3]).
NOTE: Bits not defined in this table shall be cleared by the sender and discarded by the receiver of the command.		

5.2.3.22 SSID

The SSID AVP is of type UTF8String and it shall contain the Service Set Identifier which identifies a specific 802.11 extended service set (see IEEE Std 802.11-2012 [40]). It shall contain a string of 1 to 32 octets.

### 5.2.3.23 HESSID

The HESSID AVP is of type UTF8String and it shall contain a 6-octet MAC address that identifies the Homogenous Extended Service Set (see IEEE Std 802.11-2012 [40]). It shall be encoded in upper-case ASCII characters with the octet values separated by dash characters. It shall contain a string of 17 octets. Example: "00-10-A4-23-19-C0".

## 5.2.4 Session Handling

The Diameter protocol between the non-3GPP access network and the 3GPP AAA Server or 3GPP AAA Proxy, shall always keep the session state, and use the same Session-Id parameter for the lifetime of each Diameter session.

A Diameter session shall identify a given user. In order to indicate that the session state is to be maintained, the Diameter client and server shall not include the Auth-Session-State AVP, either in the request or in the response messages (see IETF RFC 3588 [7]).

---

# 6 SWd Description

## 6.1 Functionality

### 6.1.1 General

For a general description of the SWd reference point refer to 3GPP TS 23.234 [21], Section 6.3.11.1 "General Description of the Wd Reference Point".

The functionality of the SWd reference point is to transport AAA messages similar to those provided in 3GPP TS 23.234 [21], Section 6.3.11.2 including:

- Carrying data for authentication signalling between 3GPP AAA Proxy and 3GPP AAA Server;
- Carrying data for authorization signalling between 3GPP AAA Proxy and 3GPP AAA Server;
- Carrying charging signalling per user;
- Carrying keying data for the purpose of radio interface integrity protection and encryption;
- Carrying authentication data for the purpose of tunnel establishment, tunnel data authentication and encryption, for the case in which the ePDG is in the VPLMN;
- Carrying mapping of a user identifier and a tunnel identifier sent from the ePDG to the 3GPP AAA Proxy through the 3GPP AAA Server;
- Used for purging a user from the access network for immediate service termination;
- Enabling the identification of the operator networks amongst which the roaming occurs;
- If QoS mechanisms are applied: carrying data for AN QoS capabilities/policies (e.g. the supported 3GPP QoS profiles) within authentication request from 3GPP AAA Proxy to 3GPP AAA Server.
- Carrying the IP Mobility Capabilities between 3GPP AAA Proxy and 3GPP AAA Server.

### 6.1.2 Procedures Description

#### 6.1.2.1 Trusted non-3GPP Access / Access Gateway related procedures

##### 6.1.2.1.1 Trusted Non-3GPP Access Authentication and Authorization

When used in connection with the STa interface, the SWd interface shall support the trusted non-3GPP access authentication and authorization procedure defined in clause 5.1.2.1. For this procedure, the 3GPP AAA Proxy shall

forward the Diameter commands received from the 3GPP AAA Server and the trusted non-3GPP access network as a stateful Diameter proxy, with the following exceptions:

- The 3GPP AAA Proxy may reject an authentication and authorization request, if roaming is not allowed for the users of the given HPLMN.
- When forwarding an authentication and authorization request, the 3GPP AAA Proxy shall check the presence and value of the visited network identifier. If the AVP was missing, it shall insert it, if the AVP was present, it may overwrite the AVP value before forwarding the request.
- The 3GPP AAA Proxy may modify the service authorization information in the authentication and authorization answer that it forwards to the trusted non-3GPP access network, in order to enforce the QoS limitations according to the local policies and the roaming agreement with the home operator.
- The 3GPP AAA Proxy may decide about the trustworthiness of the non-3GPP access from the VPLMN point of view and insert a trust relationship indicator to the authentication and authorization request.

The 3GPP AAA Proxy shall decide about using the S2a-PMIP based S8 chaining and in case it has selected that option, it shall select the Serving GW to be invoked and it shall add the Serving GW address to the authentication and authorization answer that is sent upon successful completion of the authentication.

Table 6.1.2.1.1/1 describes the trusted non-3GPP access authentication and authorization request forwarded on the SWd interface.

Table 6.1.2.1.1-1: Trusted non-3GPP Access Authentication and Authorization Request on SWd

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
EAP payload	EAP-payload	M	This IE shall contain the Encapsulated EAP payload used for the UE – 3GPP AAA Server mutual authentication
Authentication Request Type	Auth-Request-Type	M	This IE shall define whether the user is to be authenticated only, authorized only or both. AUTHORIZE_AUTHENTICATE shall be used in this case.
UE Layer-2 address	Calling-Station-ID	M	This IE shall contain the Layer-2 address of the UE.
Supported 3GPP QoS profile	QoS-Capability	O	If the trusted non-3GPP Access supports QoS mechanisms, this information element may be included to contain the access network's QoS capabilities as defined in IETF RFC 5777 [9].
Mobility Capabilities	MIP6-Feature-Vector	C	This information element shall contain the mobility capabilities of the trusted non-3GPP access network, if dynamic mobility mode selection is done. This information may also be used to decide whether to authorize access to EPC to a user accessing a TWAN.  The PMIP6_SUPPORTED flag and/or the GTPv2_SUPPORTED flag shall be set if the trusted non-3GPP access network supports PMIPv6 and/or GTPv2. PMIP6_SUPPORTED flag is defined in IETF RFC 5779 [2].  The flag MIP6_INTEGRATED shall be set if DHCPv6 based Home Agent address discovery is supported as defined in IETF RFC 5447 [6].  The MIP4_SUPPORTED flag shall be set if the trusted non-3GPP access supports MIPv4 FA-CoA mode.
Access Type	RAT-Type	M	This IE shall contain the trusted non-3GPP access network technology type that is serving the UE.
Access Network Identity	ANID	M	This IE shall contain the access network identifier used for key derivation at the HSS. (See 3GPP TS 24.302 [26] for all possible values)
Visited Network Identifier	Visited-Network-Identifier	M	This IE shall contain the Identifier that allows the home network to identify the Visited Network.
Full Name for Network	Full-Network-Name	O	This IE shall contain the full name for network as specified in 3GPP TS 24.302 [26]. This AVP may be inserted by the non-3GPP access network depending on its local policy and only when it is not connected to the UE's Home Network. If the Visited Network Identifier is present, this AVP shall be set.
Short Name for Network	Short-Network-Name	O	This IE shall contain the short name for network as specified in 3GPP TS 24.302 [26]. This AVP may be inserted by the non-3GPP access network depending on its local policy and only when it is not connected to the UE's Home Network. If the Visited Network Identifier is present, this AVP shall be set.
APN Id	Service-Selection	O	If present, this information element shall contain the Network Identifier part of the APN the user wants to connect to (if available).
Terminal Information	Terminal-Information	O	If present, this information element shall contain information about the user's mobile equipment. The type of identity carried depends on the access technology type. For HRPD access network, the 3GPP2-MEID AVP shall be included in this grouped AVP.
Trust Relationship Indicator	AN-Trusted	O	If present, This AVP shall express the trusted/untrusted decision about the non-3GPP IP access, from the VPLMN's point of view.
Selected Trusted WLAN Identifier	WLAN-Identifier	O	If present, this IE shall contain the Trusted WLAN Identifier selected by the UE to access the Trusted WLAN Access Network (see clause 16 of 3GPP TS 23.402 [3]).
DER Flags	DER-Flags	O	This Information Element contains a bit mask. See 5.2.3.20 for the meaning of the bits.

Transport Access Type	Transport-Access-Type	C	For interworking with Fixed Broadband access networks (see 3GPP TS 23.139 [39]), if the access network needs to receive the IMSI of the UE in the authentication response, then this information element shall be present, and it shall contain the value "BBF" (see subclause 5.2.3.19).
-----------------------	-----------------------	---	---

NOTE: For more details on the 3GPP AAA Proxy behaviour, refer to clause 5.1.2.1.3.

#### 6.1.2.1.2 HSS/AAA Initiated Detach for Trusted non-3GPP Access

When used in connection with the STa interface, the SWd interface shall support the HSS initiated detach procedure defined in clause 5.1.2.2.

For this procedure, the 3GPP AAA Proxy shall forward the Diameter commands received from the 3GPP AAA Server and the access network GW as a stateful Diameter proxy.

#### 6.1.2.1.3 Access and Service Authorization information update

When used in connection with the STa interface, the SWd interface shall support the trusted non-3GPP access and service authorization information update procedure defined in clause 5.1.2.3. For this procedure, the 3GPP AAA Proxy shall forward the Diameter commands received from the 3GPP AAA Server and the trusted non-3GPP access network as a stateful Diameter proxy, with the following exceptions:

- When forwarding an authentication and authorization request, the 3GPP AAA Proxy shall check the presence and value of the visited network identifier. If the AVP was missing, it shall insert it, if the AVP was present, it may overwrite the AVP value before forwarding the request.
- The 3GPP AAA Proxy may modify the service authorization information in the authentication and authorization answer that it forwards to the trusted non-3GPP access GW, in order to enforce the QoS limitations according to the local policies and the roaming agreement with the home operator.

Table 6.1.2.1.3/1 describes the trusted non-3GPP access authorization request forwarded on the SWd interface. As the content is very similar to that of the request received on the STa interface, only those AVPs are listed that are handled differently on the two interfaces.

**Table 6.1.2.1.3/1: Trusted Non-3GPP Access Authorization Request on SWd interface**

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Request-Type	Auth-Req-Type	M	This IE shall contain the Authorization Request Type. The following values only shall be used: AUTHORIZE_ONLY This value shall indicate the initial request for authorization of the user to the APN.
Visited Network Identifier	Visited-Network-Identifier	M	This IE shall contain an identifier that allows the home network to identify the Visited Network.
Routing Information	Destination-Host	M	This IE shall contain the 3GPP AAA Server name that is obtained from the Origin-Host AVP of a previously received message.
Supported 3GPP QoS profile	QoS-Capability	O	If the trusted non-3GPP Access supports QoS mechanisms, this information element may be included to contain the access network's QoS capabilities as defined in IETF RFC 5777 [9].
Access Type	RAT-Type	O	If present, this IE contain the trusted non-3GPP access network access technology type that is serving the UE.

NOTE: For more details on the 3GPP AAA Proxy behaviour, refer to clause 5.1.2.3.3.

#### 6.1.2.1.4 Trusted non-3GPP Access Network Initiated Session Termination

When used in connection with the STa reference point, the SWd reference point shall support the access network initiated session termination procedures as defined in clause 5.1.2.4

For this procedure, the 3GPP AAA Proxy shall forward the Diameter commands received from the 3GPP AAA Server and the access network gateway as a stateful Diameter proxy.

#### 6.1.2.2 Untrusted non-3GPP Access / ePDG related procedures

When used in connection with the SWm reference point, the SWd reference point shall support the following procedures:

- Authentication procedures as defined in clause 7.1.2.1
- Authorization procedures as defined in clause 7.1.2.2
- Access network/ePDG initiated session termination procedures as defined in clause 7.1.2.3
- HSS/AAA initiated detach procedures as defined in clause 7.1.2.4
- Service authorization information update procedures as defined in clause 7.1.2.5

For all these procedures, the 3GPP AAA Proxy shall forward the Diameter commands received from the 3GPP AAA Server and the ePDG as a stateful Diameter proxy, with the following exceptions:

- The 3GPP AAA Proxy may reject an authentication or an authorization request, if roaming is not allowed for the users of the given HPLMN.
- The 3GPP AAA Proxy may modify the service authorization information in the authorization answer that it forwards to the ePDG, in order to enforce the QoS limitations according to the local policies and the roaming agreement with the home operator.
- The 3GPP AAA Proxy shall decide about using the S8-S2b chaining and in case it has selected that option, it shall select the Serving GW to be invoked and it shall add the Serving GW address to the authentication answer that is sent upon successful completion of the authentication.

NOTE: For more detailed behavior of the 3GPP AAA Proxy, refer to subclauses 7.1.2.1.3 and 7.1.2.2.3 respectively.

When used in connection with the SWa interface point, the SWd reference point shall support the following procedures:

- Authentication and authorization procedure as defined in clause 4.1.2.1
- HSS/AAA initiated detach procedures as defined in clause 4.1.2.2
- Untrusted non-3GPP access network initiated detach procedures as defined in clause 4.1.2.3
- Re-Authentication and Re-Authorization Procedure as defined in clause 4.1.2.4

For all these procedures, the 3GPP AAA Proxy shall forward the Diameter commands received from the 3GPP AAA Server and the untrusted non-3GPP access network as a stateful Diameter proxy, with the following exceptions:

- The 3GPP AAA Proxy may reject an authentication and authorization request, if roaming is not allowed for the users of the given HPLMN.
- When forwarding an authentication and authorization request, the 3GPP AAA Proxy shall insert the visited network identifier.

#### 6.1.2.3 PDN GW related procedures

When used in connection with the S6b reference point, the SWd reference point shall support the following procedures:

- Authentication and authorization procedures when using DSMIP as defined in clause 9.1.2.1
- Authorization procedures when using NBM as defined in clause 9.1.2.2

- PDN GW initiated session termination procedures as defined in clause 9.1.2.3
- HSS/AAA initiated detach procedures as defined in clause 9.1.2.4
- Service authorization information update procedures as defined in clause 9.1.2.5

For all these procedures, the 3GPP AAA Proxy shall forward the Diameter commands received from the 3GPP AAA Server and the PDN GW as a stateful Diameter proxy, with the following exceptions:

- The 3GPP AAA Proxy may reject an authentication or authorization request, if roaming is not allowed for the users of the given HPLMN
- The 3GPP AAA Proxy may modify the service authorization information in the authorization answers that it forwards to the PDN GW, in order to enforce the QoS limitations according to the local policies and the roaming agreement with the home operator.

NOTE: For more detailed behavior of the 3GPP AAA Proxy, refer to subclauses 9.1.2.1.4, 9.1.2.2.4, 9.1.2.3.4, and 9.1.2.4.4, respectively.

## 6.2 Protocol Specification

### 6.2.1 General

The SWd reference point shall be based on Diameter, as defined in IETF RFC 3588 [7] and contain the following additions and extensions:

- IETF RFC 4005 [4], which defines a Diameter protocol application used for Authentication, Authorization and Accounting (AAA) services in the Network Access Server (NAS) environment.
- IETF RFC 4072 [5], which provides a Diameter application to support the transport of EAP (IETF RFC 3748 [8]) frames over Diameter.
- IETF RFC 5779 [2], which defines Diameter extensions and application for PMIPv6 MAG to AAA and LMA to AAA interfaces.
- IETF RFC 5447 [6], which defines Diameter extensions for Mobile IPv6 NAS to AAA interface.

There is no separate application ID defined for the SWd interface. The application ID used by the 3GPP AAA Proxy depends on the command sent over SWd.

NOTE: Even though the 3GPP AAA Proxy may add new AVPs to the Diameter commands forwarded to/from the 3GPP AAA Server, there is no AVP present in the SWd reference point that would not be present in the interface that is used in connection with it. Therefore, the same Application ID can be used.

### 6.2.2 Commands

#### 6.2.2.1 Commands used in connection with the STa interface

##### 6.2.2.1.1 Commands for STa PMIPv6 or GTPv2 authentication and authorization procedures

###### 6.2.2.1.1.1 Diameter-EAP-Request (DER) Command

The Diameter-EAP-Request (DER) command, indicated by the Command-Code field set to 268 and the "R" bit set in the Command Flags field, is sent from a trusted non-3GPP access network NAS to a 3GPP AAA server. The ABNF is re-used from the IETF RFC 5779 [2].

```
< Diameter-EAP-Request > ::= < Diameter Header: 268, REQ, PXY, 16777250 >
< Session-Id >
```

```

{ Auth-Application-Id }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Auth-Request-Type }
{ EAP-Payload }
[ User-Name ]
[ Calling-Station-Id ]
...
[ RAT-Type ]
[ ANID ]
[ QoS-Capability ]
[ MIP6-Feature-Vector ]
[ Visited-Network-Identifier ]
[ Service-Selection ]
[ Terminal-Information ]
[ AN-Trusted ]
[ Full-Network-Name ]
[ Short-Network-Name ]
*[ Supported-Features ]
[ WLAN-Identifier ]
[ DER-Flags ]
...
*[ AVP ]

```

#### 6.2.2.1.1.2 Diameter-EAP-Answer (DEA) Command

The Diameter-EAP-Answer (DEA) command, indicated by the Command-Code field set to 268 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA server to a 3GPP AAA Proxy. The ABNF is re-used from the IETF RFC 5779 [2]. The ABNF also contains AVPs that are reused from IETF RFC 4072 [5].

```

< Diameter-EAP-Answer > ::= < Diameter Header: 268, PXY, 16777250 >
< Session-Id >
{ Auth-Application-Id }
{ Result-Code }
[ Experimental-Result ]
{ Origin-Host }
{ Origin-Realm }
{ Auth-Request-Type }
[ EAP-Payload ]
[ User-Name ]
[ Session-Timeout ]
[ Accounting-Interim-Interval ]
[ EAP-Master-Session-Key ]
[ Context-Identifier ]
[ APN-OI-Replacement ]
*[ APN-Configuration ]
[ MIP6-Feature-Vector ]
[ Mobile-Node-Identifier ]
*[ Redirect-Host ] ]
[ Trace-Info ]
[ Subscription-ID ]
*[ Supported-Features ]
[ DEA-Flags ]
...
*[ AVP ]

```

#### 6.2.2.1.2 Commands for STa HSS/AAA Initiated Detach for Trusted non-3GPP Access

The ABNFs defined for the STa interface in clause 5.2.2.2 and in its subclauses apply.

### 6.2.2.1.3 Commands for STa Access and Service Authorization Update Procedure

The ABNFs defined for the STa interface in clause 5.2.2.3 and in its subclauses apply.

### 6.2.2.1.4 Commands for Trusted non-3GPP Access network Initiated Session Termination

The ABNFs defined for the STa interface in clause 5.2.2.4 and in its subclauses apply.

### 6.2.2.2 Commands used in connection with the SWm interface

The ABNFs defined for the SWm interface in clause 7.2.2 and in its subclauses apply.

### 6.2.2.3 Commands used in connection with the S6b interface

The ABNFs defined for the S6b interface in clause 9.2.2 and in its subclauses apply.

## 6.2.3 Information Elements

### 6.2.3.1 General

The following table describes the Diameter AVPs defined for the SWd interface protocol in NBM mode, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted.

**Table 6.2.3.1/1: Diameter SWd AVPs**

Attribute Name	AVP Code	Section defined	Value Type	AVP Flag rules			
				Must	May	Should not	Must not
MIP6-Feature-Vector	124	5.2.3.3	Unsigned64	M			V,P
QoS-Capability	578	5.2.3.4	Grouped	M			V,P
RAT-Type	1032	5.2.3.6	Enumerated	M,V			P
ANID	1504	5.2.3.7	UTF8String	M,V			P
Service-Selection	493	5.2.3.5	UTF8String	M			V,P
Mobile-Node-Identifier	506	5.2.3.2	UTF8String	M			V,P
AN-Trusted	1503	5.2.3.9	Enumerated	M,V			P
Full-Network-Name	1516	5.2.3.14	OctetString	V			M,P
Short-Network-Name	1517	5.2.3.15	OctetString	V			M,P
WLAN-Identifier	1509	5.2.3.18	Grouped	V			M,P
APN-Configuration	1430	8.2.3.7	Grouped	M,V			P
Visited-Network-Identifier	600	9.2.3.1.2	OctetString	M,V			P
DER-Flags	1520	5.2.3.20	Unsigned32	V			M,P
DEA-Flags	1521	5.2.3.21	Unsigned32	V			M,P
SSID	1524	5.2.3.22	UTF8String	V			M,P
HESSID	1525	5.2.3.23	UTF8String	V			M,P

The following table describes the Diameter AVPs re-used by the SWd interface protocol from existing Diameter Applications, including a reference to their respective specifications and when needed, a short description of their use within SWd. Other AVPs from existing Diameter Applications, except for the AVPs from Diameter Base Protocol, do not need to be supported.

Table 6.2.3.1/2: SWd re-used Diameter AVPs

Attribute Name	Reference	Comments	M-bit
Accounting-Interim-Interval	IETF RFC 3588 [7]		
Auth-Request-Type	IETF RFC 3588 [7]		
Calling-Station-Id	IETF RFC 4005 [6]		
Subscription-ID	IETF RFC 4006 [20]		Must not set
EAP-Master-Session-Key	IETF RFC 4072 [5]		
EAP-Payload	IETF RFC 4072 [5]		
RAT-Type	3GPP TS 29.212 [23]		
Re-Auth-Request-Type	IETF RFC 3588 [7]		
Session-Timeout	IETF RFC 3588 [7]		
User-Name	IETF RFC 3588 [7]		
Terminal-Information	3GPP TS 29.272 [29]		
APN-OI-Replacement	3GPP TS 29.272 [29]		
Supported-Features	3GPP TS 29.229 [24]	See NOTE 1.	
Feature-List-ID	3GPP TS 29.229 [24]	See NOTE 1.	
Feature-List	3GPP TS 29.229 [24]	See NOTE 1.	
NOTE 1: There is no separate Diameter application ID defined for the SWd interface so a separate supported feature list is not required. The supported features depend on the command being proxied over SWd.			
NOTE 2: The M-bit settings for re-used AVPs override those of the defining specifications that are referenced. Values include: "Must set", "Must not set". If the M-bit setting is blank, then the defining specification applies.			

Only those AVP initially defined in this reference point and for this procedure are described in the following subchapters.

## 7 SWm Description

### 7.1 Functionality

#### 7.1.1 General

The SWm reference point is defined between the ePDG and the 3GPP AAA Server or between the ePDG and the 3GPP AAA Proxy. The definition of the reference point and its functionality is given in 3GPP TS 23.402 [3].

The SWm reference point shall be used to authenticate and authorize the UE.

The SWm reference point is also used to transport NBM related mobility parameters in a case the UE attaches to the EPC via the S2b (based on PMIPv6 or GTPv2) and SWn reference points (i.e. IP Mobility Mode Selection information).

Additionally the SWm reference point may also be used to transport DSMIPv6 related mobility parameters in case the UE attaches to the EPC using the S2c reference point. In particular, in this case the SWm reference point may be used for conveying the Home Agent IP address or FQDN from the AAA server to the ePDG for Home Agent discovery based on IKEv2 (see TS 24.303 [13]).

## 7.1.2 Procedures Description

### 7.1.2.1 Authentication and Authorization Procedures

#### 7.1.2.1.1 General

The authentication and authorization procedure shall be used between the ePDG and 3GPP AAA Server/Proxy. When a PDN connection is activated by the UE an IKEv2 exchange shall be initiated. It shall be invoked by the ePDG, on receipt from the UE of a "tunnel establishment request" message. This shall take the form of forwarding an IKEv2 exchange with the purpose of authenticating in order to set up an IKE Security Association (SA) between the UE and the ePDG.

During the Access Authentication and Authorization procedure the ePDG may provide information on its PMIPv6 or GTPv2 capabilities to the 3GPP AAA Server. The 3GPP AAA Server may perform IP mobility mode selection between NBM or HBM as specified in subclause 4.1.3.2 of 3GPP TS 23.402 [3]. The 3GPP AAA Server may provide to the ePDG an indication if either NBM or local IP address assignment shall be used. If NBM shall be used, the ePDG then decides the S2b protocol variant to use.

Upon a successful authorization, when NBM is used, the 3GPP AAA server shall return NBM related information back to the ePDG. This information may include the assigned PDN GW, UE IPv6 HNP and/or UE IPv4-HoA.

Upon a successful authorization, when DSMIPv6 is used, to enable HA address discovery based on IKEv2 (see TS 24.303 [13]), the 3GPP AAA server may also download PDN GW identity to the ePDG.

The PDN Gateway identity is a FQDN and/or IP address of the PDN GW. If a FQDN is provided, the ePDG shall derive it to IP address according to the selected mobility management protocol.

If DSMIPv6 is used, a single IKE SA is used for all PDN connections of the user. If PMIPv6 or GTPv2 is used, a separate IKE SA is created for each PDN connection of the user (refer to 3GPP TS 24.302 [26]).

Each new additional IKE SA shall be handled in a different Diameter session. In such cases, the IP mobility mode selected during the first authentication and authorization procedure is valid for all PDN connections of the user, therefore, dynamic IP mobility mode selection is not executed during the further procedures. The ePDG may select the same or different S2b protocol variant(s) towards different PDN GWs when NBM has been selected.

The SWm reference point shall perform authentication and authorization based on the reuse of the DER/DEA command set defined in Diameter EAP application, IETF RFC 4072 [5].

Table 7.1.2.1.1/1: Authentication and Authorization Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
EAP payload	EAP-Payload	M	This information element shall contain the encapsulated EAP payload used for the UE - 3GPP AAA Server mutual authentication
Authentication Request Type	Auth-Request-Type	M	This information element shall indicate whether the user is to be authenticated only, authorized only or both. It shall have the value of AUTHORIZE_AUTHENTICATE.
APN	Service-Selection	C	This information element shall contain the Network Identifier part of the APN for which the UE is requesting authorization. This AVP shall be present when the ePDG has received an APN from the UE in the IKEv2 signalling.
Visited Network Identifier (See 9.2.3.1.2)	Visited-Network-Identifier	C	This information element shall contain the identifier that allows the home network to identify the Visited Network. This AVP shall be present if the ePDG is not in the UE's home network i.e. the UE is roaming.
Access Type	RAT-Type	C	This information element shall be present if the access type is known by the ePDG. If present, it shall contain the non-3GPP access network access technology type that is serving the UE.
Mobility features	MIP6-Feature-Vector	O	This AVP shall be present, if the handling of any of the flags listed here requires dynamic (i.e. per user) handling for the VPLMN-HPLMN relation of the ePDG and 3GPP AAA Server. If present, the AVP shall contain the mobility features supported by the ePDG. Flags that are not relevant in the actual relation shall be set to zero. If dynamic IP mobility mode selection is used, the PMIP6_SUPPORTED flag and/or the GTPv2_SUPPORTED flag shall be set by the ePDG if PMIPv6 and/or GTPv2 are supported. PMIP6_SUPPORTED flag is defined in IETF RFC 5779 [2]. The MIP6_INTEGRATED flag shall be used to indicate to the 3GPP AAA server that the ePDG supports IKEv2 based Home Agent address discovery.
AAA Failure Indication	AAA-Failure-Indication	O	If present, this information element shall indicate that the request is sent after the ePDG has determined that a previously assigned 3GPP AAA Server is unavailable.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.
UE local IP address	UE-Local-IP-Address	O	The ePDG shall include this IE based on local policy for Fixed Broadband access network interworking as specified in 3GPP TS 23.139 [39]. If present, it shall contain the source IPv4 or IPv6 address of the IKE_SA_AUTH message from the UE.

