ETSI TS 123 402 V13.6.0 (2016-07)

Universal Mobile Telecommunications System (UMTS);
LTE;
Architecture enhancements for non-3GPP accesses
(3GPP TS 23.402 version 13.6.0 Release 13)

Reference
RTS/TSGS-0223402vd60

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/standards-search

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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

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 2016.
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 (https://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**", "**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 11
Introduction 11
1 Scope 12
2 References 12
3 Definitions, Symbols and Abbreviations 15
3.1 Definitions 15
3.2 Abbreviations 16
4 Architecture Model and Concepts 17
4.1 Concepts 17
4.1.0 General Concepts 17
4.1.1 General Concepts for Interworking Between E-UTRAN and CDMA2000 17
4.1.2 General Concepts for Interworking Between 3GPP Accesses and WiMAX 18
4.1.3 IP Mobility Management Selection Principles 18
4.1.3.1 Static Configuration of Inter-technology Mobility Mechanism 18
4.1.3.2 Networks Supporting Multiple IP Mobility Mechanisms 18
4.1.3.2.1 IP Mobility Management Selection During Initial Attach to a Non-3GPP Access 19
4.1.3.2.2 IPMS solutions 20
4.1.3.2.3 IP Mobility Management Selection on Handover between accesses 20
4.1.4 Trusted/untrusted non-3GPP access network detection 21
4.1.5 Non-seamless WLAN offload 21
4.2 Architecture Reference Model 21
4.2.1 Architecture for 3GPP Accesses with PMIP-based S5/S8 21
4.2.2 Non-roaming Architectures for EPS 22
4.2.3 Roaming Architectures for EPS 24
4.3 Network Elements 28
4.3.1 Access Networks 28
4.3.1.1 E-UTRAN 28
4.3.1.2 Trusted and Untrusted Non-3GPP Access Network 28
4.3.2 MME 29
4.3.3 Gateway 29
4.3.3.1 General 29
4.3.3.2 Serving GW 29
4.3.3.3 PDN GW 30
4.3.4 ePDG 30
4.3.5 PCRF 31
4.3.5.1 Home PCRF 31
4.3.5.2 Visited PCRF 31
4.4 Reference Points 31
4.4.1 List of Reference Points 31
4.4.2 Reference Point Requirements 33
4.4.2.1 S5 Reference Point Requirements 33
4.4.2.2 Void 33
4.4.2.3 Void 33
4.4.2.4 Void 33
4.5 High Level Functions 34
4.5.1 PDN GW Selection Function for Non-3GPP Accesses for S2a and S2b 34
4.5.1a PDN GW Selection Function for eHRPD with SIPTO support 35
4.5.2 PDN GW Selection Function for S2c 35
4.5.3 Serving GW Selection Function for Non-3GPP Accesses 36

4.5.4 ePDG Selection....36
4.5.4.1 General....36
4.5.4.2 ePDG FQDNs Construction....36
4.5.4.3 UE Configuration By HPLMN....37
4.5.4.4 UE ePDG Selection Procedure....37
4.5.4.5 ePDG Selection with DNS-based Discovery of Regulatory Requirements....38
4.5.4a ePDG selection for emergency bearer services....39
4.5.4a.1 General....39
4.5.4a.2 Static selection....39
4.5.4a.3 Dynamic selection.....39
4.5.5 PCRF Selection....39
4.5.6 DSMIPv6 Home Link Detection Function....40
4.5.7 IMS Emergency Session Support....40
4.5.7.1 Overview....40
4.5.7.2 IMS Emergency Session Support over WLAN access to EPC....40
4.5.7.2.1 Introduction....40
4.5.7.2.2 Architecture Reference Model for Emergency Services....41
4.5.7.2.3 PDN GW selection function for Emergency Services....41
4.5.7.2.4 QoS for Emergency Services....42
4.5.7.2.5 PCC for Emergency Services....42
4.5.7.2.6 IP Address Allocation....42
4.5.7.2.7 Handling of PDN Connections for Emergency Bearer Services....42
4.5.7.2.8 Network provided WLAN Location Information....42
4.5.8 APN congestion Control Function for eHRPD....44
4.5.9 GTP-C signalling based Load and Overload Control for trusted and untrusted WLAN....44
4.5.9.1 GTP-C load control....44
4.5.9.2 GTP-C overload control....44
4.6 Identities....46
4.6.1 User Identification....46
4.6.2 EPS bearer identity with GTP based S2b/S2a....46
4.7 IP Address Allocation....46
4.7.1 IP Address Allocation with PMIP-based S5/S8....46
4.7.2 IP Address Allocation in Trusted Non-3GPP IP Access using PMIPv6 on S2a....50
4.7.3 IP Address Allocation in Untrusted Non-3GPP IP Access using PMIPv6 or GTP on S2b....53
4.7.4 IP Address Allocation using S2c....54
4.7.5 IPv6 Prefix Delegation using S2c....54
4.7.6 IPv6 Prefix Delegation using PMIP-based S5/S8....54
4.8 Network Discovery and Selection....56
4.8.0 General Principles....56
4.8.1 Architecture for Access Network Discovery Support Functions....57
4.8.2 Network Elements....58
4.8.2.1 Access Network Discovery and Selection Function (ANDSF)....58
4.8.2.1.1 General....58
4.8.2.1.2 Inter-System Mobility Policy....58
4.8.2.1.3 Access Network Discovery Information....59
4.8.2.1.4 Inter-System Routing Policy....59
4.8.2.1.5 Inter-APN Routing Policy....60
4.8.2.1.6 WLAN Selection Policy....61
4.8.2.1.7 VPLMNs with preferred WLAN Selection Rules....62
4.8.2.1.8 Void....63
4.8.2.1.9 Home Network Preferences....63
4.8.2.1.10 Visited Network Preferences....63
4.8.2a UE Procedures....64
4.8.2a.1 Selection of Active ANDSF Rules....64
4.8.2a.2 UE Behavior Based on the ANDSF Information....65
4.8.2b WLAN Selection based on WLANSP....67
4.8.3 Reference Points....69
4.8.4 ANDSF Discovery....69
4.8.5 Void....69
4.8.6 Support of RAN Assistance Information....69
4.8.6.1 General....69
4.8.6.2 ANDSF Rules Utilizing RAN Assistance Information....69

4.8.6.3 Evaluation of ANDSF Rules with RAN Validity Conditions 70
4.8.6.4 Co-existence with RAN Rules 71
4.8.7 Support of LWA, LWIP and RCLWI 72
4.8.7.1 General 72
4.8.7.2 Co-existence with LWA and RCLWI 72
4.8.7.3 Co-existence with LWIP 73
4.9 Authentication and Security 73
4.9.1 Access Authentication in non-3GPP Accesses 73
4.9.2 Tunnel Authentication 73
4.10 QoS Concepts 74
4.10.1 General 74
4.10.2 Void 74
4.10.3 The EPS Bearer with PMIP-based S5/S8 and E-UTRAN access 74
4.10.4 Application of PCC in the Evolved Packet System 75
4.10.5 PDN connectivity service with GTP based S2b 75
4.11 Charging for Non-3GPP Accesses 76
4.12 Multiple PDN Support 77
4.13 Detach principles 78

5 Functional Description and Procedures for 3GPP Accesses with PMIP-based S5/S8 78
5.1 Control and User Plane Protocol Stacks 78
5.1.1 Void 78
5.1.2 General 78
5.1.3 Control Plane 79
5.1.3.1 Serving GW - PDN GW 79
5.1.4 User Plane 80
5.1.4.1 UE – PDN GW User Plane with E-UTRAN 80
5.1.4.2 UE – PDN GW User Plane with 2G access via the S4 Interface 81
5.1.4.3 UE – PDN GW User Plane with 3G Access via the S4 Interface 82
5.1.4.4 UE – PDN-GW User Plane with 3G Access via the S12 Interface 82
5.2 Initial E-UTRAN Attach with PMIP-based S5 or S8 83
5.3 Detach for PMIP-based S5/S8 86
5.4 Dedicated Bearer Procedures for E-UTRAN Access with PMIP-based S5/S8 88
5.4.1 General 88
5.4.2 Dedicated Bearer Activation 89
5.4.3 Bearer Modification with Bearer QoS Update 89
5.4.3.1 PCC Initiated Bearer Modification with Bearer QoS Update 89
5.4.3.2 HSS-Initiated Subscribed QoS Modification 89
5.4.4 Dedicated Bearer Modification without Bearer QoS Update 90
5.4.5 Dedicated Bearer Deactivation 91
5.4.5.1 PCC-initiated Dedicated Bearer Deactivation 91
5.4.5.2 Void 91
5.4.5.3 MME-initiated Dedicated Bearer Deactivation 91
5.5 UE-initiated Resource Request and Release 92
5.6 Multiple PDN Support with PMIP-based S5/S8 93
5.6.1 UE requested PDN connectivity 93
5.6.2 PDN Disconnection 95
5.6.2.1 UE, MME or S-GW initiated PDN Disconnection 95
5.6.2.2 PDN-GW-initiated PDN Disconnection 96
5.7 Handover and Tracking area Update Procedures for PMIP-based S5/S8 Interface 97
5.7.0 Intra-LTE TAU and Inter-eNodeB Handover without Serving GW Relocation 97
5.7.1 Intra-LTE TAU and Inter-eNodeB Handover with Serving GW Relocation 98
5.7.2 TAU/RAU or Handover between GERAN A/Gb Mode or UTRAN Iu Mode and E-UTRAN 99
5.8 ME Identity Check Procedures for PMIP-based S5/S8 102
5.9 UE-triggered Service Request for PMIP-based S5/S8 102
5.10 PMIP-based S5/S8 procedures for GERAN/UTRAN over S4 103
5.10.1 General 103
5.10.2 GPRS procedures that update the PDN GW 104
5.10.3 UE allocated resources 105
5.10.4 Network allocated resources 105
5.10.5 UE released resources 106
5.10.6 PDN GW released resources 106