Table 7.1.2.1.1/2: Authentication and Authorization Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	O	This information element, if present, shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
EAP payload	EAP-Payload	O	If present, this information element shall contain the encapsulated EAP payload used for UE - 3GPP AAA Server mutual authentication
Master-Session-Key	EAP-Master-Session-Key	C	This IE shall contain keying material for protecting the communication between the user and the ePDG. It shall be present when Result Code is set to DIAMETER_SUCCESS.
Authentication Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_AUTHENTICATE. See IETF RFC 4072 [5].
Result code	Result-Code / Experimental-Result-Code	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter Base Protocol or as per in NASREQ.
3GPP AAA Server Name	Redirect-Host	C	This information element shall be sent if the Result-Code value is set to DIAMETER_REDIRECT_INDICATION. When the user has previously been authenticated by another 3GPP AAA Server, it shall contain the Diameter identity of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter Base Protocol (IETF RFC 3588 [7]). The command shall contain zero or more occurrences of this information element. When choosing a destination for the redirected message from multiple Redirect-Host AVPs, the receiver shall send the Diameter request to the first 3GPP AAA Server in the ordered list received in the Diameter response. If no successful response to the Diameter request is received, the receiver shall send the Diameter request to the next 3GPP AAA Server in the ordered list. This procedure shall be repeated until a successful response is received from a 3GPP AAA Server.
Mobility Capabilities	MIP6-Feature-Vector	O	This AVP shall be present if it was received in the authentication and authorization request and the authentication and authorization succeeded/ It shall contain the authorized mobility features. Flags that are not relevant in the actual relation shall be set to zero. The PMIP6_SUPPORTED flag and/or the GTPv2_SUPPORTED flag shall be set to indicate that NBM (PMIPv6 or GTPv2) is to be used. The ASSIGN_LOCAL_IP flag shall be set to indicate that a local IP address is to be assigned. The MIP6_INTEGRATED flag shall be set if a Home Agent address is provided for IKEv2 based Home Agent address discovery. In the latter case HA information for IKEv2 discovery is provided via the APN-Configuration AVP.
APN-OI replacement	APN-OI-Replacement	C	This AVP shall indicate the domain name to replace the APN-OI in the non-roaming case or in the home routed roaming case when constructing the PDN GW FQDN upon which it needs to perform a DNS resolution. See 3GPP TS 23.003 [3]. It shall only be included if NBM is used and the Result-Code AVP is set to DIAMETER_SUCCESS.
APN and PGW Data	APN-Configuration	C	This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS. The APN-Configuration is a grouped AVP, defined in 3GPP TS 29.272 [29]. When NBM is used, the following information elements per APN may be included: - APN - APN-AMBR - Authorized 3GPP QoS Profile - User home IP Address (if static IPv4 and/or IPv6 is allocated to the UE's subscribed APN) - Allowed PDN types - PDN GW identity (if the PDN connection was active in case of HO, or if there is a static PDN GW allocated to the UE's subscribed APN) - PDN GW allocation type - VPLMN Dynamic Address Allowed - Visited Network Identifier When local IP address assignment is used, this AVP shall only be present if IKEv2 based Home Agent discovery is used and - if the PDN connection was active in case of HO, or

			<ul style="list-style-type: none"> <li>- if there is static PDN GW allocated to the UE's subscribed APN, or</li> <li>- if the 3GPP AAA Server/Proxy selects the PDN GW based on the identity of the ePDG</li> </ul> <p>In these cases, the following information elements shall be included:</p> <ul style="list-style-type: none"> <li>- HA-APN (Home Agent APN as defined in 3GPP TS 23.003 [14])</li> <li>- PDN GW identity</li> </ul> <p>NOTE 1.</p>
Trace information	Trace-Info	C	<p>This AVP shall be included if the subscriber and equipment trace has been activated for the user in the HSS and signalling based activation is used to download the trace activation from the HSS to the ePDG.</p> <p>Only the Trace-Data AVP shall be included to the Trace-Info AVP and shall contain the following AVPs:</p> <ul style="list-style-type: none"> <li>- Trace-Reference</li> <li>- Trace-Depth</li> <li>- Trace-Event-List, for PGW</li> <li>- Trace-Collection-Entity</li> </ul> <p>The following AVPs may also be included in the Trace-Data AVP:</p> <ul style="list-style-type: none"> <li>- Trace-Interface-List, for PGW, if this AVP is not present, trace report generation is requested for all interfaces for PGW listed in 3GPP TS 32.422 [32]</li> <li>- Trace-NE-Type-List, with the only allowed value being "PDN GW". If this AVP is not included, trace activation in PDN GW is required.</li> </ul>
MSISDN	Subscription-ID	C	<p>This AVP shall contain the MSISDN of the UE and shall be sent only if it is available.</p>
Session time	Session-Timeout	C	<p>If the authorization succeeded, then this IE shall contain the time this authorization is valid for.</p>
Permanent User Identity	Mobile-Node-Identifier	C	<p>This information element shall be present if NBM is used. It shall contain an AAA/HSS assigned permanent user identity (i.e. IMSI in EPC root NAI format as defined in clause 19 of 3GPP TS 23.003 [14]) to be used by:</p> <ul style="list-style-type: none"> <li>- the MAG in subsequent PBUs as the MN-ID identifying the user in the EPS network for PMIP based S2b,</li> <li>- by the ePDG to derive the IMSI to send in subsequent Create Session Request for GTP based S2b.</li> </ul> <p>This IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.</p>
Serving GW Address	MIP6-Agent-Info	O	<p>This AVP shall be used only in chained S2b-S8 cases and it shall be sent only if the Result-Code AVP is set to DIAMETER_SUCCESS.</p>
UE Charging Data	3GPP-Charging-Characteristics	O	<p>This information element contains the type of charging method to be applied to the user (see 3GPP TS 29.061 [31]).</p>
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	<p>If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.</p>
NOTE 1:			<p>If a static PDN GW allocated to the UE's subscribed APN has been received from the HSS, the 3GPP AAA Server/Proxy shall only provide the static PDN GW address in the Authentication and Authorization Answer.</p>

### 7.1.2.1.2 3GPP AAA Server Detailed Behaviour

On receipt of the DER message, the 3GPP AAA Server shall check that the user data exists in the 3GPP AAA Server. If not, the 3GPP AAA Server shall use the procedures defined for the SWx interface to obtain access authentication and authorization data.

If the HSS returns DIAMETER\_ERROR\_USER\_UNKWNOWN, the 3GPP AAA Server shall return the same error to the ePDG.

If the HSS indicates that the user is currently being served by a different 3GPP AAA Server, the 3GPP AAA Server shall respond to the ePDG with the Result-Code set to DIAMETER\_REDIRECT\_INDICATION and Redirect-Host set to the Diameter identity of the 3GPP AAA Server currently serving the user (as indicated in the 3GPP-AAA-Server-Name AVP returned in the SWx authentication response from the HSS).

Otherwise, the 3GPP AAA Server shall proceed with the authentication and authorization procedure. The 3GPP AAA Server shall use the procedures defined in SWx interface to obtain authorization data from HSS.

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

If the user does not have non-3GPP access subscription, then 3GPP AAA Server shall respond to the non-3GPP access network with Experimental-Result-Code DIAMETER\_ERROR\_USER\_NO\_NON\_3GPP\_SUBSCRIPTION.

If a Visited- Network-Identifier is present in the request and if the user is not allowed to roam in the visited network, then the 3GPP AAA Server shall return Experimental-Result-Code set to DIAMETER\_ERROR\_ROAMING\_NOT\_ALLOWED.

Otherwise the 3GPP AAA Server shall run EAP-AKA as specified in 3GPP TS 33.402 [19]. Exceptions to the cases specified here shall be treated by 3GPP AAA Server as error situations, the Result-Code shall be set to DIAMETER\_UNABLE\_TO\_COMPLY and, therefore, no authentication information shall be returned.

Upon receiving the authentication and authorization request from the ePDG, the 3GPP AAA Server marks the trust relationship as "untrusted" with the User Identity. If the 3GPP AAA Server detects that an S6b session already exists for this UE and the S6b session was established as a result of an authentication request for DSMIPv6, the 3GPP AAA Server shall send the trust relationship to the PDN GW as specified in clause 9.1.2.5.

Once authentication is successfully completed, the 3GPP AAA Server shall perform the following authorization checking (if there is an error in any of the steps, the 3GPP AAA Server shall stop processing and return the corresponding error code):

- 1) Check if the user is barred to use the non 3GPP Access. If it is so, then the Result-Code shall be set to DIAMETER\_AUTHORIZATION\_REJECTED
- 2) Check whether the user is barred to use the subscribed APNs. If it is so, Result-Code shall be set to DIAMETER\_AUTHORIZATION\_REJECTED.
- 3) Check if there was request for an APN received. If not, AAA Server shall check, whether the user already has an active PDN connection to the default APN. If it is so, the Result-Code shall be set to DIAMETER\_UNABLE\_TO\_COMPLY. Otherwise, the default APN of the user is selected to be used during the actual authentication and authorization procedure.
- 4) Check if user has a subscription for the requested APN or for the wildcard APN. If not, Experimental-Result-Code shall be set to DIAMETER\_ERROR\_USER\_NO\_APN\_SUBSCRIPTION
- 5) If present, check the flags of the received MIP6-Feature-Vector AVP: The evaluation of the flags is executed only in the first authentication and authorization procedure for the user after an initial attach or handover, in all the subsequent procedures, the AAA Server shall insert the same values.
  - If the MIP6-INTEGRATED flag is set and the 3GPP AAA server has authorized IKEv2 Home Agent assignment, the 3GPP AAA server shall include the Home Agent addresses in the APN-Configuration AVP in the response and the MIP6-Feature-Vector AVP with the MIP6-INTEGRATED flag set. In this case, the 3GPP AAA Sever may select the Home Agent based on the identity of the ePDG as included in the Origin-Host AVP in the authentication and authorization request if no static PDN GW address is received from the HSS. If the HA assignment via IKEv2 is not used, the MIP6-Feature-Vector AVP with the MIP6-INTEGRATED flag not set shall be sent.
  - The PMIP6\_SUPPORTED and/or GTPv2\_SUPPORTED flag indicates to the 3GPP AAA server whether the ePDG supports NBM or not. As specified in 3GPP TS 23.402 [3], based on the information it has regarding the UE (see 3GPP TS 24.302 [26]), local/home network capabilities and local/home network policies, the 3GPP AAA server may perform mobility mode selection. If the 3GPP AAA server decides that NBM should be used, the PMIP6\_SUPPORTED and GTPv2\_SUPPORTED flags shall be set in the response to indicate the NBM support of the UE to the ePDG. If only the PMIP6\_SUPPORTED or the GTPv2\_SUPPORTED flag is present in the response, the ePDG shall assume that this also indicates the NBM support of the UE to the ePDG and the ePDG may select any S2b protocol variant (PMIPv6 or GTPv2). If the 3GPP AAA server decides that a local IP address should be assigned, the ASSIGN\_LOCAL\_IP flag shall be set in the response to indicate to the ePDG that a local IP address should be assigned.

NOTE: When selecting DSMIPv6, the AAA server assumes that the ePDG has the capability to assign a local IP address to the UE.

- The 3GPP AAA server shall not set the PMIP6\_SUPPORTED/GTPv2\_SUPPORTED and ASSIGN\_LOCAL\_IP flags both at the same time in the response.

Upon successful authentication and authorization, the 3GPP AAA Server shall return user data relevant to the APN as received from the HSS. The Result-Code shall be set to DIAMETER\_SUCCESS.

Exceptions to the cases specified here shall be treated by 3GPP AAA Server as error situations, the Result-Code shall be set to DIAMETER\_UNABLE\_TO\_COMPLY and, therefore, no authorization information shall be returned.

For Fixed Broadband access network interworking as specified in 3GPP TS 23.139 [39], the 3GPP AAA server shall determine if the UE is connected via a BBF-defined WLAN access according to the UE local IP address in UE-Local-IP-Address AVP from the ePDG. If the UE is connected via a BBF-defined WLAN access, the 3GPP AAA server shall perform the enabling UE reflective QoS function as specified in 3GPP TS 24.139 [43].

#### 7.1.2.1.3 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy shall be required to handle roaming cases in which the ePDG is in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy with the following additions.

On receipt of the first authentication and authorization request, the 3GPP AAA Proxy shall check locally configured information whether users from the HPLMN are allowed to activate a PDN connection from the non-3GPP access network via this (V)PLMN. If not, the Experimental-Result-Code shall be set to DIAMETER\_ERROR\_ROAMING\_NOT\_ALLOWED and the authentication response shall be sent to the ePDG.

On receipt of the authentication and authorization answer that completes a successful authentication, the 3GPP AAA Proxy

- may check locally configured information about using the chained S8-S2b option towards the given HPLMN. If chaining is required, the 3GPP AAA Proxy shall select a Serving GW from its network configuration database and shall include the Serving GW address in the response.
- shall check locally configured information for the maximum allowed static QoS parameters valid for visitors from the given HPLMN and modify the QoS parameters received from the 3GPP AAA Server, to enforce the policy limitations.
- shall record the state of the connection (i.e. Authorization Successful).
- may select the Home Agent based on the identity of the ePDG as included in the Origin-Host AVP in the authentication and authorization request if IKEv2 based Home Agent discovery is used and VPLMN Dynamic Address Allowed AVP is received. In this case, the 3GPP AAA proxy shall include the Home Agent addresses in the APN-Configuration AVP in the response and the MIP6-Feature-Vector AVP with the MIP6-INTEGRATED flag set if no static PDN GW address is received from the 3GPP AAA Server.

#### 7.1.2.1.4 ePDG Detailed Behaviour

The ePDG shall initiate a new authentication and authorization procedure for each new IKE\_SA. Each IKE\_SA shall be handled in a different session.

The ePDG shall set flags signalling its capabilities to the same value in all authentication and authorization procedure for the same user (include the same MIP6-Feature-Vector). During the second and further authentication and authorization procedures, the ePDG shall discard the flag values received from the AAA Server and reuse the values received during the first procedure executed for the user.

For PMIPv6/GTPv2 based S2b, when receiving a Serving GW address in an authentication response, the ePDG shall check, whether it has already a Serving GW address stored for the user.

- If it has no Serving GW address available, it shall store the received value and use it as LMA address when creating PMIP bindings.
- If it has already a stored Serving GW address value, it shall ignore the received SGW-Address AVP.

NOTE 1: In case of untrusted access, there is an authentication session started for all PDN connection setup requests of a user. These sessions may invoke different 3GPP AAA Proxies, which in turn may assign different Serving GWs to the user. The ePDG behaviour ensures that in spite of this possibility, the same Serving GW is used for all PDN connections of the user.

NOTE 2: The ePDG knows if NBM is used or if a local IP address is assigned based on the flags in the MIP6-Feature-Vector or based on preconfigured information. If the PMIP6\_SUPPORTED and/or the GTPv2\_SUPPORTED flag are set in the MIP6-Feature-Vector received from the 3GPP AAA Server, the ePDG knows that NBM is used.

For PMIPv6/GTPv2 based S2b, the ePDG shall utilize the downloaded APN configuration data to authorize the UE requested home address types: IPv4 home address and/or IPv6 home network prefix.

The ePDG may use the Visited\_Network\_Identifier to determine the S2b protocol type (PMIPv6 or GTPv2). The ePDG may be configured with the S2b protocol variant(s) on a per HPLMN granularity, or may retrieve information regarding the S2b protocol variants supported by the PDN GW (PMIPv6 or/and GTPv2) from the Domain Name Service Function as described in 3GPP TS 29.303[34].

If GTPv2 is used on S2b and if the Trace-Info AVP including Trace-Data has been received in the authorization response, the ePDG shall send a GTPv2 Trace Session Activation message (see 3GPP TS 29.274 [38]) to the PGW to start a trace session for the user.

If DSMIPv6 is used and if ePDG has received the PGW identity in form of the FQDN from the 3GPP AAA server, then the ePDG may obtain the IP address of the Home Agent functionality of that PGW as described in 3GPP TS 29.303 [34].

If the ePDG determines that a previously assigned 3GPP AAA Server is unavailable, it may attempt to send a new authentication and authorization request to an alternate 3GPP AAA Server. If the ePDG receives from this new server a redirect indication towards the former server (due to the HSS having stored the former 3GPP AAA Server identity), it shall terminate all previously existing sessions and PDN connections for that user, and it shall re-send again the request towards the new server, but it shall include the AAA-Failure-Indication AVP in the new request.

## 7.1.2.2 Authorization Procedures

### 7.1.2.2.1 General

This procedure shall be used between the ePDG and 3GPP AAA Server and Proxy. It shall be invoked by the ePDG, upon receipt of a valid Re-Authorization Request message from the 3GPP AAA Server (see section 7.1.2.5).

This procedure shall be used by the ePDG to update the previously provided authorization parameters. This may happen due to a modification of the subscriber profile in the HSS (for example, removal of a specific APN associated with the subscriber, or change of the identity of a dynamically allocated PDN GW, see subclause 8.1.2.3).

This procedure is mapped to the Diameter command codes AA-Request (AAR) and AA-Answer (AAA) specified in RFC 4005 [4]. Information element contents for these messages are shown in tables 7.1.2.2.1/1 and 7.1.2.2.1/2.

**Table 7.1.2.2.1/1: SWm Authorization Request**

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Request Type	Auth-Request-Type	M	This information element shall contain the type of request. It shall have the value AUTHORIZE_ONLY.

Table 7.1.2.2.1/2: SWm Authorization Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15], and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_ONLY. See IETF RFC 4072 [5].
Registration Result	Result-Code/ Experimental Result Code	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter Base Protocol or as per in NASREQ.
UE IPv4 Home Address	PMIP6-IPv4-Home-Address	O	If the authorization succeeded, and the user has an IPv4-HoA statically defined as part of his profile data, then this IE may be present. It shall contain the IPv4-HoA allocated and assigned to the UE.
APN-OI replacement	APN-OI-Replacement	C	This AVP shall indicate the domain name to replace the APN-OI in the non-roaming case or in the home routed roaming case when constructing the PDN GW FQDN upon which it needs to perform a DNS resolution. See 3GPP TS 23.003 [3]. It shall only be included if NBM is used and the Result-Code AVP is set to DIAMETER_SUCCESS.
APN and PGW Data	APN-Configuration	C	This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS. APN-Configuration is a grouped AVP, defined in 3GPP TS 29.272 [29]. When NBM is used, the following information elements per APN may be included: <ul style="list-style-type: none"> <li>- APN</li> <li>- APN-AMBR</li> <li>- Authorized 3GPP QoS profile</li> <li>- Statically allocated User IP Address (IPv4 and/or IPv6)</li> <li>- Allowed PDN types</li> <li>- PDN GW identity</li> <li>- PDN GW allocation type</li> <li>- VPLMN Dynamic Address Allowed</li> <li>- Visited Network Identifier</li> </ul> When local IP address assignment is used, this AVP shall only be present if IKEv2 based Home Agent discovery is used and <ul style="list-style-type: none"> <li>- if the PDN connection was active in case of HO, or</li> <li>- if there is static PDN GW allocated to the UE's subscribed APN.</li> </ul> In these cases, the following information elements shall be included: <ul style="list-style-type: none"> <li>- HA-APN (Home Agent APN as defined in 3GPP TS 23.003 [14])</li> <li>- PDN GW identity</li> </ul>
Trace information	Trace-Info	C	This AVP shall be included if the subscriber and equipment trace has been activated for the user in the HSS and signalling based activation is used to download the trace activation from the HSS to the ePDG.  Only the Trace-Data AVP shall be included if trace activation is requested. Only the Trace-Reference AVP shall be included if trace deactivation is requested.  If the Trace-Data AVP is included, it shall contain the following AVPs: <ul style="list-style-type: none"> <li>- Trace-Reference</li> <li>- Trace-Depth</li> <li>- Trace-Event-List, for PGW</li> <li>- Trace-Collection-Entity</li> </ul> The following AVPs may also be included in the Trace-Data AVP: <ul style="list-style-type: none"> <li>- Trace-Interface-List, for PGW, if this AVP is not present, trace report generation is requested for all interfaces for PGW listed in 3GPP TS 32.422 [32]</li> <li>- Trace-NE-Type-List, with the only allowed value being "PDN GW". If this AVP is not included, trace activation in PDN GW is required.</li> </ul>
MSISDN	Subscription-ID	C	This AVP shall contain the MSISDN of the UE and shall be sent only if it is available.
UE Charging Data	3GPP-Charging-Characteristics	O	If present, this information element shall contain the type of charging method to be applied to the user (see 3GPP TS 29.061 [31]).

Session time	Session-Timeout	C	If the authorization succeeded, then this IE shall contain the time this authorization is valid for.
--------------	-----------------	---	--

#### 7.1.2.2.2 3GPP AAA Server Detailed Behaviour

The 3GPP AAA Server shall process the steps in the following order (if there is an error in any of the steps, the 3GPP AAA Server shall stop processing and return the corresponding error code):

- 1) Check that the user exists in the 3GPP AAA Server. The check shall be based on Diameter Session-id and User Name. If the Session-Id included in the request does not correspond with any active session, or if an active session is found but it does not belong to the user identified by the User Name parameter, Experimental-Result-Code shall be set to DIAMETER\_ERROR\_USER\_UNKNOWN.
- 2) Check whether the user is allowed to access the APN. If not, Result-Code shall be set to DIAMETER\_AUTHORIZATION\_REJECTED.
- 3) The 3GPP AAA Server shall return user data relevant to the APN as received from the HSS. The Result-Code shall be set to DIAMETER\_SUCCESS.

Once the Authentication and Authorization procedure successfully finishes, the 3GPP AAA Server shall download, together with authentication data, the list of authorized APNs and the authorized mobility protocols in the authentication and authorization response from the HSS (see SWx procedure in Section 8.1.2.1).

Exceptions to the cases specified here shall be treated by 3GPP AAA Server as error situations, the Result-Code shall be set to DIAMETER\_UNABLE\_TO\_COMPLY and, therefore, no authorization information shall be returned.

#### 7.1.2.2.3 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy shall be required to handle roaming cases in which the ePDG is in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy, with the following extensions.

On receipt of the authorization answer, the 3GPP AAA Proxy:

- Shall check locally configured information for the maximum allowed static QoS parameters valid for visitors from the given HPLMN and modify the QoS parameters received from the 3GPP AAA Server, to enforce the policy limitations.
- Shall record the state of the connection (i.e. Authorization Successful).

#### 7.1.2.2.4 ePDG Detailed Behaviour

The ePDG shall initiate the authorization procedure after successfully completing the authentication of the user. The ePDG shall initiate a separate authorization session for each IKE\_SA of the user.

If NBM is used, at successful completion of the procedure, the ePDG shall store the APN configuration data received from the 3GPP AAA Server. The ePDG shall utilize these data to authorize the requested home address types: IPv4 home address and/or IPv6 home network prefix.

**NOTE:** The user will be allowed to create PDN connections only to the subscribed APNs and use the address types that are allowed by the subscribed PDN types.

Upon receiving the authorization response:

- If NBM is used and if any other Result-Code than DIAMETER\_SUCCESS was received in the response, the ePDG shall release the corresponding PDN connection (PMIPv6 binding or GTPv2 tunnel) and IKE\_SA of the user.
- If DSMIPv6 is used,
  - If any other Result-Code than DIAMETER\_SUCCESS was received, the ePDG shall release the corresponding IKE\_SA of the user.

- If the Result-Code DIAMETER\_SUCCESS was received in the response, the ePDG shall update the previously provided authorization parameters.

NOTE: The ePDG knows if NBM is used or if a local IP address is assigned based on the flags in the MIP6-Feature-Vector received during the initial authentication and authorization procedure or based on preconfigured information. If the PMIP6\_SUPPORTED and/or the GTPv2\_SUPPORTED flag are set in the MIP6-Feature-Vector received from the 3GPP AAA Server, the ePDG knows that NBM is used.

If GTPv2 is used on S2b and if the Trace-Info AVP including Trace-Data has been received in the authorization response, the ePDG shall send a GTPv2 Trace Session Activation message (see 3GPP TS 29.274 [38]) to the PGW to start a trace session for the user. If the Trace-Info AVP including Trace-Reference (directly under the Trace-Info) has been received in the authorization response, the ePDG shall send a GTPv2 Trace Session Deactivation message to the PGW to stop the ongoing trace session, identified by the Trace-Reference. For details, see 3GPP TS 32.422 [32].

If DSMIPv6 is used and if ePDG has received the PGW identity in form of the FQDN from the 3GPP AAA server, then the ePDG may obtain the IP address of the Home Agent functionality of that PGW as described in 3GPP TS 29.303 [34].

### 7.1.2.3 ePDG Initiated Session Termination Procedures

#### 7.1.2.3.1 General

The SWm reference point allows the ePDG to inform the 3GPP AAA Server/Proxy 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 are to be removed.

The SWm Session Termination Request procedure shall be initiated by the ePDG to the 3GPP AAA Server which shall remove associated non-3GPP Access information. The AAA Server shall then return the SWm Session Termination Answer containing the result of the operation. These procedures are based on the reuse of Diameter Base IETF RFC 3588 [7] STR and STA commands

**Table 7.1.2.3.1/1: SWm Session Termination Request**

Information Element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Termination Cause	Termination-Cause	M	This information element shall contain the reason for the disconnection.

**Table 7.1.2.3.1/2: SWm Session Termination Answer**

Information Element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code	M	This IE shall contain the result of the operation.

#### 7.1.2.3.2 3GPP AAA Server Detailed Behavior

Upon reception of the Session Termination Request message from the ePDG, the 3GPP AAA Server shall check that there is an ongoing session associated to the two parameters received (Session-Id and User-Name).

If an active session is found and it belongs to the user identified by the User-Name parameter, the 3GPP AAA Server shall release the session resources associated to the specified session and a Session Termination Response shall be sent to the ePDG, indicating DIAMETER\_SUCCESS.

Otherwise, the 3GPP AAA Server returns a Session Termination Response with the Diameter Error DIAMETER\_UNKNOWN\_SESSION\_ID.

### 7.1.2.3.3 3GPP AAA Proxy Detailed Behavior

The 3GPP AAA Proxy is required to handle roaming cases in which the ePDG is located in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy.

On receipt of the Session Termination Request message from the ePDG, the 3GPP AAA Proxy shall route the message to the 3GPP AAA Server.

On receipt of the Session Termination Answer message from the 3GPP AAA Server, the 3GPP AAA Proxy shall route the message to the ePDG, and it shall release any local resources associated to the specified session only if the result code is set to DIAMETER\_SUCCESS.

### 7.1.2.4 3GPP AAA Server Initiated Session Termination Procedures

#### 7.1.2.4.1 General

The SWm reference point shall allow the 3GPP AAA Server to request the termination of an IKE\_SA between UE and ePDG, and therefore the termination of all mobility session established for all associated PDN connections.

If the user has several accesses (IKE\_SA) active at an ePDG, a separate Session Termination procedure shall be initiated for each of them.

The procedure shall be initiated by the 3GPP AAA Server. This procedure is based on the reuse of NASREQ IETF RFC 4005 [4] ASR, ASA, STR and STA commands.

**Table 7.1.2.4.1/1: SWm Abort Session Request**

Information Element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Auth-Session-State	Auth-Session-State	O	If present, this information element indicates to the ePDG whether the 3GPP AAA Server requires an STR message.

**Table 7.1.2.4.1/2: SWm Abort Session Answer**

Information Element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code	M	This IE shall contain the result of the operation.

**Table 7.1.2.4.1/3: SWm Session Termination Request**

Information element name	Mapping to Diameter AVP	Cat.	Description
Termination-Cause	Termination-Cause	M	This information element shall contain the reason why the session was terminated. It shall be set to "DIAMETER_ADMINISTRATIVE" to indicate that the session was terminated in response to an ASR message.

**Table 7.1.2.4.1/4: SWm Session Termination Answer**

Information element name	Mapping to Diameter AVP	Cat.	Description
Result-Code	Result-Code	M	This IE shall contain the result of the operation.

#### 7.1.2.4.2 3GPP AAA Server Detailed Behaviour

The 3GPP AAA Server shall make use of this procedure to instruct the ePDG to terminate the IKE\_SA between UE and ePDG.

In the DSMIPv6 case, the 3GPP AAA Server shall initiate first the detach procedure over the S6b reference point towards the PDN GW. When this process has finalized, the 3GPP AAA Server can initiate the termination of the IKE\_SA towards the ePDG.

The 3GPP AAA Server shall include the Auth-Session-State AVP in the ASR command with a value of NO\_STATE\_MAINTAINED if it does not require a STR from the ePDG. If it does require a STR from the ePDG, the 3GPP AAA Server shall either omit the Auth-Session-State AVP from the ASR command or include the Auth-Session-State AVP in the ASR command with a value of STATE\_MAINTAINED.

On receipt of the ASR command, the ePDG shall check if there is an ongoing session associated with the received Session-Id. If an active session is found and it belongs to the user identified by the User-Name parameter, the ePDG shall terminate the associated IKE\_SA between UE and ePDG and return an ASA to the 3GPP AAA Server with the Result-Code to DIAMETER\_SUCCESS. Otherwise, the ePDG shall return an ASA to the 3GPP AAA Server with the Result-Code set to DIAMETER\_UNKNOWN\_SESSION\_ID.

On receipt of the ASA with a Result-Code of DIAMETER\_SUCCESS, the 3GPP AAA Server shall release any local resources associated with the specified session.

If required by the 3GPP AAA Server, the ePDG shall send an STR with the Termination-Cause set to DIAMETER\_ADMINISTRATIVE. The 3GPP AAA Server shall set the Result-Code to DIAMETER\_SUCCESS and return the STA command to the ePDG.

#### 7.1.2.4.3 3GPP AAA Proxy Detailed Behaviour

When the 3GPP AAA Proxy receives the ASR from the 3GPP AAA Server it shall route the request to the ePDG.

If the 3GPP AAA Proxy requires an STR but the 3GPP AAA Server does not, the 3GPP AAA Proxy may override the value of the Auth-Session-State in the ASR and set it to STATE\_MAINTAINED. In this case, the 3GPP AAA Proxy shall not forward the STR received from the ePDG onto the 3GPP AAA Server and shall return an STA command to the ePDG with the Result-Code set to DIAMETER\_SUCCESS. The 3GPP AAA Proxy shall not override the value of the Auth-Session-State AVP under any other circumstances.

On receipt of the ASA message with Diameter Result Code set to DIAMETER\_SUCCESS, the 3GPP AAA Proxy shall route the successful response to the 3GPP AAA Server and shall release any local resources associated with the session.

When the 3GPP AAA Proxy receives the STR from ePDG, it shall route the request to the 3GPP AAA Server. On receipt of the STA message, the 3GPP AAA Proxy shall route the response to the ePDG.

### 7.1.2.5 Authorization Information Update Procedures

#### 7.1.2.5.1 General

This procedure shall be used between the 3GPP AAA Server and the ePDG for the purpose of modifying the previously provided authorization parameters. This may happen due to a modification of the subscriber profile in the HSS (for example change of the identity of a dynamically allocated PDN GW, see subclause 8.1.2.3).

This procedure shall be performed in two steps:

- The 3GPP AAA Server shall issue an unsolicited re-authorization request towards the ePDG. Upon receipt of such a request, the ePDG shall respond to the request and indicate the disposition of the request. This procedure is based on the Diameter commands Re-Auth-Request and Re-Auth-Answer specified in IETF RFC 3588 [7]. Information element contents for these messages shall be as shown in tables 7.1.2.5.1/1 and 7.1.2.5.1/2.
- Upon receiving the re-authorization request, the ePDG shall immediately invoke the authorization procedure specified in 7.1.2.2 for the session indicated in the request. This procedure is based on the Diameter

commands Re-Auth-Request (RAR) and Re-Auth-Answer (RAA) specified in IETF RFC 4005 [4]. Information element contents for these messages are shown in tables 7.1.2.2.1/1 and 7.1.2.2.1/2.

**Table 7.1.2.5.1/1: SWm Authorization Information Update Request**

Information Element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Re-Auth Request Type	Re-Auth-Request-Type	M	This IE shall define whether the user is to be authorized only or authenticated and authorized. AUTHORIZE_ONLY shall be set in this case.
Routing Information	Destination-Host	M	This information element shall be obtained from the Origin-Host AVP, which was included in a previous command received from the trusted non-3GPP access.

**Table 7.1.2.5.1/2: SWm Authorization Information Update Answer**

Information Element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Result	Result-Code	M	This IE shall contain the result of the operation.

### 7.1.2.5.2 3GPP AAA Server Detailed Behaviour

The 3GPP AAA server shall make use of the re-authorization procedure defined in the Diameter base protocol, IETF RFC 3588 [7] to indicate that relevant service authorization information shall be updated in the ePDG.

### 7.1.2.5.3 ePDG Detailed Behaviour

Upon receipt of the Re-authorization Request message from the 3GPP AAA Server or the 3GPP AAA Proxy, the ePDG shall check that there is an ongoing session associated to any of the parameters received in the message (identified by the Session-Id AVP and the User-Name AVP).

If an active session is found, the ePDG shall initiate an authorization procedure for the session identified by the Session-Id AVP and the User-Name AVP and a Re-authorization Answer message shall be sent to the 3GPP AAA Server or the 3GPP AAA Proxy with the Result-Code indicating DIAMETER\_SUCCESS.

If the Session-Id included in the request does not correspond with any active session, or if an active session is found but it does not belong to the user identified by the User Name parameter, then an Re-authorization Answer message shall be sent to the 3GPP AAA Server or the 3GPP AAA Proxy with the Result-Code indicating DIAMETER\_UNKNOWN\_SESSION\_ID.

Exceptions to the cases specified here shall be treated by ePDG as error situations, the Result-Code shall be set to DIAMETER\_UNABLE\_TO\_COMPLY and, therefore, no authorization procedure shall be initiated.

Table 7.1.2.5.3/1 details the valid result codes that the ePDG can return in the response.

**Table 7.1.2.5.3/1: Re-authorization Answer valid result codes**

Result-Code AVP value	Condition
DIAMETER_SUCCESS	The request succeeded.
DIAMETER_UNKNOWN_SESSION_ID	The request failed because the user is not found in ePDG.
DIAMETER_UNABLE_TO_COMPLY	The request failed.

## 7.2 Protocol Specification

### 7.2.1 General

The SWm reference point shall be based on Diameter, as defined in IETF RFC 3588 [7] and contain the following additions and extensions:

- IETF RFC 4005 [4], which defines a Diameter protocol application used for Authentication, Authorization and Accounting (AAA) services in the Network Access Server (NAS) environment.
- IETF RFC 4072 [5], which provides a Diameter application to support the transport of EAP (IETF RFC 3748 [8]) frames over Diameter.
- IETF RFC 5779 [2], which defines a Diameter extensions and application for PMIPv6 MAG to AAA and LMA to AAA interfaces.
- IETF RFC 5447 [6], which defines Diameter extensions for Mobile IPv6 NAS to AAA interface.

In the case of an untrusted non-3GPP IP access, the MAG to 3GPP AAA server or the MAG to 3GPP AAA proxy communication shall use the MAG to AAA interface functionality defined in IETF RFC 5779 [2] and the NAS to AAA interface functionality defined in IETF RFC 5447 [6].

The Diameter application for the SWm reference point shall use the Diameter Application Id with value 16777264.

### 7.2.2 Commands

#### 7.2.2.1 Commands for SWm Authentication and Authorization Procedures

##### 7.2.2.1.1 Diameter-EAP-Request (DER) Command

The Diameter-EAP-Request (DER) command, indicated by the Command-Code field set to 268 and the "R" bit set in the Command Flags field, is sent from a ePDG to a 3GPP AAA Server/Proxy. The ABNF is based on the one in IETF RFC 5779 [2].

```

< 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 ]
    [ AAA-Failure-Indication ]
    *[ Supported-Features ]
    [ UE-Local-IP-Address ]
    ...
    *[ AVP ]

```

##### 7.2.2.1.2 Diameter-EAP-Answer (DEA) Command

The Diameter-EAP-Answer (DER) command, indicated by the Command-Code field set to 268 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA Server/Proxy to the ePDG. The ABNF is based on the one in IETF RFC 5779 [2].

```

< Diameter-EAP-Answer > ::= < Diameter Header: 268, PXY, 16777264 >

```

```

< Session-Id >
{ Auth-Application-Id }
{ Auth-Request-Type }
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
[ EAP-Payload ]
[ User-Name ]
[ 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 ]
*[ Redirect-Host ]
*[ Supported-Features ]
...
*[ AVP ]

```

#### 7.2.2.1.3 Diameter-AA-Request (AAR) Command

The AA-Request (AAR) command, indicated by the Command-Code field set to 265 and the "R" bit set in the Command Flags field, is sent from a ePDG to a 3GPP AAA Server/Proxy.

```

<AA-Request> ::=
< Diameter Header: 265, REQ, PXY, 16777264 >
< Session-Id >
{ Auth-Application-Id }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Auth-Request-Type }
[ User-Name ]
...
*[ AVP ]

```

#### 7.2.2.1.4 Diameter-AA-Answer (AAA) Command

The AA-Answer (AAA) command, indicated by the Command-Code field set to 265 and the "R" bit cleared in the Command Flags field, is sent from 3GPP AAA Server/Proxy to a ePDG.

```

<AA-Answer> ::=
    < Diameter Header: 265, REQ, PXY, 16777264 >
    < Session-Id >
    { Auth-Application-Id }
    { Auth-Request-Type }
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    [ User-Name ]
    [ APN-OI-Replacement ]
    [ APN-Configuration ]
    [ Trace-Info ]
    [ Subscription-ID ]
    [ 3GPP-Charging-Characteristics ]
    [ Session-Timeout ]
    ...
    *[ AVP ]

```

## 7.2.2.2 Commands for ePDG Initiated Session Termination

### 7.2.2.2.1 Session-Termination-Request (STR) Command

The Session-Termination-Request (STR) command, indicated by the Command-Code field set to 275 and the "R" bit set in the Command Flags field, is sent from a ePDG to a 3GPP AAA Server/Proxy. The ABNF is based on the one in IETF RFC 3588 [7], and is defined as follows:

```

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

```

### 7.2.2.2.2 Session-Termination-Answer (STA) Command

The Session-Termination-Answer (STA) command, indicated by the Command-Code field set to 275 and the "R" bit clear in the Command Flags field, is sent from a 3GPP AAA Server/Proxy to a ePDG. The ABNF is based on the one in IETF RFC 3588 [7], and is defined as follows:

```

< Session-Termination-Answer > ::=
    < Diameter Header: 275, PXY, 16777264 >
    < Session-Id >
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    ...
    *[ AVP ]

```

## 7.2.2.3 Commands for 3GPP AAA Server Initiated Session Termination

### 7.2.2.3.1 Abort-Session-Request (ASR) Command

The Abort-Session-Request (ASR) command shall be indicated by the Command-Code field set to 274 and the "R" bit set in the Command Flags field, and shall be sent from a 3GPP AAA Server/Proxy to an ePDG. The ABNF is based on that in IETF RFC 4005 [4].

```

< Abort-Session-Request > ::=
    < Diameter Header: 274, REQ, PXY, 16777264 >
    < Session-Id >
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }

```

```

    { Destination-Host }
    { Auth-Application-Id }
    [ User-Name ]
    [ Auth-Session-State ]
    ...
    *[ AVP ]

```

#### 7.2.2.3.2 Abort-Session-Answer (ASA) Command

The Abort-Session-Answer (ASA) command shall be indicated by the Command-Code field set to 274 and the "R" bit cleared in the Command Flags field, and shall be sent from a ePDG to a 3GPP AAA Server/Proxy. The ABNF is based on that in IETF RFC 4005 [4].

```

< Abort-Session-Answer > ::= < Diameter Header: 274, PXY, 16777264 >
    < Session-Id >
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    ...
    *[ AVP ]

```

#### 7.2.2.3.3 Session-Termination-Request (STR) Command

The Session-Termination-Request (STR) command, indicated by the Command-Code field set to 275 and the "R" bit set in the Command Flags field, is sent from an ePDG to a 3GPP AAA Server/Proxy. The Command Code value and ABNF are re-used from the IETF RFC 3588 [7] Session-Termination-Request command.

```

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

```

#### 7.2.2.3.4 Session-Termination-Answer (STA) Command

The Session-Termination-Answer (STA) command, indicated by the Command-Code field set to 275 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA Server/Proxy to an ePDG. The Command Code value and ABNF are re-used from the IETF RFC 3588 [7] Session-Termination-Answer command.

```

<Session-Termination-Answer> ::= < Diameter Header: 275, PXY, 16777264 >
    < Session-Id >
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    *[ AVP ]

```

### 7.2.2.4 Commands for Authorization Information Update

#### 7.2.2.4.1 Re-Auth-Request (RAR) Command

The Re-Auth-Request (RAR) command shall be indicated by the Command-Code field set to 258 and the "R" bit set in the Command Flags field, and shall be sent from a 3GPP AAA Server/Proxy to a ePDG. The ABNF is based on the one in IETF RFC 4005 [4] and is defined as follows.

```

< Re-Auth-Request > ::= < Diameter Header: 258, REQ, PXY, 16777264 >
    < Session-Id >
    { Origin-Host }
    { Origin-Realm }

```

```

    { Destination-Realm }
    { Destination-Host }
    { Auth-Application-Id }
    { Re-Auth-Request-Type }
    [ User-Name ]
    ...
    *[ AVP ]

```

#### 7.2.2.4.2 Re-Auth-Answer (RAA) Command

The Re-Auth-Answer (RAA) command shall be indicated by the Command-Code field set to 258 and the "R" bit cleared in the Command Flags field, and shall be sent from a ePDG to a 3GPP AAA Server/Proxy. The ABNF is based on the one in IETF RFC 4005 [4] and is defined as follows.

```

< Re-Auth-Answer > ::=
    < Diameter Header: 258, PXY, 16777264 >
    < Session-Id >
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    [ User-Name ]
    ...
    *[ AVP ]

```

### 7.2.3 Information Elements

#### 7.2.3.1 General

The following table describes the Diameter AVPs defined for the SWm interface protocol for untrusted non-3GPP access, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted.

**Table 7.2.3.1/1: Diameter SWm AVPs**

Attribute Name	AVP Code	Section defined	Value Type	AVP Flag rules			
				Must	May	Should not	Must not
APN-Configuration	1430	8.2.3.7	Grouped	M,V			P
Mobile-Node-Identifier	506	5.2.3.2	OctetString	M			V,P
MIP6-Feature-Vector	124	5.2.3.3	Unsigned64	M			V,P
QoS-Capability	578	9.2.3.2.4	Grouped	M			V,P
RAT-Type	1032	5.2.3.6	Enumerated	M,V			P
Visited-Network-Identifier	600	9.2.3.1.2	OctetString	M,V			P
Trace-Info	1505	8.2.3.1.3	Grouped	V			M,P
Service-Selection	493	5.2.3.5	UTF8String	M			V,P

The following table describes the Diameter AVPs re-used by the SWm interface protocol from existing Diameter Applications, including a reference to their respective specifications and when needed, a short description of their use within SWm. Other AVPs from existing Diameter Applications, except for the AVPs from Diameter Base Protocol, do not need to be supported.

Table 7.2.3.1/2: SWm re-used Diameter AVPs

Attribute Name	Reference	Comments
Auth-Request-Type	IETF RFC 3588 [7]	
Subscription-ID	IETF RFC 4006 [20]	
EAP-Master-Session-Key	IETF RFC 4072 [5]	
EAP-Payload	IETF RFC 4072 [5]	
Re-Auth-Request-Type	IETF RFC 3588 [7]	
Session-Timeout	IETF RFC 3588 [7]	
User-Name	IETF RFC 3588 [7]	
MIP6-Agent-Info	IETF RFC 5447 [6]	
APN-OI-Replacement	3GPP TS 29.272 [29]	
Supported-Features	3GPP TS 29.229 [24]	
Feature-List-ID	3GPP TS 29.229 [24]	See section 7.2.3.2
Feature-List	3GPP TS 29.229 [24]	See section 7.2.3.3
3GPP-Charging-Characteristics	3GPP TS 29.061 [31]	
UE-Local-IP-Address	3GPP TS 29.212 [23]	

Only those AVP initially defined in this reference point and for this procedure are described in the following subchapters.

### 7.2.3.2 Feature-List-ID AVP

The syntax of this AVP is defined in 3GPP TS 29.229 [24]. For this release, the Feature-List-ID AVP value shall be set to 1 for the SWm application.

### 7.2.3.3 Feature-List AVP

The syntax of this AVP is defined in 3GPP TS 29.229 [24]. A null value indicates that there is no feature used by the SWm application.

NOTE: There are no SWm features defined for this release.

## 7.2.4 Session Handling

The Diameter protocol between the ePDG and the 3GPP AAA Server or the 3GPP AAA Proxy shall always keep the session state, and use the same Session-Id parameter for the lifetime of each Diameter session.

A Diameter session shall identify

- a PDN Connection of a given user, if NBM is used
- a user, if DSMIPv6 is used.

In order to indicate that the session state is to be maintained, the Diameter client and server shall not include the Auth-Session-State AVP, either in the request or in the response messages (see IETF RFC 3588 [7]).

## 8 SWx Description

### 8.1 Functionality

#### 8.1.1 General

The SWx reference point is defined between the 3GPP AAA Server and the HSS. The description of the reference point and its functionality is given in 3GPP TS 23.402 [3].

The SWx reference point is used to authorize the UE and to transport NBM related mobility parameters when NBM is used to establish connectivity to the EPC.

The SWx is used to authenticate and authorize the UE when the S2a, S2b or S2c reference points are used to connect to EPC. This reference point is also used to update the HSS with the PDN-GW address information. Additionally, this reference point may be used to retrieve and update other mobility related parameters including static QoS profiles for non-3GPP accesses.

Additional requirements for the SWx interface can be found in section 12 of 3GPP TS 23.402 [3].

## 8.1.2 Procedures Description

### 8.1.2.1 Authentication Procedure

#### 8.1.2.1.1 General

This procedure is used between the 3GPP AAA Server and the HSS. The procedure is invoked by the 3GPP AAA Server when a new set of authentication information for a given subscriber is to be retrieved from an HSS. This can happen for example, when a new trusted or untrusted non 3GPP/IP access subscriber has accessed the 3GPP AAA Server for authentication or when a new set of authentication information is required for one of the subscribers already registered in the 3GPP AAA server. The procedure shall be invoked by 3GPP AAA Server when it detects that the VPLMN or access network has changed.

**Table 8.1.2.1.1/1: Authentication request**

Information element name	Mapping to Diameter AVP	Cat.	Description
IMSI	User-Name (See IETF RFC 3588 [7])	M	This information element shall contain the user IMSI, formatted according to 3GPP TS 23.003 [14], clause 2.2.
Visited Network Identifier	Visited-Network-Identifier	C	This IE shall contain the identifier that allows the home network to identify the Visited Network. The 3GPP AAA Server shall include this information element when received from signalling across the SWd.
Number Authentication Items	SIP-Number-Auth-Items	M	This information element shall indicate the number of authentication vectors requested
Authentication Data	SIP-Auth-Data-Item	M	See tables 8.1.2.1.1/2 and 8.1.2.1.1/3 for the contents of this information element. The content shown in table 8.1.2.1.1/2 shall be used for a normal authentication request; the content shown in table 8.1.2.1.1/3 shall be used for an authentication request after synchronization failure.
Routing Information	Destination-Host	C	If the 3GPP AAA Server knows the HSS name, this AVP shall be present. This information is available if the 3GPP AAA Server already has the HSS name stored. The HSS name shall be obtained from the Origin-Host AVP, which is received from a previous command from the HSS or from the SLF; otherwise only the Destination-Realm is included so that it is resolved to an HSS address in an SLF-like function. Once resolved the Destination-Host AVP is included with the suitable HSS address and it is stored in the 3GPP AAA Server for further usage.
Access Network Identity	ANID	C	This IE shall contain the access network identifier used for key derivation at the HSS. (See 3GPP TS 24.302 [26] for all possible values). This IE shall be present if the Authentication Method is EAP-AKA".
Access Type	RAT-Type	M	This IE shall contain the radio access technology that is serving the UE. (See 3GPP TS 29.212 [23] for all possible values)
Terminal Information	Terminal-Information	O	This information element shall contain information about the user's mobile equipment. The AVP shall be present only if received from the non-3GPP access GW, in authentication and authorization request. The AVP shall be transparently forwarded by the 3GPP AAA server.
AAA Failure Indication	AAA-Failure-Indication	O	If present, this information element shall indicate that the 3GPP AAA Server currently registered in the HSS, is unavailable.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

**Table 8.1.2.1.1/2: Authentication Data content - request**

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Method	SIP-Authentication-Scheme	M	This information element shall indicate the authentication method It shall contain one of the values EAP-AKA or EAP-AKA'. EAP-AKA' is specified in IETF RFC 5448 [27].

**Table 8.1.2.1.1/3: Authentication Data content - request, synchronization failure**

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Method	SIP-Authentication-Scheme	M	This information element shall indicate the authentication method It shall contain one of the values EAP-AKA or EAP-AKA'.
Authorization Information	SIP-Authorization	M	This IE shall contain the concatenation of Rand, as sent to the terminal, and auts, as received from the terminal. Rand and auts shall both be binary encoded.

Table 8.1.2.1.1/4: Authentication answer

Information element name	Mapping to Diameter AVP	Cat.	Description
IMSI	User-Name (See IETF RFC 3588 [7])	M	This information element shall contain the user IMSI, formatted according to 3GPP TS 23.003 [14], clause 2.2.
Number Authentication Items	SIP-Number-Auth-Items	C	This AVP shall indicate the number of authentication vectors delivered in the Authentication Data information element. It shall be present when the result is DIAMETER_SUCCESS.
Authentication Data	SIP-Auth-Data-Item	C	If the SIP-Number-Auth-Items AVP is equal to zero or it is not present, then this AVP shall not be present. See table 8.1.2.1.1/5 for the contents of this information element.
3GPP AAA Server Name	3GPP-AAA-Server-Name	C	This AVP shall contain the Diameter address of the 3GPP AAA Server. This AVP shall be sent when the user has been previously authenticated by another 3GPP AAA Server and therefore there is another 3GPP AAA Server serving the user.
Result	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for SWx errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

Table 8.1.2.1.1/5: Authentication Data content - response

Information element name	Mapping to Diameter AVP	Cat.	Description
Item Number	SIP-Item-Number	C	This information element shall be present in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVPs, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.
Authentication Method	SIP-Authentication Scheme	M	This IE shall contain one of the values EAP-AKA or EAP-AKA'.
Authentication Information AKA	SIP-Authenticate	M	This IE shall contain, binary encoded, the concatenation of the authentication challenge RAND and the token AUTN. See 3GPP TS 33.203 [16] for further details about RAND and AUTN.
Authorization Information AKA	SIP-Authorization	M	This IE shall contain binary encoded, the expected response XRES. See 3GPP TS 33.203 [16] for further details about XRES.
Confidentiality Key AKA	Confidentiality-Key	M	This information element shall contain the confidentiality key CK or CK'. It shall be binary encoded.
Integrity Key AKA	Integrity-Key	M	This information element shall contain the integrity key IK or IK'. It shall be binary encoded.

### 8.1.2.1.2 Detailed behaviour

The HSS shall, in the following order (if there is an error in any of the steps, the HSS shall stop processing and return the corresponding error code):

1. Check that the user exists in the HSS. If not Experimental-Result-Code shall be set to DIAMETER\_ERROR\_USER\_UNKNOWN.

2. Check that the user has non-3GPP subscription. If not Experimental-Result-Code shall be set to DIAMETER\_ERROR\_USER\_NO\_NON\_3GPP\_SUBSCRIPTON.
3. If a Visited-Network-Identifier is present, check that the user is allowed to roam in the visited network. If the user is not allowed to roam in the visited network, Experimental-Result-Code shall be set to DIAMETER\_ERROR\_ROAMING\_NOT\_ALLOWED.
4. Check RAT-Type AVP. If the access type indicates any value that is restricted for the user, then the Experimental-Result-Code shall be set to DIAMETER\_ERROR\_RAT\_TYPE\_NOT\_ALLOWED.
5. The HSS shall check if there is an existing 3GPP AAA Server already assisting the user
  - If there is a 3GPP AAA Server already serving the user, the HSS shall compare the 3GPP AAA server name received in the request to the 3GPP AAA Server name stored in the HSS.
  - If they are not identical and the received message contains the AAA-Failure-Indication AVP, the HSS shall remove the old 3GPP AAA Server name previously assigned for this subscriber, and store the name of the new 3GPP AAA Server that sent the request containing the AAA-Failure-Indication AVP, and continue from step 6. The HSS should attempt to notify the old 3GPP AAA Server about the new server assignment, by means of the network initiated de-registration procedure (see sub-clause 8.1.2.2.3) indicating as reason code "NEW\_SERVER\_ASSIGNED".
  - If they are not identical the HSS shall return the old 3GPP AAA Server to the requester 3GPP AAA Server and return an error by setting the Experimental-Result-Code to DIAMETER\_ERROR\_IDENTITY\_ALREADY\_REGISTERED.
  - The requester 3GPP AAA Server, upon detection of a 3GPP AAA Server name in the response assumes that the user already has a 3GPP AAA Server assigned, so makes use of Diameter redirect function to indicate the 3GPP AAA Server name where to address the authentication request.
6. The HSS shall check the request type.
  - If the request indicates there is a synchronization failure, the HSS shall process AUTS as described in 3GPP TS 33.203 [16] and return the requested authentication information. The Result-Code shall be set to DIAMETER\_SUCCESS.
    - If the request indicates authentication, the HSS shall generate the authentication vectors for the requested authentication method, EAP-AKA or EAP-AKA', as described in 3GPP TS 33.402 [19]. The HSS shall download Authentication-Data-Item up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The result code shall be set to DIAMETER\_SUCCESS.
  - If there is no 3GPP AAA Server already serving the user, the HSS shall store the received 3GPP AAA Server name.

Exceptions to the cases specified here shall be treated by HSS as error situations, the Result-Code shall be set to DIAMETER\_UNABLE\_TO\_COMPLY. No authentication information shall be returned.

Origin-Host AVP shall contain the 3GPP AAA Server identity.

## 8.1.2.2 Location Management Procedures

### 8.1.2.2.1 General

According to the requirements described in 3GPP TS 23.402 [3], SWx reference point shall enable:

- Registration of the 3GPP AAA Server serving an authorized trusted or untrusted non-3GPP access user in the HSS.
- Retrieval of charging-related information from HSS.
- Deregistration procedure between the 3GPP AAA Server and the HSS.
- Retrieval of subscriber profile from HSS.

## 8.1.2.2.2 UE/PDN Registration/DeRegistration Notification

### 8.1.2.2.2.1 General

This procedure is used between the 3GPP AAA Server and the HSS.

- To register the current 3GPP AAA Server address in the HSS for a given non-3GPP user. This procedure is invoked by the 3GPP AAA Server after a new subscriber has been authenticated by the 3GPP AAA Server.
- To de-register the current 3GPP AAA Server address in the HSS for a given non-3GPP user. When the 3GPP AAA Server is going to remove the access information for a non-3GPP user (i.e. the STa, SWm, S6b sessions are terminated) or when the OCS has initiated a disconnection, the 3GPP AAA Server informs the HSS about an ongoing disconnection process and the HSS de-registers the non-3GPP user.
- To download the subscriber profile to the 3GPP AAA Server on demand. This procedure is invoked when for some reason the subscription profile of a subscriber is lost.
- To update the HSS with the identity and the PLMN ID of a dynamically allocated PDN GW as a result of the first PDN connection establishment associated to an APN.