5.10.7 Attach....106
5.10.8 Detach interaction using S4....107
5.10.9 Interaction with CGI/SAI reporting using S4....107
5.10.10 RAU Procedure Support....107
5.11 PDN GW initiated IPv4 address Delete Procedure....107
5.12 Location Change Reporting Procedure for PMIP-based S5/S8....109
5.13 Support for Machine Type Communications (MTC)....109
5.13.1 General....109
5.13.2 PDN GW control of overload....110
5.13.3 Usage of low access priority indicator....110

6 Functional Description and Procedures for Trusted Non-3GPP IP Accesses....110
6.1 Control and User Plane Protocol Stacks....110
6.1.1 Protocol Stacks for S2a....110
6.1.2 Protocol Stacks for S2c over Trusted Non-3GPP IP Accesses....112
6.2 Initial Attach on S2a....112
6.2.1 Initial Attach Procedure with PMIPv6 on S2a and Anchoring in PDN GW....112
6.2.2 Void....115
6.2.3 Initial Attach procedure with MIPv4 FACoA on S2a and Anchoring in PDN-GW....115
6.2.4 Initial Attach Procedure with PMIPv6 on S2a and Chained S2a and PMIP-based S8....118
6.3 Initial Attach Procedure with DSMIPv6 on S2c in Trusted Non-3GPP IP Access....119
6.4 Detach and PDN Disconnection for S2a....122
6.4.1 UE/Trusted Non-3GPP IP Access Network Initiated Detach and UE/Trusted Non-3GPP IP Access requested PDN Disconnection Procedure with PMIPv6....122
6.4.1.1 Non-Roaming, Home Routed Roaming and Local Breakout Case....122
6.4.1.2 Chained PMIP-based S8-S2a Roaming Case....124
6.4.2 HSS/AAA Initiated Detach Procedure with PMIPv6....125
6.4.2.1 Non-Roaming, Home Routed Roaming and Local Breakout Case....125
6.4.2.2 Chained PMIP-based S8-S2a Roaming Case....126
6.4.3 UE-initiated Detach Procedure and UE-Requested PDN Disconnection Procedure with MIPv4 FACoA....127
6.4.4 Network Initiated Detach Procedure with MIPv4 FACoA....128
6.4.5 HSS/AAA-initiated detach procedure with MIPv4 FACoA....129
6.5 Detach and PDN Disconnection for S2c in Trusted Non-3GPP IP Access....130
6.5.1 General....130
6.5.2 UE-initiated PDN disconnection Procedure....131
6.5.3 HSS / AAA-initiated Detach Procedure....132
6.5.4 PDN GW-initiated PDN Disconnection Procedure....133
6.6 Network-initiated Dynamic PCC....134
6.6.1 Network-initiated Dynamic PCC on S2a....134
6.6.2 Network-initiated Dynamic PCC for S2c over Trusted Non-3GPP IP Access....135
6.7 UE-initiated Resource Request and Release....136
6.7.1 UE-initiated Resource Request and Release on S2a....136
6.7.2 UE-initiated Resource Request for S2c over Trusted Non-3GPP IP Access....137
6.8 UE-initiated Connectivity to Additional PDN....137
6.8.1 UE-initiated Connectivity to Additional PDN with PMIPv6 on S2a....137
6.8.1.0 General....137
6.8.1.1 Non-Roaming, Home Routed Roaming and Local Breakout Case....137
6.8.1.2 Chained PMIP-based S8-S2a Roaming Case....139
6.8.2 UE-initiated Connectivity to Additional PDN with MIPv4 FACoA on S2a....140
6.8.3 UE-initiated Connectivity to Additional PDN from Trusted Non-3GPP IP Access with DSMIPv6 on S2c....141
6.9 Void....141
6.10 PDN GW reallocation upon attach on S2c....142
6.11 S2c Bootstrapping via DSMIPv6 Home Link over a Trusted Access....143
6.12 PDN GW initiated Resource Allocation Deactivation....143
6.12.1 PDN GW initiated Resource Allocation Deactivation with S2a PMIP....143
6.12.2 PDN GW initiated Resource Allocation Deactivation with S2a MIPv4....144
6.12.3 PDN GW initiated Resource Allocation Deactivation for Chained PMIP-based S8-S2a Roaming....145
6.12.4 Void....146
6.13 PDN GW initiated IPv4 address Delete Procedure....146
6.14 Non-3GPP access initiated IPv4 address Delete Procedure....147

6.15 IPv4 Home Address Release Procedure for S2c 148
6.16 Enhanced security support for S2c 150
6.16.1 General 150
6.16.2 Activation of enhanced security for S2c 150
6.16.3 De-activation of enhanced security for S2c 151

7 Functional Description and Procedures for Un-trusted Non-3GPP IP Accesses 152
7.1 Control and User Plane Protocol Stacks 152
7.1.1 Protocol Options for S2b 152
7.1.2 Protocol Options for S2c over Un-trusted Non-3GPP IP Accesses 153
7.2 Initial Attach on S2b 154
7.2.1 Initial Attach with PMIPv6 on S2b 154
7.2.2 Void 156
7.2.3 Initial Attach Procedure with PMIPv6 on S2b and Chained S2b and PMIP-based S8 156
7.2.4 Initial Attach with GTP on S2b 156
7.2.5 Initial Attach for emergency session (GTP on S2b) 158
7.3 Initial Attach Procedure for S2c in Untrusted Non-3GPP IP Access 160
7.4 Detach and PDN Disconnection for S2b 162
7.4.1 UE/ePDG-initiated Detach Procedure and UE-Requested PDN Disconnection with PMIPv6 on S2b 162
7.4.1.1 Non-Roaming, Home Routed Roaming and Local Breakout Case 162
7.4.1.2 Chained PMIP-based S8-S2b Roaming Case 164
7.4.2 HSS/AAA-initiated Detach Procedure with PMIPv6 on S2b 164
7.4.2.1 Non-Roaming, Home Routed Roaming and Local Breakout Case 164
7.4.2.2 Chained PMIP-based S8-S2b Roaming Case 164
7.4.3 UE/ePDG-initiated Detach Procedure and UE-Requested PDN Disconnection with GTP on S2b 165
7.4.3.1 Non-Roaming, Home Routed Roaming and Local Breakout Case 165
7.4.4 HSS/AAA-initiated Detach Procedure with GTP on S2b 166
7.4.4.1 Non-Roaming, Home Routed Roaming and Local Breakout Case 166
7.5 Detach and PDN Disconnection for S2c in Un-trusted Non-3GPP IP Access 167
7.5.1 General 167
7.5.2 UE-Initiated PDN disconnection Procedure 167
7.5.3 HSS / AAA-initiated Detach Procedure 168
7.5.4 PDN GW-initiated PDN Disconnection Procedure 170
7.6 UE-initiated Connectivity to Additional PDN 171
7.6.1 UE-initiated Connectivity to Additional PDN with PMIPv6 on S2b 171
7.6.2 UE-initiated Connectivity to Additional PDN from Un-trusted Non-3GPP IP Access with DSMIPv6 on S2c 172
7.6.3 UE-initiated Connectivity to Additional PDN with GTP on S2b 172
7.7 Void 173
7.8 S2c Bootstrapping via DSMIPv6 Home Link over an Un-Trusted Access 173
7.9 PDN GW initiated Resource Allocation Deactivation 174
7.9.1 PDN GW initiated Resource Allocation Deactivation with PMIPv6 on S2b 174
7.9.2 PDN GW initiated Resource Allocation Deactivation with GTP on S2b 175
7.10 Dedicated S2b bearer activation with GTP on S2b 176
7.11 S2b bearer modification with GTP on S2b 177
7.11.1 PDN GW initiated bearer modification 177
7.11.2 HSS Initiated Subscribed QoS Modification 179