Table 8.1.2.2.1/1: Non-3GPP IP Access Registration request

Information element name	Mapping to Diameter AVP	Cat.	Description
IMSI	User-Name (See IETF RFC 3588 [7])	M	This information element shall contain the user IMSI and shall be formatted according to 3GPP TS 23.003 [14], clause 2.2.
Server Assignment Type	Server-Assignment-Type	M	This IE shall contain the type of procedure the 3GPP AAA Server requests in the HSS. When this IE contains REGISTRATION value, the HSS shall perform a registration of the non-3GPP user. When this IE contains USER_DEREGISTRATION / ADMINISTRATIVE_DEREGISTRATION / AUTHENTICATION_FAILURE / AUTHENTICATION_TIMEOUT the HSS shall de-register the non-3GPP user. When this IE contains AAA_USER_DATA_REQUEST value, the HSS shall download the subscriber user profile towards the 3GPP AAA Server as part of 3GPP AAA Server initiated profile download request, but no registration shall be performed. When this IE contains PGW_UPDATE value, the HSS shall check if the stored 3GPP AAA server name is the currently registered 3GPP AAA server for this same user and shall update the PGW identity for the non-3GPP user. Any other value shall be considered as an error case.
Routing Information	Destination-Host	C	If the 3GPP AAA Server knows the HSS name this AVP shall be present. This information is available if the 3GPP AAA Server already has the HSS name stored. The HSS name shall be obtained from the Origin-Host AVP, which is received from the HSS as part of authentication response; otherwise only the Destination-Realm is included so that it is resolved to an HSS address in an SLF-like function. Once resolved the Destination-Host AVP shall be included with the suitable HSS address and it shall be stored in the 3GPP AAA Server for further usage.
PGW identity	MIP6-Agent-Info	C	This IE shall contain the identity of the dynamically allocated PDN GW and is included if the Server-Assignment-Type is set to PGW_UPDATE.
PGW PLMN ID	Visited-Network-Identifier	C	This IE contains the identity of the PLMN where the PDN-GW was allocated, in cases of dynamic PDN-GW assignment. It shall be present when the PGW Identity is present and does not contain an FQDN.
Context Identifier	Context-Identifier	O	This parameter shall identify the APN Configuration with which the reallocated PDN GW shall be correlated, and it may be included if it is available and the Server-Assignment-Type is set to PGW_UPDATE.
APN Id	Service-Selection	C	This information element shall contain the Network Identifier part of the APN, and it shall be included if the Server-Assignment-Type is set to PGW_UPDATE.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

Table 8.1.2.2.1/2: Non-3GPP IP Access Registration response

Information element name	Mapping to Diameter AVP	Cat.	Description
IMSI	User-Name (See IETF RFC 3588 [7])	M	This information element shall contain the user IMSI and shall be formatted according to 3GPP TS 23.003 [14], clause 2.2.
Registration result	Result-Code / Experimental-Result	M	This IE contains the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for SWx errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
User Profile	Non-3GPP-User-Data	C	This IE shall contain the relevant user profile. Section 8.2.3.1 details the contents of the AVP. It shall be present when Server-Assignment-Type in the request is equal to AAA_USER_DATA_REQUEST or REGISTRATION and the Result-Code is equal to DIAMETER_SUCCESS.
3GPP AAA Server Name	3GPP-AAA-Server-Name	C	This AVP shall contain the Diameter address of the 3GPP AAA Server. This AVP shall be present when the user has been previously authenticated by another 3GPP AAA Server and therefore there is another 3GPP AAA Server serving the user.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

#### 8.1.2.2.2 Detailed behaviour

When a new trusted or untrusted non-3GPP IP access subscriber has been authenticated by the 3GPP AAA Server, the 3GPP AAA Server initiates the registration towards the HSS. The HSS shall, in the event of an error in any of the steps, stop processing and return the corresponding error code.

At reception of the Non-3GPP IP Access Registration, the HSS shall perform (in the following order):

1. Check that the user is known. If not Experimental-Result-Code shall be set to DIAMETER\_ERROR\_USER\_UNKNOWN.
2. The HSS shall check if there is an existing 3GPP AAA Server already assisting the user
  - If there is a 3GPP AAA Server already serving the user, the HSS shall compare the 3GPP AAA Server name received in the request to the 3GPP AAA Server name stored in the HSS.
  - If they are not identical the HSS shall return the old 3GPP AAA Server to the requester 3GPP AAA Server and return an error by setting the Experimental-Result-Code to DIAMETER\_ERROR\_IDENTITY\_ALREADY\_REGISTERED.

The requester 3GPP AAA Server, upon detection of a 3GPP AAA Server name in the response assumes that the user already has a 3GPP AAA Server assigned, so makes use of Diameter redirect function to indicate the 3GPP AAA Server name where to address the Non-3GPP IP Access Registration request.

- If they are identical but there is no APN configuration information in HSS for the user, the HSS shall return the Experimental Result Code DIAMETER\_ERROR\_USER\_NO\_NON\_3GPP\_SUBSCRIPTION and it shall remove the 3GPP AAA Server name previously assigned for this subscriber.
- If there is not a 3GPP AAA Server already serving the user, the HSS shall return an error, setting the Result-Code to DIAMETER\_UNABLE\_TO\_COMPLY in the Response command.

3. After the HSS has determined that the requesting 3GPP AAA server is identical to the registered 3GPP AAA server, the HSS shall check the Server Assignment Type value received in the request:
- If it indicates REGISTRATION, the HSS shall set the subscribers User Status to REGISTERED for the authenticated and authorized trusted or untrusted non-3GPP IP access subscriber, download the relevant user profile information and set the Result-Code AVP to DIAMETER\_SUCCESS in the Server-Assignment-Response command. For those APNs that have been authorized as a consequence of having the Wildcard APN in the user subscription, the HSS shall include the specific APN name and associated PDN-GW identity inside the APN context of the Wildcard APN.
  - If it indicates USER\_DEREGISTRATION / ADMINISTRATIVE\_DEREGISTRATION / AUTHENTICATION\_FAILURE / AUTHENTICATION\_TIMEOUT, the HSS shall remove the 3GPP AAA Server name previously assigned for the subscriber, set the User Status for the subscriber to NOT\_REGISTERED and set the Result-Code AVP to DIAMETER\_SUCCESS in the Server-Assignment-Response command. The HSS shall not remove the stored dynamic PGW-ID and APN information for the subscriber.
  - If it indicates AAA\_USER\_DATA\_REQUEST, the HSS shall download the relevant user profile information to the requester 3GPP AAA Server and set the Result-Code AVP to DIAMETER\_SUCCESS in the Response command.
  - If it indicates PGW\_UPDATE, the HSS shall check if the subscriber is registered.  
 If the subscriber is registered and there is not a static PDN GW subscribed, the HSS shall store the PGW identity and PLMN (if it is received in the command) for the non-3GPP user and the APN identified by the APN Id or by the Context Identifier if present in the request; otherwise, the HSS shall not update or delete the stored PDN GW and, for this case, shall set the result code to DIAMETER\_UNABLE\_TO\_COMPLY.  
 If the APN corresponding to the PGW identity is not present in the subscription but the wild card APN is present in the subscription, the HSS shall store the new PDN GW identity and PLMN for an APN if present in the request. The HSS shall set the Result-Code AVP to DIAMETER\_SUCCESS in the Server-Assignment-Response command. If the Context Identifier is included in the request, the HSS may use it to locate the APN Configuration.  
 If the APN corresponding to the PGW identity is not present in the subscription and the wild card APN is not present in the subscription, the HSS shall reject the request and set the Result-Code AVP to DIAMETER\_UNABLE\_TO\_COMPLY.  
 If the subscriber is not registered, the HSS shall reject the request and set the Experimental-Result-Code AVP to DIAMETER\_ERROR\_IDENTITY\_NOT\_REGISTERED.
  - If it indicates any other value, the Result-Code shall be set to DIAMETER\_UNABLE\_TO\_COMPLY, and no registration/de-registration or profile download procedure shall be performed.

Origin-Host AVP shall contain the 3GPP AAA Server identity.

Once the 3GPP AAA Server has received the user profile data as a result of successful registration to the HSS, the 3GPP AAA Server shall create appropriate routing policies and IP filtering information according to the retrieved operator defined barring information. These routing policies and IP filtering information are used for the subsequent authorizations by the MAG functionality in the trusted 3GPP/IP access, or ePDG or PGW. If the subscription data received for a certain APN indicates that the APN was authorized as a consequence of having the Wildcard APN in the user subscription in HSS, then the 3GPP AAA Server shall not store this APN data beyond the lifetime of the UE sessions related to the specific APN and the 3GPP AAA Server shall delete them upon disconnection of the UE. If the PGW Identity contains an FQDN of the PDN GW, the 3GPP AAA Server shall retrieve the PGW PLMN ID from the MIP-Home-Agent-Host AVP within the MIP6-Agent-Info AVP which contains the PGW Identity.

The 3GPP AAA Server may be configured by local policy to not update the HSS with the PGW Identity used over TWAN for the default APN of the user (i.e. to skip the Non-3GPP IP Access Registration request with Server-Assignment-Type set to "PGW\_UPDATE").

**NOTE:** This 3GPP AAA Server option can be used when the same APN is configured for TWAN and other access technologies in which case the network can select different PDN GWs for PDN connections to this APN. Updating the HSS with the selected PDN GW identity for Trusted WLAN access could affect PDN connections over other access technologies.

## 8.1.2.2.3 Network Initiated De-Registration by HSS, Administrative

## 8.1.2.2.3.1 General

This procedure is used between the 3GPP AAA Server and the 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 appropriate interface.

**Table 8.3.2.3: Network Initiated Deregistration by HSS request**

Information element name	Mapping to Diameter AVP	Cat.	Description
IMSI	User-Name (See IETF RFC 3588 [7])	M	This information element shall contain the user IMSI and shall be formatted according to 3GPP TS 23.003 [14], clause 2.2.
Reason for de-registration	Deregistration-Reason	M	This IE shall contain the reason for the de-registration as the HSS shall send to the 3GPP AAA server a reason for the de-registration. The de-registration reason shall be composed of two parts: one textual message (if available) that is intended to be forwarded to the user that is de-registered, and one reason code (see 3GPP TS 29.229 [24]) that determines the behaviour of the 3GPP AAA Server.
Routing Information	Destination-Host	M	This IE shall contain the 3GPP AAA server name that is obtained from the Origin-Host AVP, which is received from the 3GPP AAA Server,
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

**Table 8.3.2.4: Network Initiated Deregistration by HSS response**

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	This IE shall contain the Result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for SWx errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

### 8.1.2.2.3.2 Detailed behaviour

The HSS shall de-register the affected identity and invoke this procedure to inform the 3GPP AAA server to remove the subscribed user from the 3GPP AAA Server.

The HSS shall send in the Deregistration-Reason AVP the reason for the de-registration, composed by a textual message (if available) aimed for the user and a reason code that determines the action the 3GPP AAA server has to perform. The possible reason codes are:

- **PERMANENT\_TERMINATION**: The non-3gpp subscription or service profile(s) has been permanently terminated. The HSS shall clear the user's 3GPP AAA Server name and set the User Status to **NOT\_REGISTERED**. The 3GPP AAA Server should start the network initiated de-registration towards the user.
- **NEW\_SERVER\_ASSIGNED**: The HSS indicates to the 3GPP AAA Server that a new 3GPP AAA Server has been allocated to the user (e.g. because the previous assigned 3GPP AAA Server was found unavailable at a certain point). The 3GPP AAA Server shall remove all user data and session information for the user indicated in the de-registration request. The 3GPP AAA Server shall not start the network initiated de-registration towards the user.

## 8.1.2.3 HSS Initiated Update of User Profile

### 8.1.2.3.1 General

According to the requirements described in 3GPP TS 23.402 [3] and 3GPP TS 32.422 [32], SWx reference point shall enable:

- Indication to 3GPP AAA Server of change of non-3GPP subscriber profile within HSS;
- Activation and deactivation of the subscriber and equipment trace in the PDN GW.

This procedure is used between the 3GPP AAA Server and the HSS. The procedure is invoked by the HSS when the subscriber profile has been modified and needs to be sent to the 3GPP AAA Server. This may happen due to a modification in the HSS.

The procedure is also invoked by the HSS to update the 3GPP AAA Server with the identity of a dynamically allocated PDN GW which is included in the APN-Configuration AVP in the User Profile as a result of the first PDN connection establishment associated with an APN over 3GPP access.

This procedure is mapped to the Diameter command codes Push-Profile-Request (PPR) and Push-Profile-Answer (PPA) specified in the 3GPP TS 29.229 [24]. Information element contents for these messages are shown in tables 8.1.2.3.1/1 and 8.1.2.3.1/2.

**Table 8.1.2.3.1/1: User Profile Update request**

Information element name	Mapping to Diameter AVP	Cat.	Description
IMSI	User-Name (See IETF RFC 3588 [7])	M	This information element shall contain the user IMSI and shall be formatted according to 3GPP TS 23.003 [14], clause 2.2.
User profile	Non-3GPP-User-Data	M	This IE shall contain the updated user profile. Section 8.2.3.1 details the contents of the AVP. In case of trace activation or deactivation, the Trace-Info AVP shall be included, and this may be the only AVP that is present under this grouped AVP.
Routing Information	Destination-Host	M	This IE shall contain the 3GPP AAA Server name that is obtained from the Origin-Host AVP, which is received from the 3GPP AAA Server
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

**Table 8.1.2.3.1/2: User Profile Update response**

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for SWx errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

### 8.1.2.3.2 HSS Detailed behaviour

The HSS shall make use of this procedure to update the relevant user profile in the 3GPP AAA server (e.g. change of subscription data or change of the identity of a dynamically allocated PDN GW associated with an APN), or activate / deactivate subscriber and equipment trace in the PDN GW.

### 8.1.2.3.3 3GPP AAA Server Detailed behaviour

The 3GPP AAA server shall overwrite, for the subscriber identity indicated in the request, current information with the information received from the HSS, except in the error situations detailed in table 8.1.2.3.3/1.

After a successful user profile download, the 3GPP AAA server shall initiate re-authentication procedure as described in sub-clause 7.2.2.4 if the subscriber has previously been authenticated and authorized to untrusted non-3GPP access. If the subscriber has previously been authenticated and authorized to trusted Non-3GPP IP Access then the 3GPP AAA server shall initiate a re-authorization procedure as described in sub-clause 5.1.2.3.

Following a successful user profile download, the 3GPP AAA server shall apply routing policies and IP filtering information as described in clause 8.1.2.2.2. . As multiple authorization sessions may exist for the user (see section 7.1.2.1), the 3GPP AAA server shall examine the need to execute re-authorization for each of these sessions, and may execute the multiple re-authorization procedures in parallel. In case the user's non-3GPP subscription has been deleted or the user's APN has been barred, the re-authorization shall be executed in all ongoing user related authorization sessions. Otherwise, the re-authorization procedure shall be invoked for the authorization sessions for which at least one of the following conditions is fulfilled:

- The user's subscribed APN has been deleted from the HSS.
- The APN configuration data has been previously downloaded to the ePDG and the new version of APN configuration received from HSS reflects a modification in these data.

Following a successful download of subscription and equipment trace data, the 3GPP AAA Server shall forward the trace data by initiating reauthorization towards all PDN GWs that have an active authorization session.

Table 8.1.2.3.3/1 details the valid result codes that the 3GPP AAA server can return in the response.

**Table 8.1.2.3.3/1: User profile response valid result codes**

Result-Code AVP value	Condition
DIAMETER_SUCCESS	The request succeeded.
DIAMETER_ERROR_USER_UNKNOWN	The request failed because the user is not found in 3GPP AAA Server.
DIAMETER_UNABLE_TO_COMPLY	The request failed.

## 8.1.2.4 Fault Recovery Procedures

### 8.1.2.4.1 HSS Reset Indication

#### 8.1.2.4.1.1 General

This procedure is used by the HSS to indicate to the 3GPP AAA Server that it has restarted, and the registration data and the dynamic data stored for a set of users may have been lost.

This procedure is mapped to the Diameter command codes Push-Profile-Request (PPR) and Push-Profile-Answer (PPA) specified in the 3GPP TS 29.229 [24]. Information Element contents for these messages are shown in tables 8.1.2.4.1.1/1 and 8.1.2.4.1.1/2.

**Table 8.1.2.4.1.1/1: HSS Reset Indication Request**

Information element name	Mapping to Diameter AVP	Cat.	Description
User List	User-Name (See IETF RFC 3588 [7])	M	This information element shall indicate the users affected by the HSS restart. It shall contain either: - The string "*", if all users are affected by the restart - The leading digits of the IMSI series of the set of users affected by the restart.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
PPR Flags	PPR-Flags	M	This Information Element contains a bit mask. See 8.2.3.17 for the meaning of the bits. The HSS shall set the Reset-Indication bit when sending PPR to the 3GPP AAA Server.

**Table 8.1.2.4.1.1/2: HSS Reset Indication Response**

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for SWx errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

#### 8.1.2.4.1.2 HSS Detailed behaviour

The HSS shall use this procedure to indicate to the 3GPP AAA Server about a restart event, affecting a set of users, for whom their registration data and dynamic data may have been lost. The HSS shall only send this command if the 3GPP AAA Server has indicated support for the "HSS Restoration" feature. In this case, the HSS shall set the Reset-Indication bit in the PPR-Flags AVP in the PPR command.

**NOTE:** If there are multiple 3GPP AAA Servers deployed in the HPLMN, and the HSS is configured (in an implementation-specific manner) in such a way that it can determine that a certain 3GPP AAA Server does not contain any of the users affected by the restart, it can skip sending the PPR command to that specific 3GPP AAA Server.

### 8.1.2.4.1.3 3GPP AAA Server Detailed behaviour

If the 3GPP AAA Server supports the "HSS Restoration" feature, it shall answer with a successful result to the PPR command, and it shall mark those users affected by the HSS restart as "pending to be restored in HSS".

The 3GPP AAA Server shall use the HSS Identity received in the Origin-Host AVP (by comparing it with the value stored after a successful MAA command) and may make use of the received "User List" Information Element in order to determine which subscriber records are impacted, if any. If the 3GPP AAA Server determines that there are no subscribers affected by the HSS restart, it shall answer with a successful result to the HSS.

### 8.1.2.4.2 HSS Restoration

#### 8.1.2.4.2.1 General

This procedure is used by the 3GPP AAA Server to restore in the HSS the registration data and the dynamic data for a certain user. The 3GPP AAA Server shall use this procedure only after having received a previous indication from HSS of a restart event affecting that user.

This procedure is mapped to the Diameter command codes Server-Assignment-Request (SAR) and Server-Assignment-Answer (SAA) specified in the 3GPP TS 29.229 [24]. Information element contents for these messages are shown in tables 8.1.2.4.2.1/1 and 8.1.2.4.2.1/2.

**Table 8.1.2.4.2.1/1: HSS Restoration Request**

Information element name	Mapping to Diameter AVP	Cat.	Description
IMSI	User-Name (See IETF RFC 3588 [7])	M	This information element shall contain the IMSI of the user, for whom the registration data and dynamic data is being restored in HSS, and it shall be formatted according to 3GPP TS 23.003 [14], clause 2.2.
Server Assignment Type	Server-Assignment-Type	M	This IE shall contain the value "RESTORATION".
Active APN	Active-APN	C	This Information Element, if present, contains the list of active APNs stored by the 3GPP AAA Server for this user, including the identity of the PDN GW assigned to each APN. For the explicitly subscribed APNs, the following information shall be present:  <ul style="list-style-type: none"> <li>- Context-Identifier: context id of subscribed APN in use</li> <li>- Service-Selection: name of subscribed APN in use</li> <li>- MIP6-Agent-Info: including PDN GW identity in use for subscribed APN</li> <li>- Visited-Network-Identifier: identifies the PLMN where the PDN GW was allocated</li> </ul> For the Wildcard APN, the following information shall be present:  <ul style="list-style-type: none"> <li>- Context-Identifier: context id of the Wildcard APN</li> <li>- Specific-APN-Info: list of APN-in use and related PDN GW identity when the subscribed APN is the wildcard APN</li> </ul>
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

Table 8.1.2.4.2.1/2: HSS Restoration Response

Information element name	Mapping to Diameter AVP	Cat.	Description
IMSI	User-Name (See IETF RFC 3588 [7])	M	This information element shall contain the user IMSI and shall be formatted according to 3GPP TS 23.003 [14], clause 2.2.
Registration result	Result-Code / Experimental-Result	M	This IE contains the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for SWx errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

### 8.1.2.4.2.2 HSS Detailed behaviour

Upon receipt of the SAR command, if the HSS supports the "HSS Restoration" feature, and the user's IMSI is known, the HSS shall update the registration data (from the Origin-Host AVP received in the 3GPP AAA Server command) and dynamic data of the user (included in the "Active APN" Information Element), and answer with a successful result.

### 8.1.2.4.2.3 3GPP AAA Server Detailed behaviour

The 3GPP AAA Server shall use this command to update the HSS with the registration data and dynamic data it has for a user affected by the HSS restart, identified by the "User List" IE received previously in the PPR command, and marked in the 3GPP AAA Server as "pending to be restored in HSS". The 3GPP AAA Server shall only make use of this procedure in the HSS has indicated support for the "HSS Restoration" feature.

The 3GPP AAA Server shall invoke the SAR command towards the HSS, after having received further interactions over other reference points (S6b, STa, SWm ...) for a user marked as "pending to be restored in HSS".

Once the 3GPP AAA Server receives confirmation from HSS, in the SAA command, that the user has been successfully restored in the HSS, via the "HSS Restoration Response" command, it shall clear the "pending to be restored in HSS" flag for that user.

## 8.2 Protocol Specification

### 8.2.1 General

The SWx reference point shall be Diameter based. This is defined as an IETF vendor specific Diameter application, where the Vendor ID is 3GPP. The Application Id used shall be 16777265.

### 8.2.2 Commands

#### 8.2.2.1 Authentication Procedure

The Multimedia-Authentication-Request (MAR) command, indicated by the Command-Code field set to 303 and the 'R' bit set in the Command Flags field, is sent by the 3GPP AAA Server to the HSS in order to request security information. This corresponds to section 8.1.2.1.

Message Format

```

< Multimedia-Auth-Request > ::= < Diameter Header: 303, REQ, PXY, 16777265 >
                                < Session-Id >
                                { Vendor-Specific-Application-Id }
                                { Auth-Session-State }
                                { Origin-Host }

```

```

{ Origin-Realm }
{ Destination-Realm }
[ Destination-Host ]
{ User-Name }
[ RAT-Type ]
[ ANID ]
[ Visited-Network-Identifier]
[ Terminal-Information ]
{ SIP-Auth-Data-Item }
{ SIP-Number-Auth-Items }
[AAA-Failure-Indication ]
*[ Supported-Features ]
...
*[ AVP ]

```

The Multimedia-Authentication-Answer (MAA) command, indicated by the Command-Code field set to 303 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Multimedia-Authentication-Request command. The Result-Code or Experimental-Result AVP may contain one of the values defined in section 6.2 of 3GPP TS 29.229 [24] in addition to the values defined in RFC 3588 [7].

#### Message Format

```

< Multimedia-Auth-Answer > ::= < Diameter Header: 303, PXY, 16777265 >
< Session-Id >
{ Vendor-Specific-Application-Id }
[ Result-Code ]
[ Experimental-Result ]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ User-Name }
[ SIP-Number-Auth-Items ]
*[ SIP-Auth-Data-Item ]
[ 3GPP-AAA-Server-Name ]
*[ Supported-Features ]
...
*[ AVP ]

```

### 8.2.2.2 HSS Initiated Update of User Profile Procedure

The Push-Profile-Request (PPR) command, indicated by the Command-Code field set to 305 and the 'R' bit set in the Command Flags field, is sent by the HSS to the 3GPP AAA Server in order to update the subscription data whenever a modification has occurred in the subscription data; this corresponds to section 8.1.2.3. This command is also sent by HSS to indicate a restart event to the 3GPP AAA Server, so the registration data and the dynamic data previously stored in HSS can be restored; this corresponds to section 8.1.2.4.1.

#### Message Format

```

< Push-Profile-Request > ::= < Diameter Header: 305, REQ, 16777265 >
< Session-Id >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
{ User-Name }
[ Non-3GPP-User-Data ]
[ PPR-Flags ]
*[ Supported-Features ]
...
*[ AVP ]

```

The Push-Profile-Answer (PPA) command, indicated by the Command-Code field set to 305 and the 'R' bit cleared in the Command Flags field, is sent by the HSS in response to the Push-Profile-Request command. The Result-Code or Experimental-Result AVP may contain one of the values defined in section 6.2 of 3GPP TS 29.229 [24] in addition to the values defined in RFC 3588 [7].

#### Message Format

```
< Push-Profile-Answer > ::= < Diameter Header: 305, PXY, 16777265 >
< Session-Id >
{ Vendor-Specific-Application-Id }
[ Result-Code ]
[ Experimental-Result ]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
*[ Supported-Features ]
...
*[ AVP ]
```

### 8.2.2.3 Non-3GPP IP Access Registration Procedure

The Server-Assignment-Request (SAR) command, indicated by the Command-Code field set to 301 and the 'R' bit set in the Command Flags field, is sent by the 3GPP AAA Server to the HSS; this corresponds to section 8.1.2.2.2. This command is also sent by the 3GPP AAA Server to restore the registration data and the dynamic data previously stored in HSS, which may have been lost after a restart; this corresponds to section 8.1.2.4.2.

#### Message Format

```
< Server-Assignment-Request > ::= < Diameter Header: 301, REQ, PXY, 16777265 >
< Session-Id >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[ Destination-Host ]
{ Destination-Realm }
[ Service-Selection ]
[ Context-Identifier ]
[ MIP6-Agent-Info ]
[ Visited-Network-Identifier ]
{ User-Name }
{ Server-Assignment-Type }
*[ Active-APN ]
*[ Supported-Features ]
...
*[ AVP ]
```

The Server-Assignment-Answer (SAA) command, indicated by the Command-Code field set to 301 and the 'R' bit cleared in the Command Flags field, is sent by the HSS to the 3GPP AAA Server to confirm the registration, de-registration, user profile download or restoration procedure. The Result-Code or Experimental-Result AVP may contain one of the values defined in section 6.2 of 3GPP TS 29.229 [24] in addition to the values defined in RFC 3588 [7].

#### Message Format

```
< Server-Assignment-Answer > ::= < Diameter Header: 301, PXY, 16777265 >
< Session-Id >
{ Vendor-Specific-Application-Id }
[ Result-Code ]
[ Experimental-Result ]
{ Auth-Session-State }
{ Origin-Host }
```

```

{ Origin-Realm }
{ User-Name }
[ Non-3GPP-User-Data ]
[ 3GPP-AAA-Server-Name ]
*[ Supported-Features ]
...
*[ AVP ]

```

### 8.2.2.4 Network Initiated De-Registration by HSS Procedure

The Registration-Termination-Request (RTR) command, indicated by the Command-Code field set to 304 and the "R" bit set in the Command Flags field, is sent by a Diameter Multimedia server to a Diameter Multimedia client in order to request the de-registration of a user. This corresponds to section 8.1.2.2.3.

#### Message Format

```

<Registration-Termination-Request> ::=
  < Diameter Header: 304, REQ, PXY, 16777265 >
  < Session-Id >
  { Vendor-Specific-Application-Id }
  { Auth-Session-State }
  { Origin-Host }
  { Origin-Realm }
  { Destination-Host }
  { Destination-Realm }
  { User-Name }
  { Deregistration-Reason }
  *[ Supported-Features ]
  ...
  *[ AVP ]

```

The Registration-Termination-Answer (RTA) command, indicated by the Command-Code field set to 304 and the "R" bit cleared in the Command Flags field, is sent by a client in response to the Registration-Termination-Request command. The Result-Code or Experimental-Result AVP may contain one of the values defined in section 6.2 of 3GPP TS 29.229 [24] in addition to the values defined in RFC 3588 [7].

#### Message Format

```

<Registration-Termination-Answer> ::=
  < Diameter Header: 304, PXY, 16777265 >
  < Session-Id >
  { Vendor-Specific-Application-Id }
  [ Result-Code ]
  [ Experimental-Result ]
  { Auth-Session-State }
  { Origin-Host }
  { Origin-Realm }
  *[ Supported-Features ]
  ...
  *[ AVP ]

```

## 8.2.3 Information Elements

### 8.2.3.0 General

The following table describes the Diameter AVPs defined for the SWx interface protocol, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted.

**Table 8.2.3.0/1: Diameter SWx AVPs**

AVP Flag rules
----------------

Attribute Name	AVP Code	Section defined	Value Type	Must	May	Should not	Must not
Non-3GPP-User-Data	1500	8.2.3.1	Grouped	M,V			P
Non-3GPP-IP-Access	1501	8.2.3.3	Enumerated	M,V			P
Non-3GPP-IP-Access-APN	1502	8.2.3.4	Enumerated	M,V			P
ANID	1504	5.2.3.7	UTF8String	M,V			P
Trace-Info	1505	8.2.3.13	Grouped	V			M,P
PPR-Flags	1508	8.2.3.17	Unsigned32	V			M,P
TWAN-Default-APN-Context-Id	1512	8.2.3.18	Unsigned32	V			M,P
TWAN-Access-Info	1510	8.2.3.19	Grouped	V			M,P
Access-Authorization-Flags	1511	8.2.3.20	Unsigned32	V			M,P
WLAN-Identifier	1509	5.2.3.18	Grouped	V			M,P
Service-Selection	493	5.2.3.5	UTF8String	M			V,P
AAA-Failure-Indication	1518	8.2.3.21	Unsigned32	V			M,P

The following table describes the Diameter AVPs re-used by the SWx interface protocol from existing Diameter Applications, including a reference to their respective specifications and when needed, a short description of their use within SWx. Other AVPs from existing Diameter Applications, except for the AVPs from Diameter Base Protocol, do not need to be supported.

**Table 8.2.3.0/2: SWx re-used Diameter AVPs**

Attribute Name	Reference	Comments
User-Name	IETF RFC 3588 [7]	
Session-Timeout	IETF RFC 3588 [7]	
Subscription-ID	IETF RFC 4006 [20]	
MIP6-Agent-Info	IETF RFC 5447 [6]	
MIP6-Feature-Vector	IETF RFC 5447 [6]	
Service-Selection	IETF RFC 5778 [11]	
3GPP-Charging-Characteristics	3GPP TS 29.061 [31]	
RAT-Type	3GPP TS 29.212 [23]	
Visited-Network-Identifier	3GPP TS 29.229 [24]	
SIP-Number-Auth-Items	3GPP TS 29.229 [24]	
SIP-Item-Number	3GPP TS 29.229 [24]	
SIP-Auth-Data-Item	3GPP TS 29.229 [24]	
SIP-Authentication-Scheme	3GPP TS 29.229 [24]	
SIP-Authenticate	3GPP TS 29.229 [24]	
SIP-Authorization	3GPP TS 29.229 [24]	
Confidentiality-Key	3GPP TS 29.229 [24]	
Integrity-Key	3GPP TS 29.229 [24]	
Server-Assignment-Type	3GPP TS 29.229 [24]	
Deregistration-Reason	3GPP TS 29.229 [24]	
Supported-Features	3GPP TS 29.229 [24]	
Feature-List-ID	3GPP TS 29.229 [24]	
Feature-List	3GPP TS 29.229 [24]	
APN-Configuration	3GPP TS 29.272 [29]	
Context-Identifier	3GPP TS 29.272 [29]	
Terminal-Information	3GPP TS 29.272 [29]	
AMBR	3GPP TS 29.272 [29]	
APN-OI-Replacement	3GPP TS 29.272 [29]	
Trace-Reference	3GPP TS 29.272 [29]	
Trace-Data	3GPP TS 29.272 [29]	
Active-APN	3GPP TS 29.272 [29]	
3GPP-AAA-Server-Name	3GPP TS 29.234 [33]	

Only those AVP initially defined in this reference point or AVP with values initially defined in this reference point and for this procedure are described in the following subchapters.

### 8.2.3.1 Non-3GPP-User-Data

The Non-3GPP-User-Data AVP is of type Grouped. It contains the information related to the user profile relevant for EPS.

AVP format:

```

Non-3GPP-User-Data ::=      < AVP Header: 1500 10415 >
                             [ Subscription-ID ]
                             [ Non-3GPP-IP-Access ]
                             [ Non-3GPP-IP-Access-APN ]
                             *[ RAT-Type ]
                             [ Session-Timeout ]
                             [ MIP6-Feature-Vector ]
                             [ AMBR ]
                             [ 3GPP-Charging-Characteristics ]
                             [ Context-Identifier ]
                             [ APN-OI-Replacement ]
                             *[ APN-Configuration ]
                             [ Trace-Info ]
                             [ TWAN-Default-APN-Context-Id ]
                             *[ TWAN-Access-Info]
                             *[ AVP ]

```

The AMBR included in this grouped AVP shall include the AMBR associated to the user's subscription (UE-AMBR).

The APN-OI-Replacement included in this grouped AVP shall include the UE level APN-OI-Replacement associated to the user's subscription. This APN-OI-Replacement has lower priority than APN level APN-OI-Replacement that is included in the APN-Configuration AVP. The Non-3GPP-IP-Access AVP, the Non-3GPP-IP-Access-APN AVP, the Context-Identifier AVP and at least one item of the APN-Configuration AVP shall always be included, except when the Non-3GPP-User-Data AVP is used for downloading trace activation or deactivation information on the SWx interface, for an already registered user. In that specific case, the Trace-Info AVP shall be included and the presence of any further AVPs is optional.

The Context-Identifier in this grouped AVP shall identify the user's default APN configuration. The TWAN-Default-APN-Context-Id AVP identifies the default APN configuration for EPC access over Trusted WLAN. This AVP shall be present if the default APN configuration for EPC access over Trusted WLAN differs from the default APN configuration for 3GPP access and other non-3GPP accesses. This AVP may be present otherwise.

### 8.2.3.2 Subscription-ID

The Subscription-ID AVP is of type Grouped and indicates the user identity to be used for charging purposes. It is defined in the IETF RFC 4006 [20]. EPC shall make use only of the IMSI and MSISDN values. This grouped AVP shall set the sub-AVP Subscription-Id-Type to value "END\_USER\_E164" and shall set the sub-AVP Subscription-Id-Data to the MSISDN value.

AVP format:

```

Subscription-Id ::=          < AVP Header: 443 >
                             [ Subscription-Id-Type ]
                             [Subscription-Id-Data ]

```

### 8.2.3.3 Non-3GPP-IP-Access

The Non-3GPP-IP-Access AVP (AVP code 1501) is of type Enumerated, and allows operators to determine if the subscriber is barred from using the non-3GPP access network. The following values are defined:

NON\_3GPP\_SUBSCRIPTION\_ALLOWED (0)

The subscriber has non-3GPP subscription and is authorized to use the non-3GPP access network.

NON\_3GPP\_SUBSCRIPTION\_BARRED (1)

The subscriber is barred from using the non-3GPP access network.

#### 8.2.3.4 Non-3GPP-IP-Access-APN

The Non-3GPP-IP-Access-APN AVP (AVP code 1502) is of type Enumerated, and allows operator to disable all APNs for a subscriber at one time. The following values are defined:

Non\_3GPP\_APNS\_ENABLE (0)

Enable all APNs for a subscriber.

Non\_3GPP\_APNS\_DISABLE (1)

Disable all APNs for a subscriber

#### 8.2.3.5 RAT-Type

This AVP is defined in chapter 5.2.3.6 and it shall include the access technology types not allowed for the user.

#### 8.2.3.6 Session-Timeout

The Session-Timeout AVP is of type Unsigned32. It is defined in IETF RFC 3588 [7] and indicates the maximum period for a session measured in seconds. This AVP is used for re-authentication purposes. If this field is not used, the non-3GPP Access Node will apply default time intervals.

#### 8.2.3.7 APN-Configuration

The APN-Configuration AVP is of type Grouped AVP and is defined in 3GPP TS 29.272 [29].

#### 8.2.3.8 ANID

The ANID AVP is defined in chapter 5.2.3.7.

#### 8.2.3.9 SIP-Auth-Data-Item

The SIP-Auth-Data-Item AVP is defined in 3GPP TS 29.229 [24]. The optional AVPs that are needed in SWx reference point are included in the ABNF representation below.

AVP format:

```
SIP-Auth-Data-Item ::= < AVP Header: 612 10415 >
[ SIP-Item-Number ]
[ SIP-Authentication-Scheme ]
[ SIP-Authenticate ]
[ SIP-Authorization ]
[ Confidentiality-Key ]
[ Integrity-Key ]
*[ AVP ]
```

#### 8.2.3.10 Confidentiality-Key

The Confidentiality-Key AVP is defined in 3GPP TS 29.229 [24]. It is of type OctetString, and contains the Confidentiality Key (CK') or, after key derivation using the Access Network Identifier, the Confidentiality Key (CK"). For the 3GPP AAA server it is transparent whether the value received corresponds to CK or CK".

#### 8.2.3.11 Integrity-Key

The Integrity-Key AVP is defined in 3GPP TS 29.229 [24]. It is of type OctetString, and contains the Integrity Key (IK) or, after key derivation using the Access Network Identifier, the Integrity Key (IK"). For the 3GPP AAA server it is transparent whether the value received corresponds to IK or IK".

### 8.2.3.12 Server-Assignment-Type AVP

The Server-Assignment-Type AVP is defined in 3GPP TS 29.229 [24] and it is of type Enumerated, and indicates the type of server update being performed in a Server-Assignment-Request operation. As part of the SWx protocol specification, the following values are additionally defined:

#### AAA\_USER\_DATA\_REQUEST (12)

This value is used to request the non-3GPP user profile data from the 3GPP AAA Server to the HSS.

#### PGW\_UPDATE (13)

This value is used to store, update or delete the PDN-GW Identity in the HSS, as requested from the 3GPP AAA Server.

#### RESTORATION (14)

This value is used to store in the HSS registration data and dynamic data that may have been potentially lost after a restart event.

### 8.2.3.13 Trace-Info

The Trace-Info AVP is of type Grouped. This AVP shall contain the information related to subscriber and equipment trace function and the required action, i.e. activation of deactivation

AVP format

Trace-Info ::= < AVP header: 1505 10415>

[Trace-Data]

[Trace-Reference]

\*[AVP]

Either the Trace-Data or the Trace-Reference AVP shall be included. When trace activation is needed, Trace-Data AVP shall be included, while the trace deactivation request shall be signalled by including the Trace-Reference directly under the Trace-Info. The Trace-Reference AVP is of type OctetString. The Diameter AVP is defined in 3GPP TS 29.272 [29].

### 8.2.3.14 Trace-Data

The Trace-Data AVP is of type Grouped. The Diameter AVP is defined in 3GPP TS 29.272 [29].

### 8.2.3.15 Feature-List-ID AVP

The syntax of this AVP is defined in 3GPP TS 29.229 [24]. For this release, the Feature-List-ID AVP value shall be set to 1 for the SWx application.

### 8.2.3.16 Feature-List AVP

The syntax of this AVP is defined in 3GPP TS 29.229 [24]. A null value indicates that there is no feature used by the SWx application. The meaning of the bits shall be as defined in table 8.2.3.16/1.

**Table 8.2.3.16/1: Features of Feature-List-ID 1 used in SWx**

Feature bit	Feature	M/O	Description
0	HSS Restoration	O	HSS Restoration  This feature is applicable for the MAR/MAA, PPR/PPA and SAR/SAA command pairs. If the 3GPP AAA Server does not indicate support for this feature in a former MAR or SAR command, the HSS shall not send a PPR command to indicate a restart event to the 3GPP AAA Server.
Feature bit: The order number of the bit within the Supported-Features AVP, e.g. "1". Feature: A short name that can be used to refer to the bit and to the feature. M/O: Defines if the implementation of the feature is mandatory ("M") or optional ("O"). Description: A clear textual description of the feature.			

Features that are not indicated in the Supported-Features AVPs within a given application message shall not be used to construct that message.

### 8.2.3.17 PPR-Flags

The PPR-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 8.2.3.17/1:

**Table 8.2.3.17/1: PPR-Flags**

Bit	Name	Description
0	Reset-Indication	This bit, when set, indicates that the HSS has undergone a restart event and the registration data and dynamic data needs to be restored, if available at the 3GPP AAA Server.
NOTE: Bits not defined in this table shall be cleared by the sending HSS and discarded by the receiving 3GPP AAA Server.		

### 8.2.3.18 TWAN-Default-APN-Context-Id

The TWAN-Default-APN-Context-Id AVP is of the type Unsigned32 and shall identify the context identifier of the subscriber's default APN to be used for Trusted WLAN access to EPC over S2a.

Note: The default APN for Trusted WLAN access to EPC over S2a can differ from the default APN for 3GPP and other non-3GPP accesses.

### 8.2.3.19 TWAN-Access-Info

The TWAN-Access-Info AVP is of type Grouped.

If no WLAN-Identifier AVP is included in the TWAN-Access-Info AVP, the allowed access methods shall apply to any arbitrary Trusted WLAN. See subclause 5.1.2.1.2.

If the Access-Authorization-Flags AVP is not present in the TWAN-Access-Info AVP, EPC access and Non-Seamless WLAN Offload shall be considered to be not allowed.

A specific Trusted-WLAN shall appear in at most one TWAN-Access-Info AVP.

There shall be at most one TWAN-Access-Info AVP not including any WLAN-Identifier.

AVP Format:

```

TWAN-Access-Info ::=
    < AVP Header: 1510 10415 >
    [ Access-Authorization-Flags ]
    [ WLAN-Identifier ]
    *[ AVP ]
  
```

### 8.2.3.20 Access-Authorization-Flags

The Access-Authorization-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 8.2.3.20/1:

**Table 8.2.3.20 /1: Access-Authorization-Flags**

Bit	Name	Description
0	EPC-Access-Authorization	This bit, when set, indicates that the UE is allowed to access the EPC when connected via Trusted WLAN access. This flag, when not set, indicates that the UE is not allowed to access EPC when connected via Trusted WLAN access.
1	NSWO-Access-Authorization	This bit, when set, indicates that the UE is allowed Non-Seamless WLAN Offload access via Trusted WLAN access. This flag, when not set, indicates that the UE is not allowed to Non-Seamless WLAN Offload via Trusted WLAN access.
NOTE: Bits not defined in this table shall be cleared by the sending HSS and discarded by the receiving 3GPP AAA Server.		

NOTE: UE is allowed to access the EPC when connected via Trusted WLAN access only if the Non-3GPP-IP-Access-APN AVP does not disable all APNs and the EPC-Access-Authorization bit is set.

### 8.2.3.21 AAA-Failure-Indication

The AAA-Failure-Indication AVP is of type Unsigned32 and it shall contain a bitmask. The meaning of the bits is defined in table 8.2.3.21/1:

**Table 8.2.3.21/1: AAA-Failure-Indication**

Bit	Name	Description
0	AAA Failure	This bit, when set, indicates that a previously assigned 3GPP AAA Server is unavailable.
NOTE: Bits not defined in this table shall be cleared by the sender and discarded by the receiver.		

## 8.2.4 Session Handling

The Diameter protocol between the 3GPP AAA Server and the HSS shall not keep the session state and each Diameter request/response interaction shall be transported over a different diameter session which is implicitly terminated.

In order to indicate that session state shall not be maintained, the diameter client and server shall include the Auth-Session-State AVP set to the value NO\_STATE\_MAINTAINED (1), as described in IETF RFC 3588 [7]. As a consequence, the server shall not maintain any state information about this session and the client shall not send any session termination request. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP shall be present in requests or responses.

## 8.3 User identity to HSS resolution

The User identity to HSS resolution mechanism enables the 3GPP AAA server to find the identity of the HSS that holds the subscriber data for a given user identity when multiple and separately addressable HSSs have been deployed by the network operator. The resolution mechanism is not required in networks that utilise a single HSS or when a 3GPP AAA server is configured to use pre-defined HSS address/identity.

This User identity to HSS resolution mechanism may rely on routing capabilities provided by Diameter and be implemented in the home operator network within dedicated Diameter Agents (Redirect Agents or Proxy Agents) responsible for determining the HSS identity based on the provided user identity. If this Diameter based implementation is selected by the Home network operator, the principles described below shall apply.

In networks where more than one independently addressable HSS are utilized by a network operator, and the 3GPP AAA server is not configured to use pre-defined HSS address/identity, each 3GPP AAA server shall be configured with the address/identity of the Diameter Agent (Redirect Agent or Proxy Agent) implementing this resolution mechanism.

To get the HSS identity that holds the subscriber data for a given user identity, the 3GPP AAA server shall send the Diameter request normally destined to the HSS to a pre-configured address/identity of a Diameter agent supporting the User identity to HSS resolution mechanism.

- If this Diameter request is received by a Diameter Redirect Agent, the Diameter Redirect Agent shall determine the HSS identity based on the provided user identity and sends to the 3GPP AAA server a notification of redirection towards the HSS identity, in response to the Diameter request. Multiple HSS identities may be included in the response from the Diameter Redirect Agent, as specified in IETF RFC 3588 [7]. In such a case, the 3GPP AAA server shall send the Diameter request to the first HSS identity in the ordered list received in the Diameter response from the Diameter Redirect Agent. If no successful response to the Diameter request is received, the 3GPP AAA server shall send a Diameter request to the next HSS identity in the ordered list. This procedure shall be repeated until a successful response from an HSS is received.
- If this Diameter request is received by a Diameter Proxy Agent, the Diameter Proxy Agent shall determine the HSS identity based on the provided user identity and shall forward the Diameter request directly to the HSS. The 3GPP AAA server shall determine the HSS identity from the response to the Diameter request received from the HSS.

After the User identity to HSS resolution, the 3GPP AAA server shall store the HSS identity/name/Realm and shall use it in further Diameter requests associated to the same user identity.

NOTE: Alternatives to the user identity to HSS resolution Diameter based implementation are outside the scope of this specification.

---

## 9 S6b and H2 Description

### 9.1 Functionality

#### 9.1.1 General

The S6b reference point is defined between the 3GPP AAA Server and the PDN-GW. The definition of the reference point and its functionality is given in 3GPP TS 23.402 [3].

When the UE attaches to the EPC using the S2c reference point, the S6b reference point is used to authenticate and authorize the UE, and update the PDN-GW address to the 3GPP AAA server and HSS.

When the UE attaches to the EPC using the S2a/S2b reference point in the PMIPv6 or GTPv2 mode, the S6b reference point is used to update the 3GPP AAA server or the 3GPP AAA proxy with the PDN-GW address information and with the selected S2a/S2b protocol variant. Furthermore, this reference point may be used to retrieve and update other mobility related parameters including static QoS profiles for non-3GPP accesses.

The S6b reference point is also used to authenticate and authorize the incoming MIPv4 Registration Request in the case the UE attaches to the EPC over the S2a reference point using MIPv4 FACoA procedures.

The S6b reference point is used by the 3GPP AAA Server in the case the UE attaches to the EPC using the S2c reference point to indicate to the PDN GW that a PDN GW reallocation shall be performed. This indication triggers the actual Home Agent reallocation procedure as specified in 3GPP TS 24.303 [13].

The S6b reference point is also used to download subscriber and equipment trace information to the PDN GW.

The H2 reference point is defined between the 3GPP AAA Server and the HA. The definition of the reference point and its functionality is given in 3GPP TS 23.327 [12].

NOTE: The H2 interface is a subset of the S6b interface in the sense that only the DSMIPv6 procedures and the respective AVPs are implemented. Therefore, in the context of DSMIPv6 the procedures described in this specification apply to both S6b and H2.

## 9.1.2 Procedures Description

### 9.1.2.1 Authentication and Authorization Procedures when using DSMIPv6

#### 9.1.2.1.1 General

The S6b interface shall enable the authentication and authorization between the UE and the 3GPP AAA Server/Proxy for DSMIPv6.

When an UE performs the DSMIPv6 initial attach, it runs an IKEv2 exchange with the PDN GW as specified in 3GPP TS 24.303 [13]. In this exchange EAP AKA is used for UE authentication over IKEv2. The PDN GW acts as an IKEv2 responder and an EAP pass-through authenticator for this authentication.

The S6b authentication and authorization procedure is invoked by the PDN GW after receiving an IKE\_SA\_AUTH message from the UE. The S6b reference point performs authentication based on reuse of the DER/DEA command set defined in Diameter EAP. The exact procedure follows the steps specified in IETF RFC 5778 [11].

**NOTE:** This procedure is only used with DSMIPv6-capable UEs; therefore, only PDNs with PDN Types IPv6 or IPv4v6 are accessible in this case.

Table 9.1.2.1/1: Authentication and Authorization Request

Information Element Name	Mapping to Diameter AVP	Cat.	Description
User identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
Authentication Request Type	Auth-Request-Type	M	This IE shall define whether the UE is to be authenticated only, authorized only or both. AUTHORIZE_AUTHENTICATE shall be used in this case.
EAP Payload	EAP-Payload	M	This IE shall contain the Encapsulated payload for UE – 3GPP AAA Server mutual authentication
PGW PLMN ID	Visited-Network-Identifier	C	This IE shall contain the identifier that allows the home network to identify the PLMN where the PGW is located. It shall be present when the PGW Identity does not contain an FQDN.
Access Type	RAT-Type	C	This Information Element shall contain the non-3GPP access network technology type that is serving the UE. This IE shall be present if it is available when the PDN GW sends the request.
PDN GW Identity	MIP6 -Agent-Info	M	This IE shall contain the FQDN and/or IPv6 address(es) of the PDN GW that the user shall be connected to. If the PDN GW includes the IP address in the PDN GW Identity, it shall include the HA IPv6 address and, if used, the IPv4 address, as DSMIPv6 is used.
MIP Subscriber Profile	MIP6-Feature-Vector	M	This AVP shall be included to inform the 3GPP AAA Server about the used mobility protocol. None of the PMIP6_SUPPORTED or MIP4_SUPPORTED flags shall be set, since DSMIPv6 is used in this case.
APN	Service-Selection	O	If present, this IE shall contain the Network Identifier part of the APN extracted from the IKE_AUTH message. It shall include the APN that the user shall be connected to. It shall be only included if received from UE. In case it is not received, the 3GPP AAA Server shall assign the received PDN-GW identity to the default APN.
QoS capabilities	QoS-Capability	O	This IE shall be included if present in the request message. It shall indicate to the 3GPP AAA Server that the PGW requests downloading a static QoS profile for the UE. The PGW may include this IE only at the initial attach of the UE.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.
Care of Address	MIP-Careof-Address	O	If present, this IE shall contain the IPv4 or the IPv6 Care of Address of the UE as defined in IETF RFC 5778 [11]
AAA Failure Indication	AAA-Failure-Indication	O	If present, this information element shall indicate that the request is sent after the PDN-GW has determined that a previously assigned 3GPP AAA Server is unavailable.
DER S6b Flags	DER-S6b-Flags	O	This Information Element contains a bit mask. See 9.2.3.7 for the meaning of the bits.
UE local IP address	UE-Local-IP-Address	O	The PDN GW shall include this IE based on local policy for Fixed Broadband access network interworking as specified in 3GPP TS 23.139 [39]. If present, it shall contain the source IPv4 or IPv6 address of the IKE_SA_AUTH message from the UE.

Table 9.1.2.1/2: Authentication and Authorization Answer

Information Element Name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	O	This information element, if present, shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
EAP Payload	EAP-Payload	O	If present, this IE shall contain the Encapsulated payload for UE – 3GPP AAA Server mutual authentication
Master Session Key	EAP-Master-Session-Key	C	This IE shall contain the Keying material for protecting the communication between the UE and PDN GW. It shall be present only if the result code is set to success.
Authentication Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_AUTHENTICATE. See IETF RFC 4072 [5].
Result Code	Result-Code / Experimental-Result-Code	M	<p>This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter Base Protocol or as per in NASREQ. The Result-Code DIAMETER_MULTI_ROUND_AUTH shall be used in the responses that trigger further requests from the PDN GW and DIAMETER_SUCCESS shall be included at the successful completion of the authentication and authorization procedure.</p> <p>The Experimental-Result AVP shall be used for S6b errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.</p> <p>If the Result-Code is set to DIAMETER_SUCCESS_RELOCATE_HA as defined in IETF RFC 5778 [11], then the 3GPP AAA server is indicating to the PGW that it shall initiate a HA switch procedure towards the UE.</p>
MIP Subscriber Profile	MIP6-Feature-Vector	C	This AVP shall be present if the authorization was successful. None of the PMIP6_SUPPORTED or MIP4_SUPPORTED flags shall be set, since DSMIPv6 is used in this case.
Permanent User Identity	Mobile-Node-Identifier	C	<p>This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS.</p> <p>This IE shall contain an AAA/HSS assigned permanent user identity (i.e. an IMSI in EPC root NAI format as defined in clause 19 of 3GPP TS 23.003 [14]). This IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.</p>
APN and PGW Data	APN-Configuration	C	<p>This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS.</p> <p>This AVP shall contain the default APN, the list of authorized APNs, user profile information.</p> <p>APN-Configuration is a grouped AVP including the following information elements per APN:</p> <ul style="list-style-type: none"> <li>- APN</li> <li>- Authorized 3GPP QoS profile</li> <li>- Statically allocated User IP Address (IPv4 and/or IPv6)</li> <li>- Allowed PDN type (IPv4, IPv6, IPv4v6, IPv4_OR_IPv6)</li> <li>- APN-AMBR</li> </ul>
Reallocated PGW Address	MIP6-Agent-Info	C	<p>This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS_RELOCATE_HA indicating to the PDN GW that it shall initiate a HA switch procedure towards the UE.</p> <p>This information element shall contain the PDN GW identity of the target PDN GW.</p>
Session Time	Session-Timeout	C	If the authentication and authorization succeeded, then this IE shall contain the time this authorization is valid for.
QoS resources	QoS-Resources	C	<p>This AVP shall be included only if the QoS-Capability AVP was received in the authorization request and the authorization succeeded. Then the 3GPP AAA server shall include a static QoS profile in this IE during the UE initial attach if the PDN GW included QoS-Capabilities AVP in the request message and the UE has been provisioned with a static QoS profile. The QoS profile template value in this IE shall be set to 0.</p>

UE Charging Data	3GPP-Charging-Characteristics	O	If present, this information element shall contain the type of charging method to be applied to the user (see 3GPP TS 29.061 [31]).
3GPP AAA Server Name	Redirect-Host	C	This information element shall be sent if the Result-Code value is set to DIAMETER_REDIRECT_INDICATION. When the user has previously been authenticated by another 3GPP AAA Server, it shall contain the Diameter identity of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter Base Protocol (IETF RFC 3588 [7]). The command shall contain zero or more occurrences of this information element. When choosing a destination for the redirected message from multiple Redirect-Host AVPs, the receiver shall send the Diameter request to the first 3GPP AAA Server in the ordered list received in the Diameter response. If no successful response to the Diameter request is received, the receiver shall send the Diameter request to the next 3GPP AAA Server in the ordered list. This procedure shall be repeated until a successful response is received from a 3GPP AAA Server.
Trust Relationship Indicator	AN-Trusted	C	This AVP shall contain the 3GPP AAA Server's decision on handling the non-3GPP access network, i.e. trusted, or untrusted. This AVP shall be present if the 3GPP AAA Server is able to make decision on whether the access network is Trusted or Untrusted.
Trace information	Trace-Info	C	This AVP shall be included if the subscriber and equipment trace has been activated for the user in the HSS and signalling based activation is to be used to download the trace activation from the HSS to the PDN GW. Only the Trace-Data AVP shall be included to the Trace-Info AVP and shall contain the following AVPs: - Trace-Reference - Trace-Depth - Trace-Event-List, for PGW - Trace-Collection-Entity The following AVPs may also be included in the Trace-Data AVP: - Trace-Interface-List, for PGW, if this AVP is not present, trace report generation is requested for all interfaces for PGW listed in 3GPP TS 32.422 [32] - Trace-NE-Type-List, with the only allowed value being "PDN GW". If this AVP is not included, trace activation in PDN GW is required.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.