8 Handovers without Optimizations Between 3GPP Accesses and Non-3GPP IP Accesses 180
8.1 Common Aspects for Handover without Optimizations for Multiple PDNs 180
8.2 Handovers between non-3GPP IP access with PMIPv6 on S2a/S2b and 3GPP Access 181
8.2.1 Handover from Trusted or Untrusted Non-3GPP IP Access with PMIPv6 on S2a/S2b to 3GPP Access 181
8.2.1.1 General Procedure for GTP based S5/S8 for E-UTRAN Access 181
8.2.1.2 Using PMIP-based S5/S8 184
8.2.1.3 General Procedure for GTP-based S5/S8 for UTRAN/GERAN 187
8.2.1.4 Using PMIP-based S5/S8 190
8.2.2 3GPP Access to Trusted Non-3GPP IP Access Handover with PMIPv6 on S2a 191
8.2.3 3GPP Access to Untrusted Non-3GPP IP Access Handover with PMIPv6 on S2b 194
8.2.4 Void 197
8.2.5 Void 197
8.2.6 Non-3GPP IP Access to 3GPP Access Handover with PMIPv6 on S2a/b for Chained PMIP-based S8 197

8.2.7 3GPP Access to Non-3GPP IP Access Handover with PMIPv6 on S2a/b for Chained PMIP-based S8..198
8.2.8 Void 201
8.2.9 Void 201
8.3 Handover from 3GPP access to Trusted Non-3GPP IP Access with MIPv4 FACoA on S2a 202
8.3b Handover from Trusted Non-3GPP IP Access with MIPv4 FACoA on S2a to 3GPP access 204
8.4 Handovers with DSMIPv6 on S2c 205
8.4.1 Trusted or Untrusted Non-3GPP IP Access with DSMIPv6 over S2c to 3GPP Access Handover 205
8.4.2 3GPP Access to Trusted Non-3GPP IP Access Handover with DSMIPv6 over S2c 206
8.4.3 3GPP Access to Untrusted Non-3GPP IP Access Handover with DSMIPv6 over S2c 208
8.5 Handover with Access Network Discovery and Selection 211
8.5.1 Handover between 3GPP Access and Trusted / Untrusted Non-3GPP IP Access with access network discovery and selection 211
8.6 Handovers between non-3GPP IP access with GTP on S2b and 3GPP Access 212
8.6.1 Handover from Untrusted Non-3GPP IP Access with GTP on S2b to 3GPP Access 212
8.6.1.1 General Procedure for GTP based S5/S8 for E-UTRAN Access 212
8.6.1.2 General Procedure for GTP-based S5/S8 for UTRAN/GERAN 214
8.6.2 Handover from 3GPP access to untrusted Non-3GPP IP Access with GTP on S2b 215
8.6.2.1 3GPP Access to Untrusted Non-3GPP IP Access Handover with GTP on S2b 215

9 Handovers with Optimizations Between E-UTRAN Access and CDMA2000 Access 218
9.1 Architecture and Reference Points 218
9.1.1 Architecture for Optimized Handovers between E-UTRAN Access and cdma2000 HRPD Access 218
9.1.2 Reference Points 219
9.1.2.1 Reference Point List 219
9.1.2.2 Requirements for the S101 Reference Point 219
9.1.2.3 S101 Protocol Stack 220
9.1.2.4 S101 Session Identifier 220
9.1.2.5 Requirements for the S103 Reference Point 220
9.1.2.6 S103 Protocol Stack 220
9.2 Overview of Handover Procedures 221
9.2.1 General 221
9.2.2 Support for HO of IMS Emergency Sessions 221
9.3 Optimized Active Handover: E-UTRAN Access to cdma2000 HRPD Access 222
9.3.0 Introduction 222
9.3.1 Pre-registration Phase 222
9.3.2 Handover Phase 225
9.4 Optimized Idle-mode Mobility: E-UTRAN Access to cdma2000 HRPD Access 228
9.5 Void 229
9.5.1 Void 229
9.5.2 Void 229
9.6 Void 229
9.7 S101 Tunnel Redirection Procedure 229

10 Handovers with Optimizations Between 3GPP Accesses and Mobile WiMAX 231
10.1 Optimizations for network-controlled dual radio handover 231
10.1.1 General Principles 231

11 Handover Optimizations Applicable to All Non-3GPP Accesses 231

12 Interactions Between HSS and AAA Server 232
12.0 General 232
12.1 Location Management Procedures 232
12.1.1 UE Registration Notification 232
12.1.2 AAA-initiated UE De-registration Notification 233
12.1.3 HSS-initiated UE De-registration Notification 233
12.1.4 PDN GW Identity Notification from AAA Server 234
12.1.5 PDN GW Identity Notification from MME/SGSN 235
12.2 Subscriber Profile Management Procedures 235
12.2.1 HSS-initiated User Profile Update Procedure 236
12.2.2 AAA-initiated Provide User Profile Procedure 236
12.3 Authentication Procedures 237

13 Information Storage 237
13.0 General 237

13.1 HSS 237
13.2 MME 237
13.3 S-GW 237
13.4 Handling of Wild Card APN 238
14 Void 238
15 Functional Description and Procedures for 3GPP Accesses with S2c 238
15.1 S2c Bootstrapping via DSMIPv6 Home Link 238
16 Architecture, Functional description and Procedures for GTP and PMIPv6 based S2a over Trusted WLAN Access 240
16.1 Architecture and Functional Description 240
16.1.1 Architecture 240
16.1.2 High level functions 242
16.1.3 Reference points 244
16.1.3.1 STa reference point 244
16.1.3.2 SWw reference point 244
16.1.3.3 S2a reference point 245
16.1.4 Protocol Stacks 245
16.1.4A Control Plane 247
16.1.4A.1 Negotiation of connection mode 247
16.1.4A.2 EAP-AKA' extensions 248
16.1.4A.3 PDN connection management Control plane 248
16.1.4A.3.1 WLAN Control Protocol (WLCP) 248
16.1.4B User plane 249
16.1.4B.1 User plane for PDN connection 249
16.1.5 IP address allocation 249
16.1.5.1 General 249
16.1.5.2 IP address allocation in Transparent Single-Connection Mode 250
16.1.5.3 IP address allocation in Single-Connection Mode 250
16.1.5.4 IP address allocation in Multi-Connection Mode 251
16.1.6 Bearer model for PDN connectivity service with GTP based S2a 252
16.1.7 Access Network information reporting in case of a TWAN Access 252
16.2 Initial Attach in WLAN on S2a 254
16.2.1 Initial Attach in WLAN on GTP S2a 254
16.2.2 Initial Attach in WLAN on PMIP S2a 259
16.2.3 HSS retrieval of information about an UE from the TWAN serving that UE 260
16.3 Detach and PDN disconnection in WLAN on S2a 261
16.3.1 Detach and PDN disconnection in WLAN on GTP S2a 261
16.3.1.1 UE/TWAN Initiated Detach and UE/TWAN requested PDN Disconnection Procedure in WLAN on GTP S2a 261
16.3.1.2 HSS/AAA Initiated Detach Procedure in WLAN on GTP S2a 262
16.3.2 Detach and PDN disconnection in WLAN on PMIP S2a 263
16.3.2.1 UE/TWAN Initiated Detach and UE/TWAN requested PDN Disconnection Procedure in WLAN on PMIP S2a 263
16.3.2.2 HSS/AAA Initiated Detach Procedure in WLAN on PMIP S2a 263
16.4 PDN GW initiated Resource Allocation Deactivation in WLAN on S2a 264
16.4.1 PDN GW initiated Resource Allocation Deactivation in WLAN on GTP S2a 264
16.4.2 PDN GW initiated Resource Allocation Deactivation in WLAN on PMIP S2a 265
16.5 Dedicated bearer activation in WLAN on GTP S2a 265
16.6 Network-initiated bearer modification in WLAN on GTP S2a 267
16.6.1 PDN GW Initiated Bearer Modification 267
16.6.2 HSS Initiated Bearer Modification 268
16.7 Detach in WLAN on S2a for Multi-connection Mode 269
16.7.1 Detach in WLAN on GTP S2a 269
16.7.1.1 UE/TWAN Initiated Detach Procedure in WLAN on GTP S2a 269
16.7.1.2 HSS/AAA Initiated Detach Procedure in WLAN on GTP S2a 270
16.7.2 Detach in WLAN on PMIP S2a 270
16.7.2.1 UE/TWAN Initiated Detach Procedure in WLAN on PMIP S2a 270
16.7.2.2 HSS/AAA Initiated Detach Procedure in WLAN on PMIP S2a 271
16.8 UE Initiated PDN connectivity request procedure in WLAN on S2a for Multi-connection Mode 271
16.8.1 Supporting GTP S2a 271

16.8.2 Supporting PMIP S2a 273
16.9 UE/TWAN Initiated PDN disconnection for Multi-connection Mode 274
16.9.1 Supporting GTP S2a 274
16.9.2 Supporting PMIP S2a 275
16.10 Handover procedure from 3GPP access to WLAN on S2a 275
16.10.1 Handover procedure from 3GPP access to WLAN on S2a in single-connection mode 275
16.10.1.1 Handover in single-connection mode from 3GPP access to WLAN on GTP S2a 275
16.10.1.2 Handover in single-connection mode from 3GPP access to WLAN on PMIP S2a 278
16.10.2 Handover procedure from 3GPP access to WLAN on S2a in multi-connection mode 279
16.10.2.1 Handover in multi-connection mode from 3GPP access to WLAN on GTP S2a 279
16.10.2.2 Handover in multi-connection mode from 3GPP access to WLAN on PMIP S2a 280
16.11 Handover procedure from WLAN on S2a to 3GPP access 281

17 E-UTRAN-HRPD Inter-RAT SON Support 281
17.1 Architecture and Interface 281
17.1.1 Architecture for E-UTRAN-HRPD Inter-RAT SON Support 281
17.1.2 Reference Points 282
17.1.2.1 Reference Point List 282
17.1.2.2 Requirements for the S121 interface 282
17.1.2.3 S121 Protocol Stack 282

Annex A (informative): GTP - PMIP Roaming 283

A.1 Direct Peering Scenario 283

A.2 Proxy-based interworking 285

Annex B (informative): Guidance for Contributors to this Specification 287

Annex C (informative): Handover Flows Between Non-3GPP Accesses 289

C.1 General 289

C.2 Trusted Non-3GPP IP Access to Trusted Non-3GPP IP Access with DSMIPv6 over S2c Handover 289

C.3 Untrusted Non-3GPP IP Access with PMIPv6 to Trusted Non-3GPP IP Access with PMIPv6 Handover in the Non-Roaming Scenario 290

C.4 Trusted/Untrusted Non-3GPP IP Access with DSMIPv6 to Trusted Non-3GPP IP Access with PMIPv6 Handover in the Non-Roaming Scenario 291

C.5 Handover Between Two Untrusted Non-3GPP IP Accesses Connected to the Same ePDG 293

C.6 Handovers between APs of a Non-3GPP Trusted WLAN Access on S2a 294

Annex D (informative): Void 295

Annex E (informative): Gateway Relocation in the Trusted Non-3GPP IP Access 296

E.1 Gateway Relocation with PMIPv6 on S2a 296

E.2 Gateway Relocation with MIPv4 FACoA on S2a 297

Annex F (informative): Deployment of Non-3GPP Trusted WLAN Access on S2a 299

Annex G (informative): Change History 300

History 301

Foreword

This Technical Specification has been produced by the 3rd 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

Guidance to Readers of this Specification

In order to reduce the number of procedures in this specification certain editorial practices have been adopted. Though there are many independent factors, such as variants of S5/S8/S2b and attachment cases, these are in essence quite similar. So, rather than presenting the permutations of these factors separately and thereby needlessly repeating normative text, conventions have been adopted to combine this information in single procedures.

The S5 and S8 reference points in the EPC architecture have been defined to have both a GTP and PMIP variant. The GTP variant is documented in TS 23.401 [4], while the PMIP variant is documented in this specification. Every effort has been made to eliminate duplication of normative text common to both specifications. Many figures in this specification refer to procedures in TS 23.401 [4] to achieve this end. Common procedures between TS 23.401 [4] and TS 23.402 (this specification), are represented in this specification in figures by text in shaded box(es) that reference the appropriate figure and steps in TS 23.401 [4]. The details of the common steps are only captured in TS 23.401 [4].

The S2b reference point in the EPC architecture has also been defined to have both a GTP and PMIP variant. Both variants are documented in this specification. Every effort has been made to eliminate duplication of normative text common to both variants. Figures for the GTP variant of S2b refer to figures defined for the PMIP variant of S2b to achieve this end. Common procedures for both variants are represented in figures for GTP based S2b by text in shaded box(es) that reference the appropriate figure and steps defined for PMIP based S2b. The details of the common steps are only captured for the PMIP variant of S2b.

Attachment cases (as discussed in clauses 6.2.1 and 7.2.1) have been combined in a single figure. The different attachment cases can be accommodated by including optional items in the flows, for instance, a vPCRF that is only employed during when a roaming case or LBO is specified.

Multiple APN interactions may occur for many of the procedures defined in this specification. These interactions complicate the flows by introducing certain operations that may occur multiple times. Rather than produce unique flows for this purpose, we indicate where this possibility may occur in text.

1 Scope

This document specifies the stage 2 service description for providing IP connectivity using non-3GPP accesses to the Evolved 3GPP Packet Switched domain. In addition, for E-UTRAN and non-3GPP accesses, the specification describes the Evolved 3GPP PS Domain where the protocols between its Core Network elements are IETF-based.

ITU-T Recommendation I.130 [2] describes a three-stage method for characterisation of telecommunication services, and ITU-T Recommendation Q.65 [3] defines stage 2 of the method.

The specification covers both roaming and non-roaming scenarios and covers all aspects, including mobility between 3GPP and non 3GPP accesses, policy control and charging, and authentication, related to the usage of non-3GPP accesses.

TS 23.401 [4] covers architecture aspects common to the Evolved 3GPP Packet Switched domain.

The procedures defined in the present document for WLAN access selection and PLMN selection replace the corresponding I-WLAN procedures specified in TS 23.234 [5].

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] ITU-T Recommendations I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[3] ITU-T Recommendation Q.65: "The unified functional methodology for the characterization of services and network capabilities".

[4] 3GPP TS 23.401: "General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[5] 3GPP TS 23.234: "3GPP System to Wireless Local Area Network (WLAN) Interworking; System Description".

[6] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description Stage 2".

[7] Void.

[8] IETF RFC 5213: "Proxy Mobile IPv6".

[9] IETF RFC 5996, "Internet Key Exchange Protocol Version 2 (IKEv2)".

[10] IETF RFC 5555: "Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)".

[11] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[12] IETF RFC 5944, "IP Mobility Support for IPv4, revised".

[13] Void.

[14] Void.

[15] IETF RFC 4282, "The Network Access Identifier".

[16] 3GPP TS 23.003: "Numbering, addressing and identification".

[17] IETF RFC 5844: "IPv4 Support for Proxy Mobile IPv6".

[18] IETF RFC 4555, "IKEv2 Mobility and Multihoming Protocol (MOBIKE)"

[19] 3GPP TS 23.203: "Policy and Charging Control Architecture".

[20] 3GPP TS 22.278: "Service requirements for evolution of the system architecture".

[21] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[22] IETF RFC 4877, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture".

[23] IETF RFC 2784, "Generic Routing Encapsulation (GRE)".

[24] IETF RFC 2890, "Key and Sequence Number Extensions to GRE".

[25] IETF RFC 3543, "Registration Revocation in Mobile IPv4".

[26] Void.

[27] Void.

[28] IETF RFC 2131: "Dynamic Host Configuration Protocol".

[29] IETF RFC 4039: "Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)".

[30] IETF RFC 3736: "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6".

[31] Void.

[32] 3GPP2 C.S0024-A v2.0: "cdma2000 High Rate Packet Data Air Interface Specification".

[33] Void.

[34] IETF RFC 2794: "Mobile IP Network Access Identifier Extension for IPv4".

[35] Void.

[36] Void.

[37] Void.

[38] IETF RFC 4861: "Neighbor Discovery for IP Version 6 (IPv6)".

[39] IETF RFC 5446: "Service Selection for Mobile IPv4".

[40] IETF RFC 5026: "Mobile IPv6 bootstrapping in split scenario".

[41] IETF RFC 6611: "Mobile IPv6 (MIPv6) Bootstrapping for the Integrated Scenario".

[42] Void.

[43] IETF RFC 5779: "Diameter Proxy Mobile IPv6: Mobile Access Gateway and Local Mobility Anchor Interaction with Diameter Server".

[44] IETF RFC 5447: "Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction".

[45] 3GPP TS 33.402: "3GPP System Architecture Evolution: Security aspects of non-3GPP accesses".

[46] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".

[47] 3GPP TS 22.011: "Service accessibility".

[48] IETF RFC 3948: "UDP Encapsulation of IPsec ESP Packets".

[49] 3GPP2 C.S0087-0: "E-UTRAN - HRPD and CDMA2000 1x Connectivity and Interworking: Air Interface Aspects".

[50] IETF RFC 4739: "Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2) Protocol".

[51] 3GPP2 X.S0057-B: "E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects".

[52] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification".

[53] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode".

[54] Void.

[55] 3GPP TS 23.261: "IP Flow Mobility and seamless WLAN offload; Stage 2".