### 9.1.2.1.2 PDN GW Detailed Behaviour

After completing the IKE\_SA\_INIT exchange, upon receipt of an IKE\_AUTH message, including the IDi payload but not the AUTH payload, the PDN GW shall send an Diameter-EAP-Request (DER) message towards the 3GPP AAA Server / Proxy. The EAP Payload AVP shall contain an EAP-Response/Identity with the identity extracted from the IDi field.

Upon receipt of an IKE\_AUTH message with an EAP payload from the UE, the PDN GW shall send an Diameter-EAP-Request (DER) with the EAP Payload AVP containing the according EAP-Response to the 3GPP AAA Server / Proxy.

Upon receipt of a Diameter-EAP-Answer (DEA) message from the 3GPP AAA Server / Proxy, the PDN GW shall then send an IKE\_AUTH message containing the according EAP Payload to the UE.

Upon receipt of an IKE\_AUTH message with the AUTH payload after the EAP authentication was successful, the PDN\_GW shall proceed as specified in 3GPP TS 24.303 [13].

If the handover indication to the PGW is missing, i.e. IPv6 Home Network Prefix assigned to the UE is not included in IKE\_AUTH request message as specified in 3GPP TS 24.303 [13], the PGW shall notify 3GPP AAA Server that the UE performs initial attach by setting Initial-Attach-Indicator in the DER-S6b-flags AVP.

The PDN GW shall utilize the downloaded APN configuration data, among others, to decide whether the user's request for an IPv4 home address and/or IPv6 home address prefix shall be accepted or rejected.

If the Result-Code AVP is set to `DIAMETER_SUCCESS_RELOCATE_HA` and if the PGW has received a PGW identity in form of the FQDN from the 3GPP AAA server, then the PGW may obtain the IP address of the Home Agent functionality of that PGW as described in 3GPP TS 29.303 [34].

If Trace-Info AVP has been received in the authentication and authorization response, the PDN GW shall start a trace session for the user. For details, see 3GPP TS 32.422 [32].

If the PDN-GW determines that a previously assigned 3GPP AAA Server is unavailable, it may attempt to send a new authentication and authorization request to an alternate 3GPP AAA Server. If the PDN-GW receives from this new server a redirect indication towards the former server (due to the HSS having stored the former 3GPP AAA Server identity), it shall terminate all previously existing sessions and PDN connections for that user, and it shall re-send again the request towards the new server, but it shall include the AAA-Failure-Indication AVP in the new request.

### 9.1.2.1.3 3GPP AAA Server Detailed Behaviour

For S6b, on receipt of the DER message, the 3GPP AAA Server shall process the DER message according to 3GPP TS 33.402 [19]. For H2, the 3GPP AAA server shall process the DER message according to 3GPP TS 33.234 [10].

Upon successful completion, a `DIAMETER_SUCCESS` shall be returned to indicate successful authentication procedure and authentication information shall be returned. The AAA server shall also include, among others, the MIP6-Feature-Vector AVP, including the subscriber profile of the UE in terms of DSMIPv6 feature the UE is authorized to use.

If the HSS indicates that the user is currently being served by a different PDN GW, the 3GPP AAA Server shall respond to the PDN GW with the Result-Code set to `DIAMETER_SUCCESS_RELOCATE_HA` and include the new assigned PDN GW identity in the MIP6-Agent-Info AVP.

If receiving the UE Care of Address from the PDN GW and Initial-Attach-Indicator set by the PGW in DER-S6b-flags, the 3GPP AAA Server may select a different PDN GW which is closer to the UE than the currently serving PDN GW as specified in 3GPP TS 23.402 [3] based on the received UE Care of Address. In this case, the 3GPP AAA Server shall respond to the PDN GW with the Result-Code set to `DIAMETER_SUCCESS_RELOCATE_HA` and include the selected PDN GW identity in the MIP6-Agent-Info AVP.

If the HSS indicates that the user is currently being served by a different 3GPP AAA Server, the 3GPP AAA Server shall respond to the PDN-GW with the Result-Code set to `DIAMETER_REDIRECT_INDICATION` and Redirect-Host set to the Diameter identity of the 3GPP AAA Server currently serving the user (as indicated in the 3GPP-AAA-Server-Name AVP returned in the SWx authentication response from the HSS).

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

The 3GPP AAA Server shall run EAP-AKA as specified in 3GPP TS 33.402 [19]. Exceptions shall be treated as error situations and the result code shall be set to `DIAMETER_UNABLE_TO_COMPLY`.

Before sending out the AKA challenge, the 3GPP AAA Server shall decide whether the access network is handled as Trusted or Untrusted and set the value of the AN-Trusted AVP correspondingly in the answer message to indicate the trust relationship of the access network to the PDN GW. The 3GPP AAA Server shall make the decision based on the UE Identity and the trust relationship information marked during the authentication and authorization procedure over STa, SWa or SWm. If the 3GPP AAA server is unable to determine the trust relationship of the access network, it shall not include the AN-Trusted AVP in the answer message to the PDN GW.

For Fixed Broadband access network interworking as specified in 3GPP TS 23.139 [39],

- For trusted access, the 3GPP AAA server shall determine if the UE is connected via a BBF-defined WLAN access according to the UE local IP address in UE-Local-IP-Address AVP from the PDN GW. If the UE is connected via a BBF-defined WLAN access, the 3GPP AAA server shall perform the enabling UE reflective QoS function as specified in 3GPP TS 24.139 [43].
- For untrusted access, the UE local IP address is assigned by the ePDG and not by the non-3GPP access network. Hence, in this case the 3GPP AAA Server shall ignore the UE local IP address in UE-Local-IP-Address AVP from the PDN GW.

#### 9.1.2.1.4 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy is required to handle roaming cases in which the PDN GW is in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy.

On receipt of the authentication answer that completes a successful authentication, the 3GPP AAA Proxy shall record the state of the connection (i.e. Authentication Successful).

If receiving the UE Care of Address from the PDN GW which is in the VPLMN, the 3GPP AAA Proxy may select a different PDN GW which is closer to the UE than the currently serving PDN GW as specified in 3GPP TS 23.402 [3] based on the received UE Care of Address. In this case, the 3GPP AAA Proxy shall respond to the PDN GW with the Result-Code set to DIAMETER\_SUCCESS\_RELOCATE\_HA and include the selected PDN GW identity in the MIP6-Agent-Info AVP.

#### 9.1.2.2 Authorization Procedures when using PMIPv6 or GTPv2

##### 9.1.2.2.1 General

The following authorization procedures take place upon a reception of a PBU at the PDN GW from the MAG or upon a reception of a Create Session Request at the PDN GW from the trusted non-3GPP access network or from the ePDG.

The PDN GW shall update its address information to the 3GPP AAA Server and HSS. Static QoS profile information may also be downloaded at the same time. If the PDN GW reports to the 3GPP AAA server that GTPv2 is used over the S2a or S2b interface, the 3GPP AAA Server may decide not to download parameters to the PDN GW on the S6b interface which are already provided to the PGW via the trusted non-3GPP access network through the STa and GTPv2 based S2a interfaces or via the ePDG through the SWm and the GTPv2 based S2b interfaces (e.g. static QoS profile, Trace Information, APN-AMBR).

The procedures are based on the reuse of NASREQ IETF RFC 4005 [4] AAR and AAA commands and the Diameter extensions defined for PMIP in IETF RFC 5779 [2].

Table 9.1.2.2.1/1: Authorization request

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Authentication Request Type	Auth-Request-Type	M	This IE shall defines whether the UE is to be authenticated only, authorized only or both. AUTHORIZE_ONLY shall be used in this case.
PDN GW Identity	MIP6-Agent-Info	C	If present, this IE shall contain the identity of the selected PDN GW for the UE and the corresponding PDN connection. It shall be present on the first authorization request sent by the PGW to the 3GPP AAA Server for a given APN.
PGW PLMN ID	Visited-Network-Identifier	C	This IE shall contain the identifier that allows the home network to identify the PLMN where the PGW is located. It shall be present when the PGW Identity is present and does not contain an FQDN.
Mobility features	MIP6-Feature-Vector	M	This IE shall contain the mobility features used by the PDN GW. The PDN GW shall set the PMIP6_SUPPORTED flag or the GTPv2_SUPPORTED flag according to the protocol variant used over the S2a or the S2b interface.
APN	Service-Selection	M	This IE shall contain the Network Identifier part of the APN extracted from the PBU or the Create Session Request message.
QoS capabilities	QoS-Capability	O	If included in the request message, this IE shall indicate to the 3GPP AAA server that the PDN GW requests downloading a static QoS profile for the UE. The PDN GW may include this IE only at the initial attach of the UE. The PDN GW should not include this IE if GTPv2 is used over the S2a or the S2b interface.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.

Table 9.1.2.2.1/2: Authorization answer

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Result code	Result-Code	M	This IE shall contain the result of the operation. The possible values of the Result-Code AVP are defined in IETF RFC 3588 [7]. This IE shall be set to DIAMETER_SUCCESS if the update to the PDN GW address succeeded. It shall be set to DIAMETER_AUTHORIZATION_REJECTED if the update of the PDN GW address failed.
Authentication Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_ONLY. See IETF RFC 4072 [5].
Authorized mobility features	MIP6-Feature-Vector	C	The 3GPP AAA Server shall insert this AVP if the authorization was successful. The PMIP6_SUPPORTED or the GTPv2_SUPPORTED flag shall be set according to the value received in the Authorization request.
Session time	Session-Timeout	C	If the authorization succeeded, then this IE shall contain the time this authorization is valid for.
APN and PGW Data	APN-Configuration	C	This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS. This AVP shall contain the user profile information. APN-Configuration is a grouped AVP and shall include the following information elements: - APN - Authorized 3GPP QoS profile - APN-AMBR This information element may not be included in the Authorization answer, if the MIP6-Feature-Vector in the Authorization request indicates that GTPv2 is used over S2a or S2b.
QoS resources	QoS-Resources	C	This AVP shall be included only if the QoS-Capability AVP was received in the authorization request and the authorization succeeded. Then the 3GPP AAA server shall include a static QoS profile in this IE during the UE initial attach if the PDN GW included a QoS-Capabilities AVP in the request message and the UE has been provisioned with a static QoS profile. The QoS profile template value in this IE shall be set to 0.
3GPP AAA Server Name	Redirect-Host	C	This information element shall be sent if the Result-Code value is set to DIAMETER_REDIRECT_INDICATION. When the user has previously been authenticated by another 3GPP AAA Server, it shall contain the Diameter identity of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter Base Protocol (IETF RFC 3588 [7]). The command shall contain zero or more occurrences of this information element. When choosing a destination for the redirected message from multiple Redirect-Host AVPs, the receiver shall send the Diameter request to the first 3GPP AAA Server in the ordered list received in the Diameter response. If no successful response to the Diameter request is received, the receiver shall send the Diameter request to the next 3GPP AAA Server in the ordered list. This procedure shall be repeated until a successful response is received from a 3GPP AAA Server.
Trace information	Trace-Info	C	This AVP shall be included if the MIP6-Feature-Vector in the Authorization request indicates that PMIPv6 is used over S2a or S2b and if the subscriber and equipment trace has been activated or deactivated for the user in the HSS GW and signalling based activation is used to download the trace (de)activation from the HSS to the PDN GW.  In an authorization response sent during the authorization procedure at PDN connection setup, the Trace-Data AVP shall be included. In an authorization response sent during the service authorization information update procedure, - the Trace-data AVP shall be included if trace activation is requested - the Trace-Reference AVP shall be included, if trace deactivation is requested.  If the Trace-Data AVP is included, it shall contain the following AVPs: - Trace-Reference - Trace-Depth

			<ul style="list-style-type: none"> <li>- Trace-Event-List, for PGW</li> <li>- Trace-Collection-Entity</li> </ul> <p>The following AVPs may also be included in the Trace-Data AVP:</p> <ul style="list-style-type: none"> <li>- Trace-Interface-List, for PGW, if this AVP is not present, trace report generation is requested for all interfaces for PGW listed in 3GPP TS 32.422 [32]</li> <li>- Trace-NE-Type-List, with the only allowed value being "PDN GW". If this AVP is not included, trace activation in PDN GW is required.</li> </ul>
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.

#### 9.1.2.2.2 PDN GW Detailed Behaviour

Upon receipt of a PBU message from the MAG or upon receipt of a Create Session Request from the trusted non-3GPP access network or the ePDG which requires the establishment of a new PDN connection via the non-3GPP access, the PDN GW shall initiate an authorization procedure, by sending an Authorization Request message to the 3GPP AAA server or to the 3GPP AAA Proxy, with the Auth-Request-Type set to AUTHORIZE\_ONLY, in order to update the PGW Address for the APN and the selected S2a or S2b protocol variant, as well as to optionally download any UE specific APN profile information such as IP address allocation information, QoS Information, Session timeouts, Session Idle timeouts etc.

The PDN GW shall include in the request the APN where the user shall be connected to.

The PDN GW Identity and PLMN shall only be included in the initial request to the 3GPP AAA server; subsequent authorization messages (due to a handover to a different MAG, for instance) shall not include it again.

After successful reception of the Authorization Request message, the PDN GW shall check that the Result-Code is set to DIAMETER\_SUCCESS and, if so, it shall proceed to connect the user to the specified APN.

For PMIPv6 based S2a or S2b, if Trace-Info AVP including Trace-Data has been received in the authorization response, the PDN GW shall start a trace session for the user. If Trace-Info including Trace-Reference (directly under the Trace-Info) has been received in the authorization response, the PDN GW shall stop the ongoing trace session, identified by the Trace-Reference. For details, see 3GPP TS 32.422 [32].

For GTPv2 based S2a or S2b, the PDN GW shall ignore the Trace-Info AVP if received in the authorization response.

NOTE: For GTPv2 based S2a or S2b, trace is activated and deactivated via the STa and S2a interfaces or via the SWm and S2b interfaces.

#### 9.1.2.2.3 3GPP AAA Server Detailed Behaviour

Upon receipt of the Authorization Request message from the PDN GW, the 3GPP AAA Server shall update the PDN GW information for the APN for the UE on the HSS.

The 3GPP AAA Server must check whether the user's profile is available.

If the user's data exist in the 3GPP AAA Server, it shall check, whether it also has an active access authorization session for the user.

- If not, the 3GPP AAA Server shall reject the authorization request, including the Result-Code DIAMETER\_AUTHORIZATION\_REJECTED.
- If the 3GPP AAA Server has an existing authorization session,
- If the APN requested by the PDN GW is included in the list of authorized APNs of the user, then the 3GPP AAA Server shall include the Service-Selection AVP in the authorization answer and set the Result-Code to DIAMETER\_SUCCESS.

- If the APN requested by the PDN GW is not included in the list of authorized APNs, then the status code `DIAMETER_AUTHORIZATION_REJECTED` shall be returned to the PDN GW to indicate an unsuccessful authorization.

If the user's profile does not exist in the 3GPP AAA Server, it shall retrieve the Diameter identity of the 3GPP AAA Server currently serving the user from the HSS following the procedures for subscriber profile download as specified in section 8.1.2.2.2. Depending on the HSS response,

- If the HSS indicates that the user is currently being served by a different 3GPP AAA Server, the 3GPP AAA Server shall respond to the PDG-GW with the Result-Code set to `DIAMETER_REDIRECT_INDICATION` and Redirect-Host set to the Diameter identity of the 3GPP AAA Server currently serving the user (as indicated in the 3GPP-AAA-Server-Name AVP returned in the SWx authentication response from the HSS).
- If the HSS returns `DIAMETER_ERROR_USER_UNKNOWN`, the 3GPP AAA Server shall return the same error to the PDN GW.
- If the HSS sends the user's profile to the 3GPP AAA Server, the authorization shall be rejected by setting the Result-Code to `DIAMETER_AUTHORIZATION_REJECTED`. The 3GPP AAA Server shall delete the downloaded user profile.

NOTE: The last outcome corresponds to the case that the user has no active access authorization procedure. This is considered as an error situation, e.g. the Trusted Non-3GPP access network may have sent PBU without authorizing the user.

#### 9.1.2.2.4 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy is required to handle roaming cases in which the PDN GW is located in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy.

On receipt of the authorization answer, the 3GPP AAA Proxy

- shall check locally configured information for the maximum allowed static QoS parameters valid for visitors from the given HPLMN and modify the QoS parameters received from the 3GPP AAA Server, to enforce the policy limitations.
- shall record the state of the connection (i.e. Authorization Successful).

#### 9.1.2.3 PDN GW Initiated Session Termination Procedures

##### 9.1.2.3.1 General

The S6b reference point allows the PDN GW to inform the 3GPP AAA server that the UE disconnected a PDN connection associated to an APN, or that the PDN connection was handed over to the 3GPP access, and therefore the mobility session established for this PDN connection is to be removed.

The procedure shall be initiated by the PDN GW. These procedures are based on the reuse of Diameter Base IETF RFC 3588 [7] STR and STA commands.

Each PDN connection shall be identified by the Diameter Session-Id parameter.

**Table 9.1.2.3.1/1: S6b Session Termination Request**

Information Element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Termination Cause	Termination-Cause	M	This IE shall contain the reason for the disconnection, according to the values and reasons described in IETF RFC 3588 [7]. In particular:  - If the session is terminated as a result of a PDN disconnection initiated by the UE, the Termination-Cause shall be set to the value DIAMETER_LOGOUT (1)  - If the session is terminated as a result of a PDN handover towards 3GPP access, the Termination-Cause shall be set to the value DIAMETER_USER_MOVED (7)

**Table 9.1.2.3.1/2: S6b Session Termination Answer**

Information Element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for S6b errors.

### 9.1.2.3.2 PDN GW Detailed Behaviour

The PDN GW shall make use of this procedure when the PDN Connection associated to the diameter session is, either disconnected, or handed over to the 3GPP access.

Upon receipt of the Session Termination Answer message from the 3GPP AAA Server or from the 3GPP AAA Proxy, the PDN GW shall check the Result Code AVP, and in case of a DIAMETER\_SUCCESS code, it shall release the context associated to the active session identified by the Session-Id parameter used in the initial authorization exchange.

### 9.1.2.3.3 3GPP AAA Server Detailed Behaviour

Upon receipt of the Session Termination Request message from the PDN GW or from the 3GPP AAA Proxy, the 3GPP AAA Server shall check that there is an ongoing session associated to any of the parameters received in the message (Session-Id and User Name).

If an active session is found, the 3GPP AAA Server shall release the session context associated to the specified session, and a Session Termination Answer message shall be sent to the PDN GW or 3GPP AAA Proxy, indicating DIAMETER\_SUCCESS.

If the Session-Id included in the request does not correspond with any active session, or if an active session is found but it does not belong to the user identified by the User Name parameter, then a Session Termination Answer message shall be sent to the PDN GW or 3GPP AAA Proxy, indicating DIAMETER\_UNKNOWN\_SESSION\_ID.

### 9.1.2.3.4 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy is required to handle roaming cases in which the PDN GW is located in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy.

On receipt of the Session Termination Request message from the PDN GW, the 3GPP AAA Proxy shall route the message to the 3GPP AAA Server.

On receipt of the Session Termination Answer message from the 3GPP AAA Server, the 3GPP AAA Proxy shall route the message to the PDN GW, and it shall release any local resources associated to the specified sessions only if the result code is set to DIAMETER\_SUCCESS.

## 9.1.2.4 3GPP AAA Initiated Session Termination Procedures

### 9.1.2.4.1 General

The S6b reference point allows the 3GPP AAA server to order a PDN GW to remove a PDN connection previously activated by the UE.

This procedure shall be initiated by the 3GPP AAA server. This indicates to the PDN GW to remove the corresponding PDN connection (identified by Session-ID AVP and User-Name AVP). This procedure is based on the reuse of NASREQ IETF RFC 4005 [4] ASR, ASA, STR and STA commands.

The 3GPP AAA Server shall include the Auth-Session-State AVP in the ASR command with a value of NO\_STATE\_MAINTAINED if it does not require a STR from the PDN GW. If it does require a STR from the PDN GW, the 3GPP AAA Server shall either omit the Auth-Session-State AVP from the ASR command or include the Auth-Session-State AVP in the ASR command with a value of STATE\_MAINTAINED.

**Table 9.1.2.4.1/1: S6b Abort Session Request**

Information Element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Auth-Session-State	Auth-Session-State	O	If present, this information element shall indicate to the PDN GW whether the 3GPP AAA Server requires an STR message.

**Table 9.1.2.4.1/2: S6b Abort Session Answer**

Information Element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for S6b errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

**Table 9.1.2.4.1/3: S6b Session Termination Request**

Information element name	Mapping to Diameter AVP	Cat.	Description
Termination-Cause	Termination-Cause	M	This information element shall contain the reason why the session was terminated. It shall be set to "DIAMETER_ADMINISTRATIVE" to indicate that the session was terminated in response to an ASR message.

**Table 9.1.2.4.1/4: S6b Session Termination Answer**

Information element name	Mapping to Diameter AVP	Cat.	Description
Result-Code	Result-Code	M	This IE shall indicate the result of the operation.

#### 9.1.2.4.2 PDN GW Detailed Behaviour

Upon receipt of the Abort Session Request message from the 3GPP AAA Server or from the 3GPP AAA Proxy, the PDN GW shall check that there is an ongoing session with the received session-ID.

If an active session is found:

- In the PMIPv6 or GTPv2 or MIPv4 cases, the PDN GW shall release any resources associated with the identified diameter session, but it shall not terminate any associated PDN connection.
- In the DSMIPv6 case, the PDN GW shall initiate a termination procedure for the associated PDN connection, and shall release any resources associated with the identified diameter session.

If the termination procedure is successful for the identified session, an Abort Session Answer message shall be sent to the 3GPP AAA Server or 3GPP AAA Proxy, indicating DIAMETER\_SUCCESS.

If the Session-Id included in the request does not correspond with any active session, or if an active session is found but it does not belong to the user identified by the User Name parameter, then an Abort Session Answer message shall be sent to the 3GPP AAA Server or 3GPP AAA Proxy, indicating DIAMETER\_UNKNOWN\_SESSION\_ID.

If the termination procedure for the identified session cannot be completed successfully, an Abort Session Answer message shall be sent to the 3GPP AAA Server or 3GPP AAA Proxy, indicating DIAMETER\_UNABLE\_TO\_COMPLY.

If the termination procedure was successful for the identified session and the STR is required by the 3GPP AAA Server, the PDN GW shall send an STR to the 3GPP AAA Server with the Termination-Cause set to DIAMETER\_ADMINISTRATIVE.

#### 9.1.2.4.3 3GPP AAA Server Detailed Behaviour

The 3GPP AAA Server shall initiate a separate procedure for each active PDN connection of the user, even if the user has several PDN connections via the same PDN GW.

Upon receipt of the Abort Session Answer message from the PDN GW or from the 3GPP AAA Proxy, the 3GPP AAA Server shall check the Result Code AVP, and in case of a DIAMETER\_SUCCESS code, it shall release the context associated to the active session identified by the Session-Id parameter.

If the error code DIAMETER\_UNABLE\_TO\_COMPLY is received in the Result Code AVP, the 3GPP AAA Server shall not release the context for the identified session.

If the error code DIAMETER\_UNKNOWN\_SESSION\_ID is received in the Result Code AVP, the 3GPP AAA Server shall release the context for the identified session.

On receipt of the STR from PDN GW, the 3GPP AAA Server shall return an STA command with the Result-Code set to DIAMETER\_SUCCESS.

#### 9.1.2.4.4 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy is required to handle roaming cases in which the PDN GW is located in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy.

On receipt of the Abort Session Request message from the 3GPP AAA Server, the 3GPP AAA Proxy shall route the message to the PDN GW.

If the 3GPP AAA Proxy requires an STR but the 3GPP AAA Server does not, the 3GPP AAA Proxy may override the value of the Auth-Session-State in the ASR and set it to STATE\_MAINTAINED. In this case, the 3GPP AAA Proxy shall not forward the STR received from the PDN GW onto the 3GPP AAA Server and shall return an STA command to the PDN GW with the Result-Code set to DIAMETER\_SUCCESS. The 3GPP AAA Proxy shall not override the value of the Auth-Session-State AVP under any other circumstances.

On receipt of the Abort Session Answer message from the PDN GW, the 3GPP AAA Proxy shall route the message to the 3GPP AAA Server, and it shall release any local resources associated to the specified session only if the result code is set to DIAMETER\_SUCCESS.

When the 3GPP AAA Proxy receives the STR from PDN GW, it shall route the request to the 3GPP AAA Server. On receipt of the STA message, the 3GPP AAA Proxy shall route the response to the PDN GW.

## 9.1.2.5 Service Authorization Information Update Procedures

### 9.1.2.5.1 General

The S6b reference point allows the 3GPP AAA server to modify the authorization information previously provided to the PDN GW, i.e. during Service Authentication and Authorization when using DSMIPv6, or Service Authorization using PMIPv6 or GTPv2 or MIPv4, or the service authorization information provided during a previous Service Authorization update. This procedure is triggered by the modification of the non-3GPP profile of the UE or by activating or deactivating subscriber and equipment trace in the HSS. This procedure is also triggered by the authentication and authorization via STa or SWm, when the 3GPP AAA Server detects that an S6b session already exists for the UE, as specified in section 5.1.2.1.2 and 7.1.2.1.2. In this case, the 3GPP AAA Server shall use this procedure to send the trust relationship to the PDN GW.

The Service Authorization Information Update procedure is performed in two steps:

1. The 3GPP AAA server issues an unsolicited re-authentication and/or re-authorization request towards the PDN GW. Upon receipt of this request, the PDN GW responds to the request and indicates the disposition of the request. This procedure is based on the reuse of Diameter Base IETF RFC 3588 [7] RAR and RAA commands. The information element content for these messages is shown in tables 9.1.2.5.1/1 and 9.1.2.5.1/2.
2. After receiving the re-authorization request, the PDN GW invokes the authorization procedure for the APN identified by the session ID included in the former re-authorization request message. The authorization procedure for PMIPv6 or GTPv2 is described in the section 9.1.2.2. Tables 9.1.2.5.1/3 and 9.1.2.5.1/4 describe the message contents in case of DSMIPv6.

**Table 9.1.2.5.1/1: S6b Re-authorization request**

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Request Type	Re-Auth-Request-Type	M	This shall define whether re-authentication or re-authorization is required. AUTHORIZE_ONLY shall be used in this case.
RAR Flags	RAR-Flags	C	This Information Element contains a bit mask. See 9.2.3.1.x for the meaning of the bits.

**Table 9.1.2.5.1/2: S6b Re-authorization response**

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. The Experimental-Result AVP shall be used for S6b errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

Table 9.1.2.5.1/3: Authorization Request when using DSMIPv6

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Permanenet User identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Authentication Request Type	Auth-Request-Type	M	This IE defines whether the UE is to be authenticated only, authorized only or both. AUTHORIZE_ONLY shall be used in this case.
PGW PLMN ID	Visited-Network-Identifier	C	This IE shall contain the identifier that allows the home network to identify the PLMN where the PGW is located. It shall be present when the PGW Identity does not contain an FQDN.
Access Type	RAT-Type	M	This IE shall contain the non-3GPP access network technology type that is serving the UE.
PDN GW Identity	MIP6-Agent-Info	M	This IE shall contain the FQDN and/or IP address(es) of the PDN GW that the user is connected to.
APN	Service-Selection	O	This IE shall contain the Network Identifier part of the APN extracted from the IKE_AUTH message. It shall include the APN that the user shall be connected to. It shall be only included if received from UE. In case it is not received, the 3GPP AAA server shall assign the received PDN-GW identity to the default APN.
QoS capabilities	QoS-Capability	C	If included in the request message, this IE shall indicate to the 3GPP AAA server that the PGW is capable of downloading a static QoS profile for the UE. The PGW shall include this IE only during UE the initial attach.

Table 9.1.2.5.1/4: Authorization Answer when using DSMIPv6

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Result Code	Result-Code / Experimental-Result-Code	M	<p>This IE shall contain the result of the operation.</p> <p>The Result-Code AVP shall be used for errors defined in the Diameter Base Protocol or as per in NASREQ. 1xxx should be used for multi-round, 2xxx for success.</p> <p>The Experimental-Result AVP shall be used for S6b errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.</p>
Authentication Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_ONLY. See IETF RFC 4072 [5].
APN and PGW Data	APN-Configuration	C	<p>This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS.</p> <p>This AVP shall contain the default APN, the list of authorized APNs, and user profile information.</p> <p>The APN-Configuration is a grouped AVP and shall include the following information elements per APN:</p> <ul style="list-style-type: none"> <li>- APN</li> <li>- Authorized 3GPP QoS profile</li> <li>- Statically allocated User IP Address (IPv4 and/or IPv6)</li> <li>- VPLMN Dynamic Address Allowed.</li> </ul> <p>This information element might not be present if the authorization procedure is triggered by the 3GPP AAA Server to send the trust relationship to the PDN GW.</p>
Session Time	Session-Timeout	C	<p>If the authentication and authorization succeeded, then this IE shall contain the time this authorization is valid for.</p> <p>This information element might not be present if the authorization procedure is triggered by the 3GPP AAA Server to send the trust relationship to the PDN GW.</p>
QoS resources	QoS-Resources	C	<p>If the authentication and authorization succeeded, then the 3GPP AAA server shall include a static QoS profile in this IE during the UE initial attach if the PGW included QoS-Capabilities AVP in the request message and the UE has been provisioned with a static QoS profile.</p> <p>The QoS profile template value in this IE shall be set to 0.</p> <p>This IE shall contain the QoS Profile authorized by the 3GPP AAA server for the requested APN based on the subscribed QoS parameters.</p> <p>This information element might not be present if the authorization procedure is triggered by the 3GPP AAA Server to send the trust relationship to the PDN GW.</p>
Trace information	Trace-Info	C	<p>This AVP shall be included if the subscriber and equipment trace has been activated or deactivated for the user in the HSS and signaling based activation is used to download the trace (de)activation from the HSS to the PDN GW.</p> <p>Trace-data AVP shall be included (directly under the Trace-Info) if trace activation is requested</p> <p>Trace-Reference AVP shall be included, if trace deactivation is requested.</p> <p>If the Trace-Data AVP is included, it shall contain the following AVPs:</p> <ul style="list-style-type: none"> <li>- Trace-Reference</li> <li>- Trace-Depth</li> <li>- Trace-Event-List, for PGW</li> <li>- Trace-Collection-Entity</li> </ul> <p>The following AVPs may also be included in the Trace-Data AVP:</p> <ul style="list-style-type: none"> <li>- Trace-Interface-List, for PGW, if this AVP is not present, trace report generation is requested for all interfaces for PGW listed in 3GPP TS 32.422 [32]</li> <li>- Trace-NE-Type-List, with the only allowed value being "PDN GW". If this AVP is not included, trace activation in PDN GW is required.</li> </ul>
Trust Relationship Indicator	AN-Trusted	C	<p>This AVP shall contain the 3GPP AAA Server's decision on handling the non-3GPP access network, i.e. trusted, or untrusted.</p> <p>This AVP shall be sent if this re-authorization procedure is triggered by the authentication and authorization via STA or SWm, when the 3GPP</p>

			AAA Server detects that an S6b session already exists for the UE and the S6b session was established as a result of an authentication request for DSMIPv6.
--	--	--	--

### 9.1.2.5.2 Detailed Behaviour

The 3GPP AAA server shall make use of this procedure in two steps to indicate and update relevant service authorization information in the PDN GW.

The 3GPP AAA server shall send a re-authorization request for all authorization sessions that are active for the user.

Each PDN GW, upon reception of an unsolicited re-authentication and/or re-authorization request shall perform the following check and if there is an error detected, the PDN GW shall stop processing and return the corresponding error code.

Check the Re-Auth-Request-Type AVP:

1. If it indicates AUTHENTICATE\_ONLY, Result-Code shall be set to DIAMETER\_INVALID\_AVP\_VALUE.
2. If it indicates AUTHORIZE\_ONLY, then, depending on the used IP mobility protocol
  - In case of PMIPv6 or GTPv2, the PDN GW shall perform an authorization procedure as described in section 9.1.2.2.
  - In case of DSMIPv6, the PDN GW shall perform an authorization procedure, sending an authorization request described in Tables 9.1.5.1/3 and 9.1.5.1/4. If the Trust-Relationship-Update flag is set in the RAR Flags present in the request, the PDN GW may send an authorization request with only mandatory AVPs.
3. If it indicates AUTHORIZE\_AUTHENTICATE, Result-Code shall be set to DIAMETER\_INVALID\_AVP\_VALUE.

When receiving the authorization request, if the authorization procedure is triggered by the 3GPP AAA Server to send the trust relationship to the PDN GW, the 3GPP AAA Server shall send the trust relationship of the access network for the subscriber to the PDN GW with Result-Code DIAMETER\_SUCCESS. Otherwise, the 3GPP AAA Server shall check, whether

- the subscriber still has non-3GPP subscription to access EPC network
- the non-3GPP APNs are enabled for the user, and
- the updated user profile contains the APN, for which the given authorization session was created.

If any of the checked conditions are not met, the 3GPP AAA Server shall set the Result-Code to DIAMETER\_AUTHORIZATION\_REJECTED. Otherwise, it shall respond with Result-Code DIAMETER\_SUCCESS.

After successful service authorization information update procedure, the PDN GW shall overwrite the stored user and APN data, for the subscriber identity indicated in the request, with the information received from the 3GPP AAA server. A session termination shall be initiated if the subscriber is no longer authorized to use the activated APN. If only trust relationship of the access network is received, the PDN GW shall keep all stored user and APN data for the subscriber identity as indicated in the request.

For PMIPv6 based S2a or S2b, if Trace-Info AVP including Trace-Data has been received in the authorization response, the PDN GW shall start a trace session for the user. If Trace-Info including Trace-Reference (directly under the Trace-Info) has been received in the authorization response, the PDN GW shall stop the ongoing trace session, identified by the Trace-Reference. For details, see 3GPP TS 32.422 [32].

For GTPv2 based S2a or S2b, the PDN GW shall ignore the Trace-Info AVP if received in the authorization response.

**NOTE:** For GTPv2 based S2a or S2b, trace is activated and deactivated via the STa and S2a interfaces or via the SWm and S2b interfaces.

## 9.1.2.6 Authorization Procedures when using MIPv4 FACoA

### 9.1.2.6.1 General

The following authorization procedures take place upon a reception of a RRQ at the PDN GW from the FA.

The PDN GW shall update its address information to the 3GPP AAA Server and HSS. Static QoS profile information may also be downloaded at the same time.

MIPv4 security parameters shall be exchanged between the PDN GW and the 3GPP AAA Server.

The procedures are based on the reuse of NASREQ IETF RFC 4005 [4] AAR and AAA commands.

**Table 9.1.2.6.1/1: Authorization request**

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This IE shall contain the permanent user identity. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Authentication Request Type	Auth-Request-Type	M	This IE shall define whether the UE is to be authenticated only, authorized only or both. AUTHORIZE_ONLY shall be used in this case.
PDN GW Identity	MIP6-Agent-Info	O	This IE shall contain the address and possibly the FQDN of the selected PDN GW for the UE and the corresponding PDN connection
PGW PLMN ID	Visited-Network-Identifier	C	This IE shall contain the identifier that allows the home network to identify the PLMN where the PGW is located. It shall be present when the PGW Identity is present and does not contain an FQDN.
Mobility features	MIP6-Feature-Vector	M	This IE shall contain the mobility features used by the PDN GW. The MIP4_SUPPORTED flag shall be set
APN	Service-Selection	C	If present this IE shall contain the Network Identifier part of the APN extracted from the RRQ message. In case it is not received, the 3GPP AAA Server shall assign the received PDN-GW identity to the default APN.
QoS capabilities	QoS-Capability	O	If included in the request message, this IE shall indicate to the 3GPP AAA Server that the PDN GW requests downloading of a static QoS profile for the UE. The PDN GW may include this IE only at the initial attach of the UE.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.
MN-HA security parameter index	MIP-MN-HA-SPI	C	This IE shall contain the MN-HA security parameter index which is used in identifying MN-HA shared key as defined by 3GPP TS 33.402 [19]. It shall be included when the PDN-GW does not have the MN-HA shared key required to verify the MIPv4 RRQ message.

Table 9.1.2.6.1/2: Authorization answer

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Result code	Result-Code	M	This IE shall contain the result of the operation. The possible values of the Result-Code AVP are defined in IETF RFC 3588 [7]. This IE shall be set to DIAMETER_SUCCESS if the authorization of a MAG or the update to the PDN GW address succeeded. It shall be set to DIAMETER_AUTHORIZATION_REJECTED if the authorization of a new MAG or the update of the PDN GW address failed.
Authentication Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_ONLY. See IETF RFC 4072 [5].
Authorized mobility features	MIP6-Feature-Vector	C	The 3GPP AAA Server shall insert this AVP if the authorization was successful. The MIP4_SUPPORTED flag shall be set.
Session time	Session-Timeout	C	If the authorization succeeded, then this IE shall contain the time this authorization is valid for.
QoS resources	QoS-Resources	C	This AVP shall be included only if the QoS-Capability AVP was received in the authorization request and the authorization succeeded. Then the 3GPP AAA Server shall include a static QoS profile in this IE during the UE initial attach if the PDN GW included QoS-Capabilities AVP in the request message and the UE has been provisioned with a static QoS profile. The QoS profile template value in this IE shall be set to 0.
3GPP AAA Server Name	Redirect-Host	C	This information element shall be sent if the Result-Code value is set to DIAMETER_REDIRECT_INDICATION. When the user has previously been authenticated by another 3GPP AAA Server, it shall contain the Diameter identity of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter Base Protocol (IETF RFC 3588 [7]). The command shall contain zero or one occurrence of this information element.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.
MN-HA shared key	MIP-Session-Key	C	This information element contains the MN-HA shared key as defined by 3GPP TS 33.402 [19], it shall be included if the Result-Code value is set to DIAMETER_SUCCESS and the MIP-MN-HA-SPI was sent in the authorization request.
APN Data	APN-Configuration	C	This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS. This AVP shall contain the user profile information. APN-Configuration is a grouped AVP and shall include the following information elements: - APN - Authorized 3GPP QoS profile - APN-AMBR

### 9.1.2.6.2 PDN GW Detailed Behaviour

Upon receipt of a RRQ message from the FA, the PDN GW shall initiate an authorization procedure, by sending an Authorization Request message to the 3GPP AAA Server or to the 3GPP AAA Proxy, with the Auth-Request-Type set to AUTHORIZE\_ONLY, in order to update the PGW Address for the APN, as well as to download any UE specific APN profile information such as IP address allocation information, QoS Information, Session timeouts, Session Idle timeouts, MIPv4 security parameters etc.

If the APN was included in the RRQ message, the PDN GW shall include in the request the APN where the user shall be connected.

The PDN GW Identity shall only be included in the initial request to the 3GPP AAA Server; subsequent authorization messages (due to a handover to a different FA, for instance) shall not include it again.

If the PDN GW does not have a MN-HA shared key associated with the SPI received in the RRQ MN-HA-AE, the PDN GW shall include the SPI in the Authorization Request to the 3GPP AAA Server.

After successful reception of the Authorization Request message, the PDN GW shall check that the Result-Code is set to DIAMETER\_SUCCESS and, if so, it shall use the MN-HA key to verify the MN-HA AE of the RRQ received from the FA.

If the PDN-GW successfully verifies the MN-HA-AE it shall proceed to connect the user to the specified APN, and will send the RRP message to the FA.

#### 9.1.2.6.3 3GPP AAA Server Detailed Behaviour

Upon receipt of the Authorization Request message from the PDN GW, the 3GPP AAA Server shall update the PDN GW information for the APN for the UE on the HSS. If the APN was not received from the PDN GW the 3GPP AAA Server shall assign the received PDN-GW identity to the default APN .

The 3GPP AAA Server must check that the user exists. If the user's data exists in the 3GPP AAA Server, it shall check, whether it also has an active access authorization session for the user.

- If not, the 3GPP AAA Server shall reject the authorization request, including the Result-Code DIAMETER\_AUTHORIZATION\_REJECTED.
- If the 3GPP AAA Server has an existing authorization session,
  - If the APN requested by the PDN GW is included in the list of authorized APNs of the user, then the 3GPP AAA Server shall include the Service-Selection AVP in the authorization answer. If no APN was requested the Service-Selection AVP shall contain the default APN.
  - If the MN-HA-SPI was included in the request and it matches the SPI belonging to a SA of the user then the 3GPP AAA Server shall include the MIP-Session-Key of the SA in the authorization answer and set the Result-Code to DIAMETER\_SUCCESS.
  - If the MN-HA-SPI was included in the request and there is no match with a SPI belonging to a SA of the user then the status code DIAMETER\_AUTHORIZATION\_REJECTED shall be returned to the PDN GW to indicate an unsuccessful authorization.
  - If the APN requested by the PDN GW is not included in the list of authorized APNs, then the status code DIAMETER\_AUTHORIZATION\_REJECTED shall be returned to the PDN GW to indicate an unsuccessful authorization.

If the user's profile does not exist in the 3GPP AAA Server, it shall retrieve the Diameter identity of the 3GPP AAA Server currently serving the user from the HSS following the procedures for subscriber profile download as specified in section 8.1.2.2.2. Depending on the HSS response,

- If the HSS indicates that the user is currently being served by a different 3GPP AAA Server, the 3GPP AAA Server shall respond to the PDG-GW with the Result-Code set to DIAMETER\_REDIRECT\_INDICATION and Redirect-Host set to the Diameter identity of the 3GPP AAA Server currently serving the user (as indicated in the 3GPP-AAA-Server-Name AVP returned in the SWx authentication response from the HSS).
- If the HSS returns DIAMETER\_ERROR\_USER\_UNKNOWN, the 3GPP AAA Server shall return the same error to the PDN GW.
- If the HSS sends the user's profile to the 3GPP AAA Server, the authorization shall be rejected by setting the Result-Code to DIAMETER\_AUTHORIZATION\_REJECTED. The 3GPP AAA Server shall delete the downloaded user profile.

NOTE: The last outcome corresponds to the case that the user has no active access authorization procedure. This is considered as an error situation, e.g. the Trusted Non-3GPP access network may have sent RRQ without authorizing the user.

#### 9.1.2.6.4 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy is required to handle roaming cases in which the PDN GW is located in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy.

On receipt of the authorization answer, the 3GPP AAA Proxy

- shall check locally configured information for the maximum allowed static QoS parameters valid for visitors from the given HPLMN and modify the QoS parameters received from the 3GPP AAA Server, to enforce the policy limitations.
- shall record the state of the connection (i.e. Authorization Successful).

## 9.2 Protocol Specification

### 9.2.1 General

The S6b reference point shall be based on Diameter, as defined in IETF RFC 3588 [7] and contain the following additions and extensions:

- IETF RFC 4005 [4], which defines a Diameter protocol application used for Authentication, Authorization and Accounting (AAA) services in the Network Access Server (NAS) environment.
- IETF RFC 5779 [2], which defines a Diameter extensions and application for PMIPv6 MAG to AAA and LMA to AAA interfaces.
- IETF RFC 5777 [9], which defines attribute value pairs to convey QoS information between Diameter peers.

The PDN GW to 3GPP AAA server or the PDN GW to 3GPP AAA proxy communication shall use the LMA to AAA interface functionality defined in IETF RFC 5779 [2] to update the 3GPP AAA server with PDN GW identity, indicate the protocol selected on S2a or S2b and optionally retrieve mobility related parameters and static QoS profiles, when PMIPv6 or GTPv2 based S2a or S2b is used.

The PDN-GW acts as a LMA when the UE attaches to the EPC using the S2a or S2b reference points and PMIPv6 is used. The PDN GW also follows the LMA to AAA interface functionality defined in IETF RFC 5779 [2] when UE attaches to the EPC using S2a or S2b reference point and GTPv2 is used. The PDN GW acts as HA when the UE attaches to the EPC using the S2a reference point and MIPv4 is used.

In the case the UE attached to the EPC using the S2c reference point, then the communication between the PDN GW and HA, IETF RFC 5778 [11] shall be used. The Application Id to be advertised over the S6b reference point corresponds to the DSMIPv6 "Diameter Mobile IPv6 IKE (MIP6I)" Application Id as defined in IETF RFC 5778 [11].

IKEv2 EAP-based initiator authentication is used for authenticating and authorizing the UE and updating the PDN-GW identity. In this case, the PDN GW or HA shall act as the NAS, as described in 3GPP TS 33.234 [10].

### 9.2.2 Commands

#### 9.2.2.1 Commands for S6b DSMIPv6 Authorization Procedures

##### 9.2.2.1.1 Diameter-EAP-Request (DER) Command

The Diameter-EAP-Request (DER) command, indicated by the Command-Code field set to 268 and the "R" bit set in the Command Flags field, is sent from a PGW to a 3GPP AAA server. The Command Code value and the ABNF are re-used from the IETF RFC 5778 [11].

```

< Diameter-EAP-Request > ::= < Diameter Header: 268, REQ, PXY, 16777272 >
    < Session-Id >
    { Auth-Application-Id }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    { Auth-Request-Type }
    [ RAT-Type ]
    [ User-Name ]
    [ Service-Selection ]
    { EAP-Payload }
    [ MIP6-Feature-Vector ]
    [ MIP6-Agent-Info ]
    [ QoS-Capability ]
    [ Visited-Network-Identifier ]
    [ MIP-Careof-Address ]
    [ AAA-Failure-Indication ]
    *[ Supported-Features ]
    [DER-S6b-Flags]
    [ UE-Local-IP-Address]
    ...
    *[ AVP ]

```

### 9.2.2.1.2 Diameter-EAP-Answer (DEA) Command

The Diameter-EAP-Answer (DEA) command, indicated by the Command-Code field set to 268 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA server to a PGW. The Command Code value and the ABNF are re-used from the IETF RFC 5778 [11].

```

<Diameter-EAP-Answer> ::= < Diameter Header: 268, PXY, 16777272 >
    < Session-Id >
    { Auth-Application-Id }
    { Auth-Request-Type }
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    [ User-Name ]
    [ EAP-Payload ]
    [ EAP-Master-Session-Key ]
    [ Mobile-Node-Identifier ]
    [ APN-Configuration ]
    [ MIP6-Agent-Info ]
    [ MIP6-Feature-Vector ]
    [ 3GPP-Charging-Characteristics ]
    *[ QoS-Resources ]
    *[ Redirect-Host ]
    [ Trace-Info ]
    *[ Supported-Features ]
    ...
    *[ AVP ]

```

## 9.2.2.2 Commands for S6b PMIPv6 or GTPv2 Authorization Procedures

### 9.2.2.2.1 AA-Request (AAR) Command

The AA-Request (AAR) command, indicated by the Command-Code field set to 265 and the "R" bit set in the Command Flags field, is sent from a PDN GW to a 3GPP AAA server. The Command Code value and ABNF are re-used from the IETF RFC 4005 [4] AA-Request command. New AVPs are added using the \*[AVP] extension mechanism in the original ABNF.

```

<AA-Request> ::=
    < Diameter Header: 265, REQ, PXY, 16777272 >
    < Session-Id >
    { Auth-Application-Id }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    { Auth-Request-Type }
    [ User-Name ]
    [ MIP6-Agent-Info ]
    [ MIP6-Feature-Vector ]
    [ Visited-Network-Identifier ]
    [ QoS-Capability ]
    [ Service-Selection ]
    *[ Supported-Features ]
    ...
    *[ AVP ]

```

#### 9.2.2.2.2 AA-Answer (AAA) Command

The AA-Answer (AAA) command, indicated by the Command-Code field set to 265 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA server to a PDN GW. The Command Code value and ABNF are re-used from the IETF RFC 4005 [4] AA-Answer command. New AVPs are added using the \*[AVP] extension mechanism in the original ABNF.

```

<AA-Answer> ::=
    < Diameter Header: 265, PXY, 16777272 >
    < Session-Id >
    { Auth-Application-Id }
    { Auth-Request-Type }
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    ...
    [ MIP6-Feature-Vector ]
    [ Session-Timeout ]
    [ APN-Configuration ]
    [ QoS-Resources ]
    [ AN-Trusted ]
    *[ Redirect-Host ]
    [ Trace-Info ]
    *[ Supported-Features ]
    ...
    *[ AVP ]

```

#### 9.2.2.3 Commands for PDN GW Initiated Session Termination

##### 9.2.2.3.1 Session-Termination-Request (STR) Command

The Session-Termination-Request (STR) command, indicated by the Command-Code field set to 275 and the "R" bit set in the Command Flags field, is sent from a PDN GW to a 3GPP AAA server. The Command Code value and ABNF are re-used from the IETF RFC 3588 [7] Session-Termination-Request command. New AVPs are added using the \*[AVP] extension mechanism in the original ABNF.

```

<Session-Termination-Request> ::= < Diameter Header: 275, REQ, PXY, 16777272 >
< Session-Id >
{ Auth-Application-Id }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Termination-Cause }
[ User-Name ]
...
*[ AVP ]

```

#### 9.2.2.3.2 Session-Termination-Answer (STA) Command

The Session-Termination-Answer (STA) command, indicated by the Command-Code field set to 275 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA server to a PDN GW. The Command Code value and ABNF are re-used from the IETF RFC 3588 [7] Session-Termination-Answer command.

```

<Session-Termination-Answer> ::= < Diameter Header: 275, PXY, 16777272 >
< Session-Id >
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
*[ AVP ]

```

### 9.2.2.4 Commands for 3GPP AAA Server Initiated Session Termination

#### 9.2.2.4.1 Abort-Session-Request (ASR) Command

The Abort-Session-Request (ASR) command, indicated by the Command-Code field set to 274 and the "R" bit set in the Command Flags field, is sent from a 3GPP AAA Server/Proxy to a PDN GW. The ABNF is based on the one in IETF RFC 4005 [4].

```

< Abort-Session-Request > ::= < Diameter Header: 274, REQ, PXY, 16777272 >
< Session-Id >
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Destination-Host }
{ Auth-Application-Id }
[ User-Name ]
[ Auth-Session-State ]
...
*[ AVP ]

```

#### 9.2.2.4.2 Abort-Session-Answer (ASA) Command

The Abort-Session-Answer (ASA) command, indicated by the Command-Code field set to 274 and the "R" bit cleared in the Command Flags field, is sent from a PDN GW to a 3GPP AAA Server/Proxy. The ABNF is based on the one in IETF RFC 4005 [4].

```

< Abort-Session-Answer > ::= < Diameter Header: 274, PXY, 16777272 >
< Session-Id >
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
...
*[ AVP ]

```

### 9.2.2.4.3 Session-Termination-Request (STR) Command

The Session-Termination-Request (STR) command, indicated by the Command-Code field set to 275 and the "R" bit set in the Command Flags field, is sent from an PDN GW to a 3GPP AAA Server/Proxy. The Command Code value and ABNF are re-used from the IETF RFC 3588 [7] Session-Termination-Request command.

```
<Session-Termination-Request> ::= < Diameter Header: 275, REQ, PXY, 16777272 >
< Session-Id >
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Auth-Application-Id }
{ Termination-Cause }
[ User-Name ]
...
*[ AVP ]
```

### 9.2.2.4.4 Session-Termination-Answer (STA) Command

The Session-Termination-Answer (STA) command, indicated by the Command-Code field set to 275 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA Server/Proxy to an PDN GW. The Command Code value and ABNF are re-used from the IETF RFC 3588 [7] Session-Termination-Answer command.

```
<Session-Termination-Answer> ::= < Diameter Header: 275, PXY, 16777272 >
< Session-Id >
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
*[ AVP ]
```

## 9.2.2.5 Commands for S6b MIPv4 FCoA Authorization Procedures

### 9.2.2.5.1 AA-Request (AAR) Command

The AA-Request (AAR) command, indicated by the Command-Code field set to 265 and the "R" bit set in the Command Flags field, is sent from a PDN GW to a 3GPP AAA Server. The Command Code value and ABNF are re-used from the IETF RFC 4005 [4] AA-Request command. New AVPs are added using the \*[AVP] extension mechanism in the original ABNF.

```
<AA-Request> ::= < Diameter Header: 265, REQ, PXY, 16777272 >
< Session-Id >
{ Auth-Application-Id }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Auth-Request-Type }
[ User-Name ]
[ MIP6-Agent-Info ]
[ MIP6-Feature-Vector ]
[ Visited-Network-Identifier ]
[ QoS-Capability ]
[ Service-Selection ]
*[ Supported-Features ]
[MIP-MN-HA-SPI]
...
*[ AVP ]
```

### 9.2.2.5.2 AA-Answer (AAA) Command

The AA-Answer (AAA) command, indicated by the Command-Code field set to 265 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA Server to a PDN GW. The Command Code value and ABNF are re-

used from the IETF RFC 4005 [4] AA-Answer command. New AVPs are added using the \*[AVP] extension mechanism in the original ABNF.

```

<AA-Answer> ::=
    < Diameter Header: 265, PXY, 16777272 >
    < Session-Id >
    { Auth-Application-Id }
    { Auth-Request-Type }
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    ...
    [ MIP6-Feature-Vector ]
    [ Session-Timeout ]
    [ APN-Configuration ]
    [ QoS-Resources ]
    *[ Redirect-Host ]
    *[ Supported-Features ]
    [MIP-Session-Key]
    ...
    *[ AVP ]

```

## 9.2.2.6 Commands for S6b Service Authorization Information Update Procedures

### 9.2.2.6.1 Re-Auth-Request (RAR) Command

The Diameter Re-Auth-Request (RAR) command shall be indicated by the Command-Code field set to 258 and the "R" bit set in the Command Flags field and is sent from a 3GPP AAA Server or 3GPP AAA Proxy to a PDN-GW. The ABNF for the RAR command shall be as follows:

```

< Re-Auth-Request > ::=
    < Diameter Header: 258, REQ, PXY, 16777272 >
    < Session-Id >
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    { Destination-Host }
    { Auth-Application-Id }
    { Re-Auth-Request-Type }
    [ User-Name ]
    [RAR-Flags ]
    ...
    *[ AVP ]

```

### 9.2.2.6.2 Re-Auth-Answer (RAA) Command

The Diameter Re-Auth-Answer (ASA) command shall be indicated by the Command-Code field set to 258 and the "R" bit cleared in the Command Flags field and is sent from a PDN-GW to a 3GPP AAA Server or 3GPP AAA Proxy. The ABNF for the RAA commands shall be as follows:

```

< Re-Auth-Answer > ::=
    < Diameter Header: 258, PXY, 16777272 >
    < Session-Id >
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    [ User-Name ]
    ...
    *[ AVP ]

```

## 9.2.3 Information Elements

### 9.2.3.1 S6b DSMIPv6 procedures

#### 9.2.3.1.1 General

The following table describes the Diameter AVPs defined for the S6b interface protocol in DSMIPv6 mode, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted.