[56] IETF RFC 6276: "DHCPv6 Prefix Delegation for Network Mobility (NEMO)".

[57] 3GPP TS 29.274: "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3".

[58] IETF RFC 4862: "IPv6 Stateless Address Autoconfiguration".

[59] IETF RFC 4861: "Neighbor Discovery for IP version 6 (IPv6)".

[60] 3GPP TS 23.221: "Architectural requirements".

[61] 3GPP TS 32.240: "Charging architecture and principles".

[62] 3GPP TS 32.251: "Charging management; Packet Switched (PS) domain charging".

[63] 3GPP TS 29.281: "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)".

[64] 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".

[65] IEEE Std 802.1X-2004: "IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control".

[66] IETF RFC 791: "Internet Protocol".

[67] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".

[68] IETF RFC 6106: "IPv6 Router Advertisement Options for DNS Configuration".

[69] 3GPP TS 36.413: "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)".

[70] 3GPP TS 29.276: "3GPP Evolved Packet System (EPS); Optimized handover procedures and protocols between E-UTRAN access and cdma2000 HRPD Access; Stage 3".

[71] IETF RFC 768: "User Datagram Protocol".

[72] IETF RFC 5448: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[73] 3GPP TS 24.312: "Access Network Discovery and Selection Function (ANDSF) Management Object (MO)".

[74] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[75] WiFi Alliance Technical Committee, Hotspot 2.0 Technical Task Group: "Hotspot 2.0 (Release 2) Technical Specification", 2013-04-09.

Editor's Note: The above document cannot be formally referenced until it is publically available in accordance with TR 21.801 and until it is designated as an approved specification.

[76] 3GPP TS 24.244: "Wireless LAN control plane protocol for trusted WLAN access to EPC".

[77] ETSI ES 282 004 v3.4.1 (2010): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)".

[78] 3GPP TS 25.331: "Universal Terrestrial Radio Access (UTRA); Radio Resource Control (RRC); Protocol specification".

[79] 3GPP TS 36.304: "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode".

[80] 3GPP TS 25.304: "User Equipment (UE) procedures in idle mode and procedures for cell reselection in connected mode".

[81] IETF RFC 3633: "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6".

[82] IETF RFC 7148: "Prefix Delegation Support for Proxy Mobile IPv6".

[83] 3GPP TS 23.167: "IP Multimedia Subsystem (IMS) emergency sessions".

[84] 3GPP TS 36.463: "Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and Wireless LAN (WLAN); Xw application protocol (XwAP)".

3 Definitions, Symbols and Abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 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 TR 21.905 [1].

SectorID or Sector Address Identifier: This identifier is defined in 3GPP2 C.S0024-A v2.0 [32] and is used to identify an HRPD AN. The Network operator shall set the value of the SectorID according to the rules specified in clause 14.9 of 3GPP2 C.S0024-A v2.0 [32].

IFOM capable UE: A UE that is capable of routing different IP flows to the same PDN connection through different access networks (see TS 23.261 [55]).

Inter-APN routing capable UE: A UE that is capable of routing IP flows across multiple simultaneously active IP interfaces, each one associated with a specific APN. These interfaces may be linked to different access networks or to the same access network.

Non-seamless WLAN offload capable UE: A UE that is capable of non-seamless WLAN offload as defined in clause 4.1.5.

MAPCON capable UE: A UE that is capable of routing different simultaneously active PDN connections through different access networks.

Transparent Single-Connection mode: A communication mode between a UE and a trusted WLAN (TWAN) where the TWAN may set up non-seamless WLAN offload or an S2a tunnel without explicit request from the UE.

Single-Connection mode: A communication mode that is capable to support only a single connection at a time between a UE and a trusted WLAN (TWAN) . This connection can be used either for Non-Seamless WLAN Offload (as defined in clause 4.1.5) or for PDN connectivity. The use of the Single-Connection mode and the associated parameters of the connection (e.g. for NSWO, for PDN connectivity, APN, etc.) can be negotiated during authentication over TWAN.

Multi-Connection mode: A communication mode that is capable to support a single or multiple connections at a time between a UE and a trusted WLAN. One connection can be used for Non-Seamless WLAN Offload (as defined in clause 4.1.5) and one or more simultaneous connections can be used for PDN connectivity. The use of the Multi-Connection mode can be negotiated during authentication over TWAN and the requested PDN connection can be setup with the WLCP protocol for PDN connectivity.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

ANDSF	Access Network Discovery and Selection Function
DSMIPv6	Dual-Stack MIPv6
CPICH	Common Pilot Channel
DMNP	Delegated Mobile Network Prefix
EAP	Extensible Authentication Protocol
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
FACoA	Foreign Agent Care-of-Address
FQDN	Fully Qualified Domain Name
GW	Gateway
H-ANDSF	Home-ANDSF
HBM	Host-based Mobility
HRPD	High Rate Packet Data
HS-GW	HRPD Serving Gateway
IFOM	IP Flow Mobility
IKEv2	Internet Key Exchange version 2
IPMS	IP Mobility management Selection
LMA	Local Mobility Anchor
LWA	LTE-WLAN Radio Level Aggregation
LWIP	LTE-WLAN Radio Level Integration with IPsec Tunnel
MAG	Mobile Access Gateway
MAPCON	Multi Access PDN Connectivity
MIPv4	Mobile IP version 4
MIPv6	Mobile IP version 6
MME	Mobility Management Entity
MTC	Machine-Type Communications
NBM	Network-based Mobility
NSWO	Non-seamless WLAN Offload
OPI	Offload Preference Indicator
P-GW	PDN Gateway
PMIP/PMIPv6	Proxy Mobile IP version 6
RIM	RAN Information Management
RCLWI	RAN Controlled WLAN Interworking
RSRP	Reference Signal Received Power
RSSI	Received Signal Strength Indicator
SectorID	Sector Address Identifier
S-GW	Serving GW
SON	Self-Configuring and self-Optimizing network
TWAP	Trusted WLAN AAA Proxy
TWAG	Trusted WLAN Access Gateway
TWAN	Trusted WLAN Access Network
UICC	Universal Integrated Circuit Card
UWAN	Untrusted WLAN Access Network

V-ANDSF Visited-ANDSF
WiMAX Worldwide Interoperability for Microwave Access
WLCP WLAN Control Protocol

4 Architecture Model and Concepts

4.1 Concepts

4.1.0 General Concepts

The EPS supports the use of non-3GPP IP access networks to access the EPC.

The EPS supports network-based mobility management mechanism based on PMIP or GTP and host-based mobility management mechanism (e.g., MIP) over S2 reference points.

The EPS supports IETF-based network-based mobility management mechanism (i.e. PMIP) over S5 and S8 reference points.

When host-based mobility protocol (DSMIPv6 [10]) is used within the EPS and the UE camps on a 3GPP access network, in this specification the UE is considered to be on its home link.

NOTE: A scenario where the UE in EPS uses a host based mobility protocol with a HA that is outside the EPS is out of the scope of 3GPP specification.

The mobility management procedures specified to handle mobility between 3GPP and non 3GPP accesses shall include mechanisms to minimize the handover latency due to authentication and authorization for network access. This applies to UEs either supporting simultaneous radio transmission capability or not supporting it. EPS-based mobility between GERAN/UTRAN access and non-3GPP access requires S4-based SGSNs.

For multiple PDN-GWs connecting to the same PDN, all the PDN GWs shall support the same mobility protocols.

The EPC supports local breakout of traffic whether a roaming subscriber is accessing the EPC via a 3GPP or a non 3GPP access network according to the design principles described in clause 4.1 of TS 23.401 [4].

4.1.1 General Concepts for Interworking Between E-UTRAN and CDMA2000

The mobility management procedures specified to handle mobility between E-UTRAN and CDMA2000 accesses (as required by TS 22.278 [20]) shall include mechanisms to minimize the service interruption during handover and where possible support bidirectional service continuity.

- This applies to UEs supporting either single or dual radio capability.
- The mobility management procedures should minimize any performance impacts to the UE and the respective accesses, for example, UE battery consumption and network throughput.
- The mobility management procedures should minimize the coupling between the different accesses allowing independent protocol evolution in each access.

The operator may configure an indicator in HSS which is delivered to the BBERF in HSGW within the Charging Characteristics and used by the BBERF to not establish the Gateway Control Session during the IP-CAN session establishment procedure.

NOTE 1: When the Gateway Control Session session is not used, certain functions such as location information report, APN-AMBR update and dedicated bearer establishment are impacted.

NOTE 2: The decision to not establish the Gateway Control Session session applies for the life time of the IP-CAN session.

NOTE 3: The indicator in the HSS is operator specific, therefore it can only be used in non-roaming cases.

4.1.2 General Concepts for Interworking Between 3GPP Accesses and WiMAX

The mobility management procedures specified to handle mobility between 3GPP Accesses and WiMAX (as required by TS 22.278 [20]) shall include mechanisms to minimize the service interruption during handover and where possible support bidirectional service continuity.

- This applies to UEs supporting either single or dual radio capability.
- The mobility management procedures should minimize any performance impacts to the UE and the respective accesses, for example, UE battery consumption and network throughput.
- The mobility management procedures should minimize the coupling between the different accesses allowing independent protocol evolution in each access.

Furthermore, the mobility management procedures specified to handle mobility between 3GPP accesses and WiMAX should minimize the impact on legacy systems (i.e. UTRAN and GERAN).

4.1.3 IP Mobility Management Selection Principles

The Mobility mechanisms supported between 3GPP and non-3GPP accesses within an operator and its roaming partner's network would depend upon operator choice.

4.1.3.1 Static Configuration of Inter-technology Mobility Mechanism

For networks deploying a single IP mobility management mechanism, the statically configured mobility mechanism can be access type and/or roaming agreement specific. The information about the mechanism to be used in such scenario is expected to be provisioned into the terminal (or the UICC) and the network. IP session continuity between 3GPP and non-3GPP access types may not be provided in this case if there is a mismatch between what the UE expects and what the network supports. For example service continuity may not be possible if the user switches to a terminal supporting a different IP mobility management mechanism than provisioned in the network.

NOTE: The mismatch case where a trusted non-3GPP network or ePDG only supports DSMIPv6 and the UE does not, may lead to a situation where the UE receives a local IP address in the trusted non-3GPP access network or ePDG, but gains no PDN connectivity in the EPC. Depending on operator policy and roaming agreements, IP connectivity may be provided using this local IP address to access services (e.g. internet access) in the trusted non-3GPP network. However, any such use of the local IP address where the user traffic does not use the EPC is not described in this specification.

4.1.3.2 Networks Supporting Multiple IP Mobility Mechanisms

IP Mobility management Selection (IPMS) consist of two components:

- IP MM protocol selection between Network Based Mobility (NBM) and Host based mobility (HBM - MIPv4 orDSMIPv6).
- Decision on IP address preservation if NBM is selected.

IPMS does not relate to the selection between PMIPv6 and GTP over S5/S8/S2b/S2a.

Upon initial attachment to a 3GPP access, no IPMS is necessary since connectivity to a PDN GW is always established with a network-based mobility mechanism.

Upon initial attachment to a trusted non-3GPP access or ePDG and upon handover from 3GPP to a trusted non-3GPP access or ePDG, IPMS is performed before an IP address is allocated and provided to the UE.

The UE support for a specific IP Mobility Management protocol and/or IP address preservation mechanism for inter-access mobility may be known by the network-based on explicit indication from the UE.

Upon attachment to a trusted non-3GPP access or ePDG, if the access network (supporting at least NBM) is not aware of the UE capabilities and the home and access network's policies allow the usage of NBM, then NBM is used for establishing connectivity for the UE to the EPC.

When a NBM mechanism is used for establishing connectivity in the target access upon inter-access mobility, IP address preservation for session continuity based on NBM may take place as per PMIPv6 specification (RFC 5213 [8]) or according to clause 8.6 for GTP, and additionally based on the knowledge in the network of UE's capability (if available) to support NBM. Such knowledge may be based on an explicit indication from the UE upon handover that IP address preservation based on NBM management can be provided.

IP address preservation for session continuity based on HBM may take place if the network is aware of the UE capability to support DSMIPv6 or MIPv4. Such knowledge may be based on an indication to the target trusted non-3GPP access or ePDG from the HSS/AAA (e.g. in case of DSMIPv6, the UE performed S2c bootstrap before moving to the target trusted non-3GPP access or ePDG). In such a case, the trusted non-3GPP access network or ePDG provides the UE with a new IP address, local to the access network if IP mobility management protocol selected is DSMIPv6. In that case, in order to get IP address preservation for session continuity, the UE shall use DSMIPv6 over S2c reference point. This IP address shall be used as a care-of address for DSMIPv6. If the IP mobility management protocol selected is MIPv4, the address provided to the UE by the non-3GPP access network is a FACoA and IP address preservation is performed over S2a using MIPv4 FACoA procedures.

The final decision on the mobility management mechanism is made by the HSS/AAA upon UE authentication in the trusted non-3GPP access system or ePDG (both at initial attachment and handover), based on the information it has regarding the UE, local/home network capabilities and local/home network policies. If the UE provided an explicit indication of the supported mobility mechanisms, the network shall provide an indication to the UE identifying the selected mobility management mechanism.

Support of different IP mobility management protocols at local/home network is known by the AAA/HSS in one of the following ways:

- through static pre-configuration, or
- through indication of the supported IP mobility management protocols (NBM and/or MIPv4 FA CoA mode) by the trusted non-3GPP access system or ePDG as part of the AAA exchange for UE authentication.

Upon selecting a mobility management mechanism, as part of the AAA exchange for UE authentication in the trusted non-3GPP access system or ePDG, the HSS/AAA returns to the trusted non-3GPP access system or ePDG an indication on whether a local IP address shall be allocated to the UE, or if instead NBM shall be used to establish the connectivity, or the HSS/AAA returns to the trusted non-3GPP access system an indication that the address of the MIPv4 Foreign Agent shall be provided to the UE.

IPMS is performed in the following scenarios:

- Upon initial attach to a trusted non-3GPP access or ePDG, the IPMS is performed to decide how to establish IP connectivity for the UE.
- Upon handover without optimization from a 3GPP access to a non-3GPP access, the IPMS is performed to decide how to establish IP connectivity for the UE over the trusted non-3GPP access or ePDG.
- Upon change of access between a non-3GPP access and a 3GPP access or between two non-3GPP accesses, if the IP MM protocol used to provide connectivity to the UE over the trusted non-3GPP access or ePDG is a NBM protocol, then a decision is performed on whether IP address preservation is provided or not as per PMIPv6 specification, (RFC 5213 [8]) or according to clause 8.6 for GTP and additionally based on the knowledge in the network of UE's capability (if available) to support NBM.

4.1.3.2.1 IP Mobility Management Selection During Initial Attach to a Non-3GPP Access

The IPMS decision is performed as described in the following:

- If the UE indicates DSMIPv6 support only, and the network supports and selects DSMIPv6, the trusted non-3GPP access network or ePDG provides a local IP address to the UE to be used as CoA for DSMIPv6/S2c.
- If the UE indicates MIPv4 support only, and the network supports and selects MIPv4, then the trusted non-3GPP access network provides a FACoA to the UE.
- If the UE indicates DSMIPv6 or MIPv4 support only, and the network selects NBM for providing connectivity, then NBM is used for providing connectivity.

- If the UE does not indicate any capabilities, it is assumed that the UE is not able to support DSMIPv6 or MIPv4, and NBM is used for providing connectivity if the network supports NBM.

4.1.3.2.2 IPMS solutions

On handover to 3GPP access, UE shall request for IP address preservation by setting Request Type flag to "handover" during the attach procedure.

NOTE: UE requests for address preservation if S2c is used over source access network or MIPv4 FACoA is used to connect over source access network or UE is capable of Network address preservation.

When the UE provides an indication of its supported mobility modes either during initial attach or on handover, the UE provides such information to the entity performing IPMS during network access authentication, for trusted non-3GPP accesses, or during authentication for tunnel establishment with ePDG, for untrusted non-3GPP accesses.

The network then makes the decision on what mobility protocol to be used for connectivity as described in further clauses depending on the scenario.

4.1.3.2.3 IP Mobility Management Selection on Handover between accesses

On handover to non-3GPP accesses, the IPMS decision is performed as described in the following:

a. If the UE only indicates NBM support between the two access technologies involved in the handover and the network supports NBM between those two access technologies involved in the handover, then NBM is used for providing connectivity, and IP address preservation is provided with S2a or S2b procedures.

b. If the UE indicates DSMIPv6 support and the network supports and selects DSMIPv6, the trusted non-3GPP access network or ePDG provides a local IP address to the UE to be used as CoA for DSMIPv6, and IP address preservation is provided with S2c procedures.

c. If the UE indicates DSMIPv6 support only and the network does not support DSMIPv6, then NBM is used for providing basic connectivity to the existing PDN GW if NBM is supported by the trusted non-3GPP access network or ePDG. In this case, the decision for IP address preservation is made as per PMIPv6 specification, (RFC 5213 [8]) or according to clause 8.6 for GTP.

d. If the UE indicates support for both NBM and DSMIPv6, and the network based on policies selects NBM to establish the connectivity, then NBM is used to establish connectivity, and IP address preservation is provided with S2a or S2b procedures.

e. If the UE indicates support for both NBM and DSMIPv6, and the network based on policies selects DSMIPv6 to establish the connectivity, then the trusted non-3GPP access network or ePDG provides a local IP address to the UE to be used as CoA for DSMIPv6, and IP address preservation is provided with S2c procedures.

f. If the UE does not indicate any capabilities, then NBM is used for establishing connectivity if NBM is supported by the trusted non-3GPP access network or ePDG. In this case, the decision for IP address preservation is made as per PMIPv6 specification, (RFC 5213 [8]) or according to clause 8.6 for GTP.