**Table 9.2.3.1.1/1: Diameter S6b AVPs for DSMIPv6**

Attribute Name	AVP Code	Section defined	Value Type	AVP Flag rules			
				Must	May	Should not	Must not
MIP6-Agent-Info	486	9.2.3.2.2	Grouped	M			V,P
MIP6-Feature-Vector	124	9.2.3.2.3	Unsigned64	M			V,P
Visited-Network-Identifier	600	9.2.3.1.2	OctetString	M,V			P
RAR-Flags	1522	9.2.3.1.5	Unsigned32	V			M,P
QoS-Capability	578	9.2.3.2.4	Grouped	M			V,P
QoS-Resources	508	9.2.3.2.5	Grouped	M			V,P
Trace-Info	1505	8.2.3.13	Grouped	V			M,P
Service-Selection	493	5.2.3.5	UTF8String	M			V,P
Trust-Relationship-Update	1515	9.2.3.1.4	Enumerated	V			M,P
DER-S6b-Flags	1523	9.2.3.7	Unsigned32	V			M,P

#### 9.2.3.1.2 Visited-Network-Identifier

The Visited-Network-Identifier AVP contains an identifier that helps the home network to identify the visited network (e.g. the visited network domain name). The Vendor-Id shall be set to 10415 (3GPP).

The AVP shall be encoded as:

```
mnc<MNC>.mcc<MCC>.3gppnetwork.org
```

If MNC consists of only 2 digits, a leading digit "0" shall be added to the MNC value (e.g., if MNC=15 and MCC=234, the value of Visited-Network-Identifier shall be "mnc015.mcc234.3gppnetwork.org").

#### 9.2.3.1.3 Void

#### 9.2.3.1.4 Void

#### 9.2.3.1.5 RAR-Flags

The RAR-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 9.2.3.1.5/1:

**Table 9.2.3.1.5/1: RAR-Flags**

Bit	Name	Description
0	Trust-Relationship-Update-indication	This bit, when set, indicates to the PDN GW that the 3GPP AAA server only initiates the re-authorization procedure send the trust relationship to the PDN GW, and the PDN GW shall not perform any authorization procedure towards the UE.
NOTE: Bits not defined in this table shall be cleared by the sender and discarded by the receiver of the command.		

### 9.2.3.2 S6b PMIPv6 or GTPv2 procedures

#### 9.2.3.2.1 General

The following table describes the Diameter AVPs defined for the S6b interface protocol in PMIPv6 or GTPv2 mode, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted.

**Table 9.2.3.2.1/1: Diameter S6b AVPs for PMIPv6 or GTPv2**

Attribute Name	AVP Code	Section defined	Value Type	AVP Flag rules			
				Must	May	Should not	Must not
MIP6-Agent-Info	486	9.2.3.2.2	Grouped	M			V,P
MIP6-Feature-Vector	124	9.2.3.2.3	Unsigned64	M			V,P
QoS-Capability	578	9.2.3.2.4	Grouped	M			V,P
QoS-Resources	508	9.2.3.2.5	Grouped	M			V,P
Trace-Info	1505	8.2.3.13	Grouped	V			M,P
Service-Selection	493	5.2.3.5	UTF8String	M			V,P
Visited-Network-Identifier	600	9.2.3.1.2	OctetString	M,V			P

#### 9.2.3.2.2 MIP6-Agent-Info

The MIP6-Agent-Info AVP contains the PDN GW identity or (for the chained S2 - PMIP based S8 case) the Serving GW address information. This AVP is defined in IETF RFC 5447 [6]. The identity of PDN GW is either an IP address transported in MIP-Home-Agent-Address or an FQDN transported in MIP-Home-Agent-Host. The PDN GW may use its IP address if a single IP address can be used for all Access Networks and protocols towards the PDN GW. In all other cases the PDN GW shall use its FQDN. MAG/AAA/HSS shall use FQDN if known. The grouped AVP has the following grammar:

```
MIP6-Agent-Info ::=
    < AVP Header: 486 >
    *2[ MIP-Home-Agent-Address ]
    [ MIP-Home-Agent-Host ]
    [ MIP6-Home-Link-Prefix ]
    *[ AVP ]
```

#### 9.2.3.2.3 MIP6-Feature-Vector

The MIP6-Feature-Vector AVP contains a 64 bit flags field of supported mobility capabilities of the NAS. This AVP is defined in IETF RFC 5447 [6]. The NAS may include this AVP in a request message to indicate the mobility capabilities of the NAS to the 3GPP AAA server. Similarly, the Diameter server may include this AVP in an answer message to inform the NAS about which of the NAS indicated capabilities are supported or authorized by the 3GPP AAA Server.

Following capabilities are supported on S6b reference point in PMIPv6 or GTPv2 mode:

- PMIP6\_SUPPORTED
- IP4\_HOA\_SUPPORTED
- GTPv2\_SUPPORTED

#### 9.2.3.2.4 QoS-Capability

The QoS-Capability AVP contains a list of supported Quality of Service profile templates (and therefore the support of the respective parameter AVPs). This AVP is defined in IETF RFC 5777 [9].

#### 9.2.3.2.5 QoS-Resources

The QoS-Resources AVP includes a description of the Quality of Service resources for policing traffic flows. This AVP is defined in IETF RFC 5777 [9].

### 9.2.3.3 S6b Re-used Diameter AVPs

**Table 9.2.3.3/1: S6b re-used Diameter AVPs**

Attribute Name	Reference	Comments
Supported-Features	3GPP TS 29.229 [24]	
Feature-List-ID	3GPP TS 29.229 [24]	See section 9.2.3.4
Feature-List	3GPP TS 29.229 [24]	See section 9.2.3.5
MIP-Careof-Address	IETF RFC 5778 [11]	
UE-Local-IP-Address	3GPP TS 29.212 [23]	

#### 9.2.3.4 Feature-List-ID AVP

The syntax of this AVP is defined in 3GPP TS 29.229 [24]. For this release, the Feature-List-ID AVP value shall be set to 1 for the S6b application.

#### 9.2.3.5 Feature-List AVP

The syntax of this AVP is defined in 3GPP TS 29.229 [24]. A null value indicates that there is no feature used by the S6b application.

NOTE: There are no S6b features defined for this release.

### 9.2.3.6 S6b MIPv4 FACoA procedures

#### 9.2.3.6.1 General

The following table describes the Diameter AVPs defined for the S6b interface protocol in MIPv4 mode, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted.

**Table 9.2.3.6.1/1: Diameter S6b AVPs for MIPv4 FACoA**

Attribute Name	AVP Code	Section defined	Value Type	AVP Flag rules			
				Must	May	Should not	Must not
MIP6-Agent-Info	486	9.2.3.6.2	Grouped	M			V,P
MIP6-Feature-Vector	124	9.2.3.6.3	Unsigned64	M			V,P
QoS-Capability	578	9.2.3.6.4	Grouped	M			V,P
QoS-Resources	508	9.2.3.6.5	Grouped	M			V,P
MIP-MN-HA-SPI	491	9.2.3.6.6	Unsigned32	M			V,P
MIP-Session-Key	343	9.2.3.6.7	OctetString	M			V,P
Service-Selection	493	5.2.3.5	UTF8String	M			V,P

#### 9.2.3.6.2 MIP6-Agent-Info

The MIP6-Agent-Info AVP contains the PDN GW identity. This AVP is defined in IETF RFC 5447 [6]. The identity of PDN GW is either an IP address transported in MIP-Home-Agent-Address or an FQDN transported in MIP-Home-Agent-Host. The PDN GW may use its IP address if a single IP address can be used for all Access Networks and

protocols towards the PDN GW. In all other cases the PDN GW shall use its FQDN. The FA/3GPP AAA Server/HSS shall use FQDN if known. The grouped AVP has the following grammar:

```
MIP6-Agent-Info ::=
    < AVP Header: 486 >
    *2[ MIP-Home-Agent-Address ]
    [ MIP-Home-Agent-Host ]
    [ MIP6-Home-Link-Prefix ]
    *[ AVP ]
```

#### 9.2.3.6.3 MIP6-Feature-Vector

The MIP6-Feature-Vector AVP contains a 64 bit flags field of supported mobility capabilities of the NAS. This AVP is defined in IETF RFC 5447 [6]. The NAS may include this AVP in a request message to indicate the mobility capabilities of the NAS to the 3GPP AAA Server. Similarly, the Diameter server may include this AVP in an answer message to inform the NAS about which of the NAS indicated capabilities are supported or authorized by the 3GPP AAA Server.

Following capabilities are supported on S6b reference point in MIPv4 FACoA mode:

- MIP4\_SUPPORTED

#### 9.2.3.6.4 QoS-Capability

The QoS-Capability AVP contains a list of supported Quality of Service profile templates (and therefore the support of the respective parameter AVPs). This AVP is defined in IETF RFC 5777 [9].

#### 9.2.3.6.5 QoS-Resources

The QoS-Resources AVP includes a description of the Quality of Service resources for policing traffic flows. This AVP is defined in IETF RFC 5777 [9].

#### 9.2.3.6.6 MIP-MN-HA-SPI

The MIP-MN-HA-SPI AVP contains the index of the security association between the Mobile Node and the HA. This AVP is defined in IETF RFC 5778 [11].

#### 9.2.3.6.7 MIP-Session-Key

The MIP-Session-Key AVP contains the MN-HA shared key. This AVP is defined in IETF RFC 4004 [18].

#### 9.2.3.7 DER-S6b-Flags

The DER-S6b-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be asdefined in table 9.2.3.7/1:

**Table 9.2.3.7/1: DER-S6b-Flags**

Bit	Name	Description
0	Initial-Attach-Indicator	This bit, when set, indicates that a UE performs the Initial Attach procedure from non-3GPP access network. When not set, it indicates that a UE performs the Handover procedure.
NOTE: Bits not defined in this table shall be cleared by the sender and discarded by the receiver of the command.		

### 9.2.4 Session Handling

The Diameter protocol between the PDN-GW and the 3GPP AAA Server or the 3GPP AAA Proxy shall always keep session state, and use the same Session-Id parameter for the lifetime of each Diameter session.

A Diameter session shall identify a PDN Connection for a given user and an APN, while the PDN Connection is kept alive in the non-3GPP access. When the PDN Connection is either disconnected on the non-3GPP access, or handed

over to the 3GPP access, the diameter session shall be terminated. In order to indicate that the session state is to be maintained, the Diameter client and server shall not include the Auth-Session-State AVP, either in the request or in the response messages (see IETF RFC 3588 [7]).

---

## 10 Result-Code and Experimental-Result Values

### 10.1 General

This section defines result code values that shall be supported by all Diameter implementations that conform to this specification.

### 10.2 Success

Result codes that fall within the Success category shall be used to inform a peer that a request has been successfully completed. The Result-Code AVP values defined in Diameter Base Protocol RFC 3588 [7] shall be applied.

### 10.3 Permanent Failures

#### 10.3.1 General

Errors that fall within the Permanent Failures category shall be used to inform the peer that the request has failed, and should not be attempted again. The Result-Code AVP values defined in Diameter Base Protocol RFC 3588 [7] shall be applied. When one of the result codes defined here is included in a response, it shall be inside an Experimental-Result AVP and the Result-Code AVP shall be absent.

#### 10.3.2 DIAMETER\_ERROR\_USER\_UNKNOWN (5001)

This result code shall be sent by the HSS to indicate that the user identified by the IMSI is unknown (see 3GPP TS 29.299 [9]).

#### 10.3.3 DIAMETER\_ERROR\_IDENTITY\_NOT\_REGISTERED (5003)

This result code shall be sent by the HSS to indicate that there is currently no 3GPP AAA Server registered for the user (see 3GPP TS 29.299 [9]).

#### 10.3.4 DIAMETER\_ERROR\_ROAMING\_NOT\_ALLOWED (5004)

This result code shall be sent by the HSS to indicate that the subscriber is not allowed to roam in a certain non-3GPP V-PLMN (see 3GPP TS 29.299 [9]).

#### 10.3.5 DIAMETER\_ERROR\_IDENTITY\_ALREADY\_REGISTERED (5005)

This result code shall be sent by the HSS to indicate that the node identity trying to be registered by a 3GPP AAA Server is already registered for a specific user (see 3GPP TS 29.299 [9]).

#### 10.3.6 DIAMETER\_ERROR\_USER\_NO\_NON\_3GPP\_SUBSCRIPTION (5450)

This result code shall be sent by the HSS to indicate that no non-3GPP subscription is associated with the IMSI.

### 10.3.7 DIAMETER\_ERROR\_USER\_NO\_APN\_SUBSCRIPTION (5451)

This result code shall be sent by the 3GPP AAA Server to indicate that the requested APN is not included in the user's profile, and therefore is not authorized for that user.

### 10.3.8 DIAMETER\_ERROR\_RAT\_TYPE\_NOT\_ALLOWED (5452)

This result code shall be sent by the HSS to indicate the RAT type the UE is using is not allowed for the IMSI.

## 10.4 Transient Failures

### 10.4.1 General

Result codes that fall within the transient failures category shall be used to inform a peer that the request could not be satisfied at the time it was received, but may be able to satisfy the request in the future. The Result-Code AVP values defined in Diameter Base Protocol RFC 3588 [7] shall be applied. When one of the result codes defined here is included in a response, it shall be inside an Experimental-Result AVP and the Result-Code AVP shall be absent.

There are no Transient Error codes defined in this specification.

## Annex A (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2008-12	CT#42	CP-080717			V2.0.0 approved in CT#42	2.0.0	8.0.0
2009-03	CT#43	CP-090051	0002	2	Clarification on QoS Resource on S6b	8.0.0	8.1.0
		CP-090051	0003	1	Context Identifier for Update or Removal of PDN GW		
		CP-090051	0007	-	Clarification on the S6b Authorization Procedure for DSMIPv6		
		CP-090051	0009	-	Clarification on DHCPv6/IKEv2 based HA discovery		
		CP-090051	0010	1	Clarification on AAA server authentication/authorization		
		CP-090051	0011	1	Difference of S6b and H2		
		CP-090051	0013	1	STR on HSS/AAA initiated detach over STa		
		CP-090051	0014	1	STR on 3GPP AAA Server initiated detach over SWm		
		CP-090051	0015	1	STR on 3GPP AAA Server initiated detach over S6b		
		CP-090051	0016	1	Multiple 3GPP AAA identities		
		CP-090051	0019	1	User-Name AVP contains only the IMSI		
		CP-090051	0020	-	Removal of APN-Barring-Type Reference		
		CP-090051	0021	1	Charging AVPs		
		CP-090051	0022	1	MIP6-Agent-Info Definition and Usage		
		CP-090051	0023	1	REAUTHENTICATION_FAILURE Correction		
		CP-090051	0025	1	Definition of Server-Assignment-Type values		
		CP-090051	0026	-	Multiple Occurrences of SIP-Auth-Data-Item AVP		
		CP-090051	0028	1	Using MIP6-Agent-Info for SGW address		
		CP-090051	0029	1	MIP6-Agent-Info corrections		
		CP-090051	0030	1	Trace activation in PDN GW over the SWx and S6b interfaces		
		CP-090051	0031	1	Signalling VPLMN Trust of non-3GPP AN		
		CP-090051	0033	-	Corrections in Visited Network Identifier definitions		
		CP-090051	0034	2	Service Authorization Information update on S6b when using DSMIP		
		CP-090051	0035	4	STa/SWa clarifications		
		CP-090051	0036	1	IP address authorization corrections		
		CP-090051	0037	2	SWm Authentication Correction		
		CP-090051	0039	1	SWm corrections - others		
		CP-090051	0040	3	SWm Service Authorization Information Update corrections		
		CP-090051	0041	5	Combined Authentication and authorization procedure on SWm		
		CP-090051	0042	2	S6b related corrections		
		CP-090051	0044	2	Corrections to S6b/HA section 9		
		CP-090039	0045	3	User to HSS resolution		
		CP-090051	0080	1	Corrections to STR procedures for AAA_UNKNOWN_SESSION_ID		
CP-090051	0081	1	Corrections to S6b STR procedures				
CP-090236	0082	1	PDN GW update for Wildcard APN				
CP-090051	0083	-	RFC 5447 References				
2009-06	CT#44	CP-090289	0084	1	Use of Access-Restriction-Data AVP	8.1.0	8.2.0
		CP-090289	0085	-	Difference between S6b and H2		
		CP-090289	0086	1	Corrections to 29.273		
		CP-090289	0087	1	Inclusion of static IP address		
		CP-090289	0088	1	Home Agent discovery		
		CP-090289	0090	-	Incorrect command for user profile updates		
		CP-090289	0092	1	Home Agent discovery		
		CP-090289	0093	1	Formatting of APN in Service-Selection AVP		
		CP-090289	0094	-	Update of AVP Codes		
		CP-090289	0096	1	STa/SWa separation correction		
		CP-090289	0097	-	SWa corrections		
		CP-090289	0098	1	STa re-authorization and re-authentication		
		CP-090289	0101	2	SWa re-authentication		
		CP-090289	0102	1	Adding APN-OI-Replacement		
		CP-090289	0103	2	HA reallocation clarification		
2009-09	CT#45	CP-090537	0105	2	Correction on APN-OI-Replacement	8.2.0	8.3.0
		CP-090537	0106	-	Correction on the Description of Mobility Features over S6b		
		CP-090537	0111	-	EAP-AKA' IETF RFC Reference		
		CP-090537	0112	-	Removal of Remaining Editor Notes		

		CP-090537	0113	1	MIP6_SPLIT flag removal		
		CP-090537	0108	3	Support of optimized idle mode mobility		
		CP-090537	0115	-	E-UTRAN - eHRPD Connectivity and Interworking Reference		
		CP-090537	0116	2	Detailed behaviour in error cases		
		CP-090537	0118	1	Application IDs		
		CP-090537	0119	-	Service-Selection AVP Code		
		CP-090537	0120	-	PDN-Type AVP		
		CP-090537	0121	1	Clarifications on PGW Handling on S6b/H2		
2009-09	CT#45	CP-090562	0117	1	Emergency Support in AAA interfaces	8.3.0	9.0.0
2009-12	CT#46	CP-090793	0122	2	APN level APN-OI-Replacement	9.0.0	9.1.0
		CP-090774	0126	3	Correction of Allowed PDN Types		
		CP-090774	0128	2	Incorrect HSS behaviour on deregistration		
		CP-090774	0130	2	MIP6 Agent Info		
		CP-090774	0132	-	Nonce		
		CP-090774	0136	-	3GPP AAA Server detailed behaviour at HSS Initiated Update of User Profile		
		CP-090774	0140	2	Static PDN GW		
		CP-090787	0141	-	Removal of Definition of APN-Configuration		
		CP-090774	0143	1	PGW deregistration via S6b		
		CP-090774	0145	1	Add Supported-Features AVP to STa/SWa		
		CP-090774	0147	-	Add Supported-Features AVP to SWm		
		CP-090774	0149	-	Add Supported-Features AVP to SWx		
		CP-090774	0151	-	Add Supported-Features AVP to S6b		
		CP-090774	0153	1	Correction of Application ID		
		CP-090774	0155	1	Error Handling		
		CP-090774	0157	-	HSS/AAA-Initiated Disconnection		
2010-03	CT#47	CP-10024	0163	1	Correction in Subscription-ID	9.1.0	9.2.0
		CP-10024	0165	-	NAI decoration and realm-based routing clarifications		
		CP-10024	0167	-	IETF References update		
		CP-10024	0169	-	Permanent User Identity		
		CP-10024	0171	1	Static PDN GW		
		CP-10024	0173	-	QoS AVP Codes		
		CP-10024	0175	-	Indication of PLMN ID of the selected PGW		
		CP-10044	0176	-	Context-Identifier in Registration Request		
2010-06	CT#48	CP-100290	0179	1	Corrections on Session Termination between the PGW and the AAA	9.2.0	9.3.0
		CP-100277	0180	-	Corrections to implementation of CR 128 and CR 175		
		CP-100277	0181	-	PGW Identity upon successful authorization on SWm		
2010-06	CT#48	CP-100443	0184	-	Ambiguity of Presence Conditions of IEs and AVP ABNF	9.3.0	9.4.0
		CP-100457	0188	-	IETF References		
		CP-100457	0189	1	SWm missing AVPs		
2010-09	CT#49	CP-100603	0187	1	Removal of Invalid Reference	9.4.0	10.0.0
2010-12	CT#50	CP-100679	0197	1	Correcting PDN GW behaviour for S6b	10.0.0	10.1.0
		CP-100698	0194	1	Update APN and PDN GW in the 3GPP AAA Server on SWx		
		CP-100698	0195	1	Update APN and PDN GW in Non-3GPP IP Access over the STa & SWm interfaces		
		CP-100686	0196	3	SWm and S6b procedures for GTP based S2b		
		CP-100707	0200	-	MIP6 Feature Vector flags assignment		
		CP-100707	0203	-	SWx AVP Bits Definition		
		CP-100707	0206	-	Visited-Network-Identifier Data Type		
2011-03	CT#51	CP-110051	0210	1	Usage of Auth-Request-Type in response messages	10.1.0	10.2.0
		CP-110073	0208	2	Correction on PGW PLMN ID		
2011-06	CT#52	CP-110359	0214	1	Trace-Depth-List correction	10.2.0	10.3.0
		CP-110359	0217	1	MIPv4 security parameters on the STa and S6b interfaces		
		CP-110359	0221	1	PGW Update		
		CP-110359	0223	1	APN Configuration for SWx		
		CP-110360	0219	-	Authentication Timeout		
2011-12	CT#54	CP-110778	0227	1	S6b session handling after handover to 3GPP access	10.3.0	10.4.0
		CP-110778	0235	1	Incorrect access name on SWa		
		CP-110793	0228	5	Correction on Trust Relationship Indication		
		CP-110793	0238	-	Implementation Error of CR 196 R3		
2011-12	CT#54	CP-110812	0225	4	SWx Restoration	10.4.0	11.0.0
2012-03	CT#55	CP-120016	0257	1	Wrong Command Code in STa AA-Answer	11.0.0	11.1.0
		CP-120020	0251	2	Authorize the requested home address types		
		CP-120020	0260	-	Content of Service-Selection AVP		
		CP-120040	0245	1	Wildcard APN in the user subscription		
		CP-120040	0253	-	Permanent User Identity in SWm Authentication and Authorization Answer		
		CP-120040	0255	-	Encoding of Visited-Network-Identifier AVP		
		CP-120040	0256	-	Re-Authorization Errors		

		CP-120042	0254	1	Permanent User Identity at SWa		
		CP-120044	0240	1	PDN GW reallocation based on UE's location		
2012-06	CT#56	CP-120225	0243	3	Trust Relationship Indication	11.1.0	11.2.0
		CP-120238	0264	-	S6b procedures for GTP based S2a		
		CP-120247	0265	2	Missing IE in TS 29.273		
		CP-120247	0266	-	Emergency scenario for STa interface		
		CP-120247	0267	2	Visited Network Identifier		
		CP-120247	0278	1	Network Name		
		CP-120238	0268	6	STa & SWd procedures for GTP S2a & Trusted WLAN access		
		CP-120238	0269	1	Default APN for 'Trusted WLAN access'		
		CP-120238	0270	3	Informing Serving SSID to the AAA Server		
		CP-120238	0271	1	Avoiding registration of PDN-GW identity for TWAN		
		CP-120238	0275	1	Clarifications on TWAN behaviour		
		CP-120237	0273	2	PDN GW selection for S2c during tunnel establishment		
2012-09	CT#57	CP-120441	0285	-	Update of IETF draft status to RFC	11.2.0	11.3.0
		CP-120447	0287	2	PGW selection in eHRPD for SIPTO		
		CP-120461	0272	3	Recovering from AAA Server failure		
		CP-120474	0279	1	Transport Access Type AVP for BBAI		
		CP-120477	0280	1	NSWO-Capability & NSWO-Authorization AVPs		
		CP-120477	0281	-	Access Type for TWAN access		
		CP-120656	0292	1	Reference list correction to align with the corrected TS 29.212 title		
2012-12	CT#58	CP-120711	0307	1	Removal of AVP Encryption	11.3.0	11.4.0
		CP-120733	0293	-	Repeat information for Trusted non-3GPP access network		
		CP-120733	0300	5	Matching WLAN-ID between Selected WLAN ID and TWAN Access Info		
		CP-120733	0301	1	Update of draft-ietf-radext-ieee802ext reference		
		CP-120747	0294	-	Correction on Auth-Request-Type		
		CP-120747	0295	-	Description of Result IE		
		CP-120728	0297	2	Information Elements for SWa interface		
		CP-120728	0299	1	Session ID in the SWm Authorization procedure		
		CP-120750	0302	1	Trace Info for PGW		
		CP-120750	0303	1	Add the definition of trace-reference		
		CP-120741	0309	2	Use of Flag instead of Enumerated AVPs		
2013-03	CT#59	CP-130022	0314	2	About EAP-AKA' challenge message	11.4.0	11.5.0
		CP-130022	0315	1	TWAN Authorization when HE-SSID is not provided		
		CP-130022	0317	-	Missing P-Bit settings in Information Element tables		
		CP-130022	0316	-	Presence condition of PGW-ID AVP in S6b AAR command		
2013-06	CT#60	CP-130288	0313	3	New DER-S6b-flags on S6b interface	11.5.0	11.6.0
		CP-130288	0325	1	MIP4 supported flag		
		CP-130288	0323	1	3GPP AAA Proxy behavior		
		CP-130288	0321	1	Definition of HA-APN		
		CP-130288	0320	2	Trust relationship for PGW		
		CP-130293	0318	2	UE local IP address for SWm or S6b		
2013-09	CT#61	CP-130459	0337	-	Category of Authentication Data Information Element in SWx/MAR command	11.6.0	11.7.0
		CP-130472	0328	2	3GPP AAA Proxy detailed Behaviour for SWa		
		CP-130472	0330	1	Correct the general description about SWd and SWa		
2013-12	CT#62	CP-130602	0350	-	EAP Payload	11.7.0	11.8.0
		CP-130606	0340	-	IMSI for BBF in trusted S2c case		
		CP-130616	0342	5	NSWO via the trusted WLAN		
		CP-130616	0344	1	VPLMN trust relationship indicator		
		CP-130616	0355	2	EPC Access Authorization		
2014-03	CT#63	CP-140023	0365	1	Replacement of IETF WLAN AVPs	11.8.0	11.9.0
2014-12	CT#66	CP-140754	0393	2	Leading Digit of User-Name AVP	11.9.0	11.10.0

---

## History

<b>Document history</b>		
V11.3.0	October 2012	Publication
V11.4.0	January 2013	Publication
V11.5.0	April 2013	Publication
V11.6.0	July 2013	Publication
V11.7.0	September 2013	Publication
V11.8.0	December 2013	Publication
V11.9.0	March 2014	Publication
V11.10.0	January 2015	Publication