NOTE 1: In case of bullet c and f, PMIPv6 specification allows two options:

a) Preserve the IP address based on a timer; If the connection through the old access system is not torn down before the timer expires then a new prefix is assigned, or

b) Immediately assign a new prefix.

This decision can be based on operator's policies.

NOTE 2: If prior to the handover, the UE was attached to a non-3GPP access with DSMIPv6, bullets a. and c. are considered not to apply.

NOTE 3: The PDN GW capability of supporting NBM or DSMIPv6 or MIPv4 should be considered in IP Mobility Mode Selection.

The UE indication of DSMIPv6 support may be implicit, e.g. having bootstrapped a security association via the old access network. The same applies to NBM, since the network can collect information about NBM support from other sources.

On handover to 3GPP access, the only decision that needs to be made is whether IP address preservation needs to be provided or not.

4.1.4 Trusted/untrusted non-3GPP access network detection

During initial attach or handover attach a UE needs to discover the trust relationship (whether it is a Trusted or Untrusted Non-3GPP Access Network) of the non-3GPP access network in order to know which non-3GPP IP access procedure to initiate. The trust relationship of a non-3GPP access network is made known to the UE with one of the following options:

1) If the non-3GPP access supports 3GPP-based access authentication, the UE discovers the trust relationship during the 3GPP-based access authentication.

2) The UE operates on the basis of pre-configured policy in the UE.

4.1.5 Non-seamless WLAN offload

Non-seamless WLAN offload is an optional capability of a UE supporting WLAN radio access in addition to 3GPP radio access.

A UE supporting non-seamless WLAN offload may, while connected to WLAN access, route specific IP flows via the WLAN access without traversing the EPC. These IP flows are identified via user preferences, the Local Operating Environment Information defined in TS 23.261 [55], and via policies that may be statically pre-configured by the operator on the UE, or dynamically set by the operator via the ANDSF. For such IP flows the UE uses the local IP address allocated by the WLAN access network and no IP address preservation is provided between WLAN and 3GPP accesses.

For performing the non-seamless WLAN offload, the UE needs to acquire a local IP address on WLAN access, and it is not required to connect to an ePDG.

Also, in the case the WLAN access is EPC connected, it is possible for a UE which also supports seamless WLAN offload to perfom seamless WLAN offload for some IP flows and non seamless WLAN offload for some other IP flows simultaneously.

4.2 Architecture Reference Model

4.2.1 Architecture for 3GPP Accesses with PMIP-based S5/S8

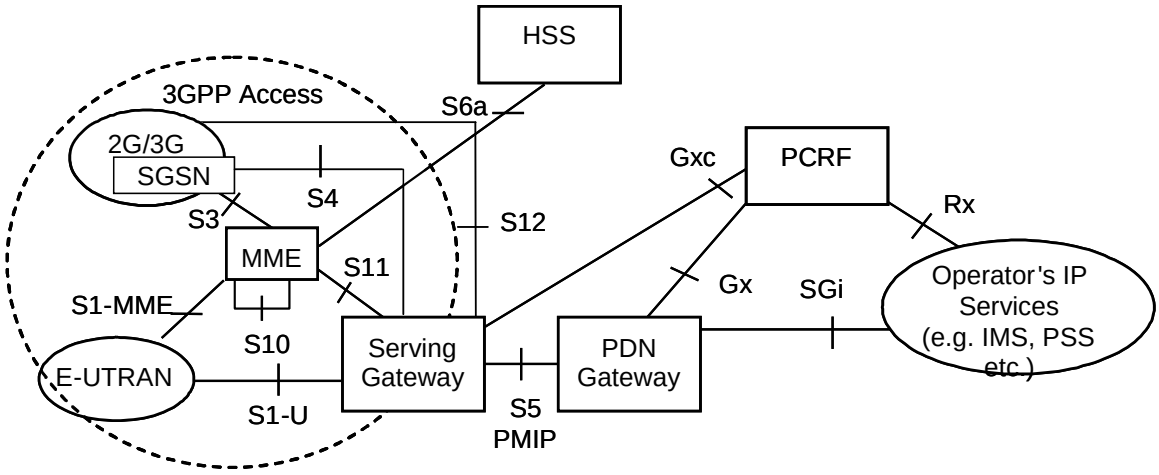


Figure 4.2.1-1: Non-Roaming Architecture for 3GPP Accesses within EPS using PMIP-based S5

NOTE: The "3GPP Access" bubble represents a collection of functional entities and interfaces for the purpose of pictorial simplification of the architectural models presented below.

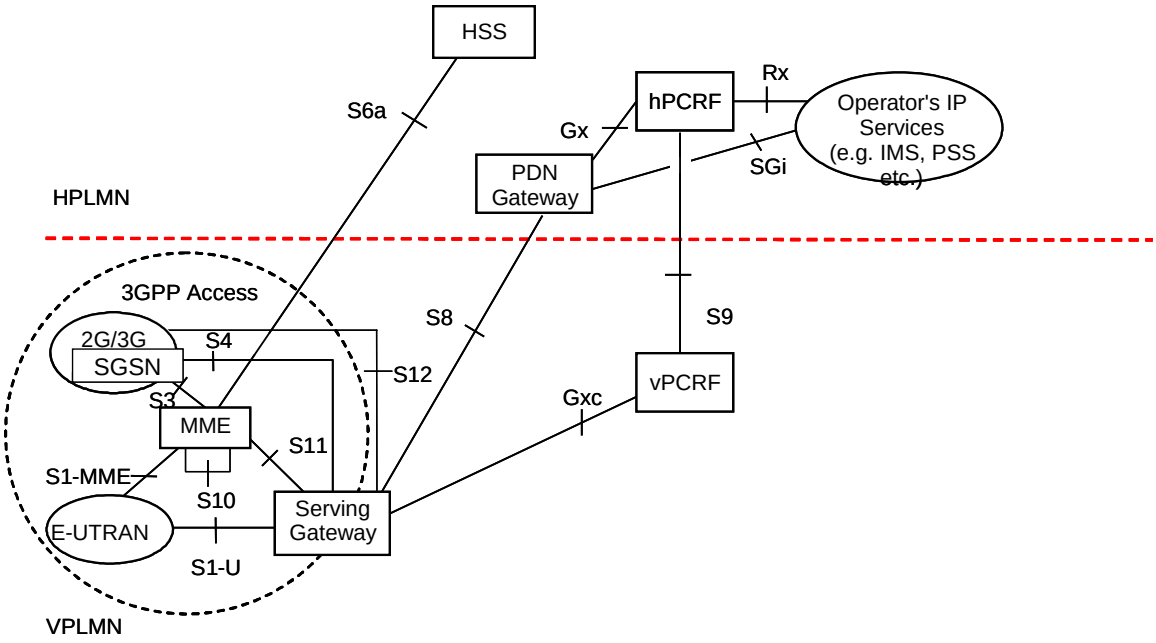


Figure 4.2.1-2: Roaming Architecture for 3GPP Accesses within EPS using PMIP-based S8

4.2.2 Non-roaming Architectures for EPS

The following considerations apply to interfaces where they occur in figures in this and the next clause:

- S5, S2a and S2b can be GTP-based or PMIP-based.
- Gxc is used only in the case of PMIP variant of S5 or S8.
- Gxa is used when the Trusted non-3GPP Access network is owned by the same operator.
- Gxb is used only in the case of PMIP variant of S2b.
- S9 is used instead of Gxa to the Trusted non-3GPP Access network not owned by the same operator.
- Gxa or S9 are terminated in the Trusted non-3GPP Accesses if supported.
- S2c is used only for DSMIPv6 bootstrapping and DSMIPv6 De-Registration (Binding Update with Lifetime equals zero) when the UE is connected via 3GPP access. Dashed lines are used in Figure 4.2.2-2, Figure 4.2.3-3 and Figure 4.2.3-5 to indicate this case.

NOTE 1: SWu shown in Figure 4.2.2-1 also applies to architectural reference Figures 4.2.2-2 and 4.2.3-1 to 4.2.3-5, but is not shown for simplicity.

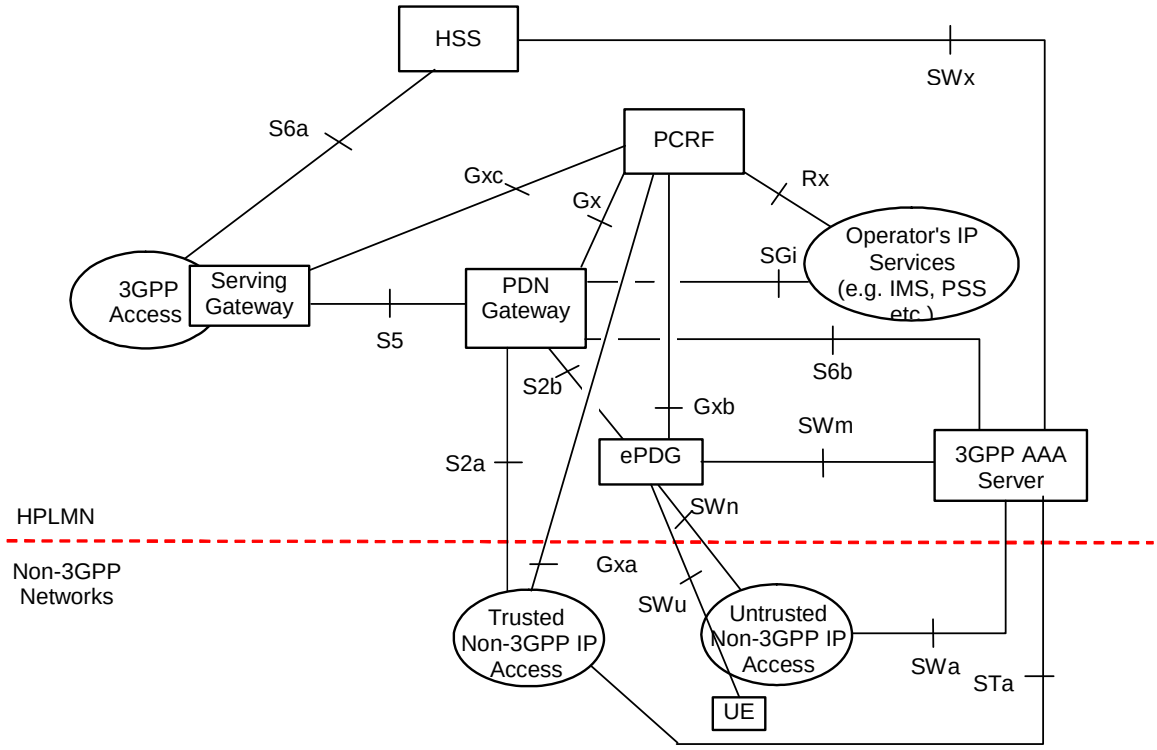


Figure 4.2.2-1: Non-Roaming Architecture within EPS using S5, S2a, S2b

NOTE 2: For S2a using a Trusted WLAN access, refer to clause 16.

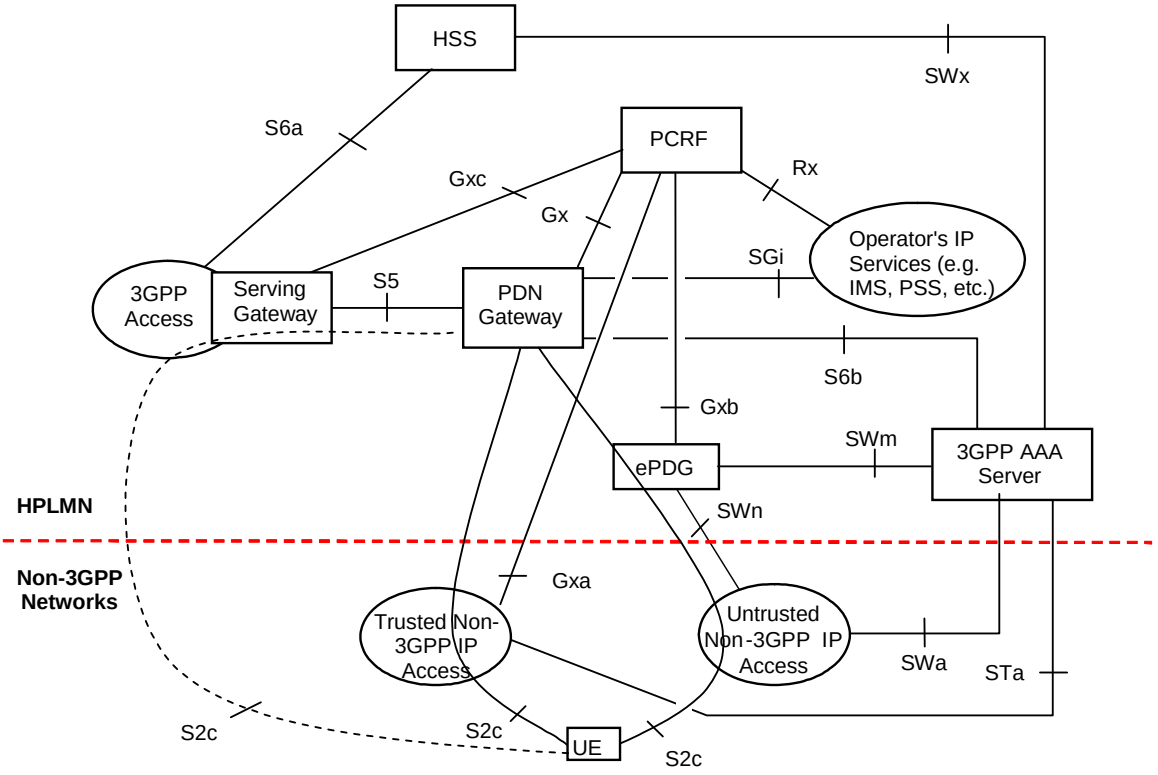


Figure 4.2.2-2: Non-Roaming Architecture within EPS using S5, S2c

4.2.3 Roaming Architectures for EPS

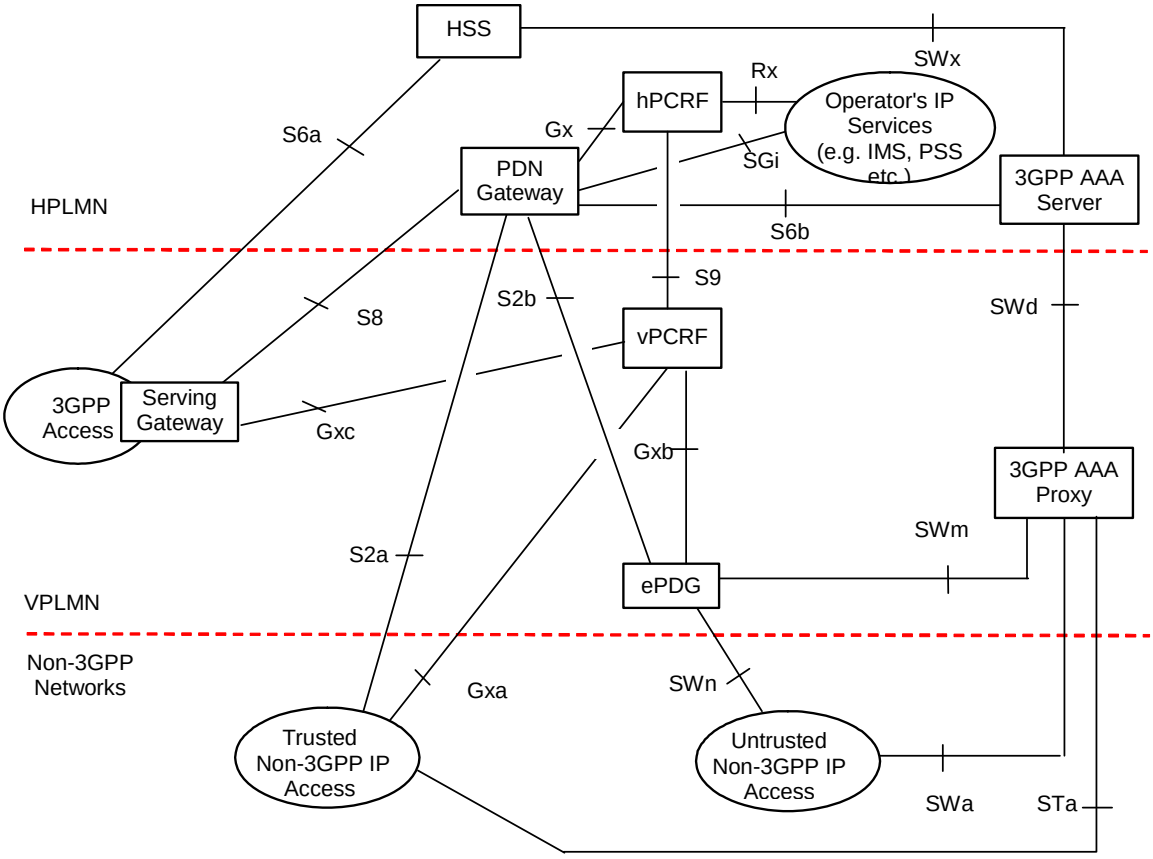


Figure 4.2.3-1: Roaming Architecture for EPS using S8, S2a– S2b - Home Routed

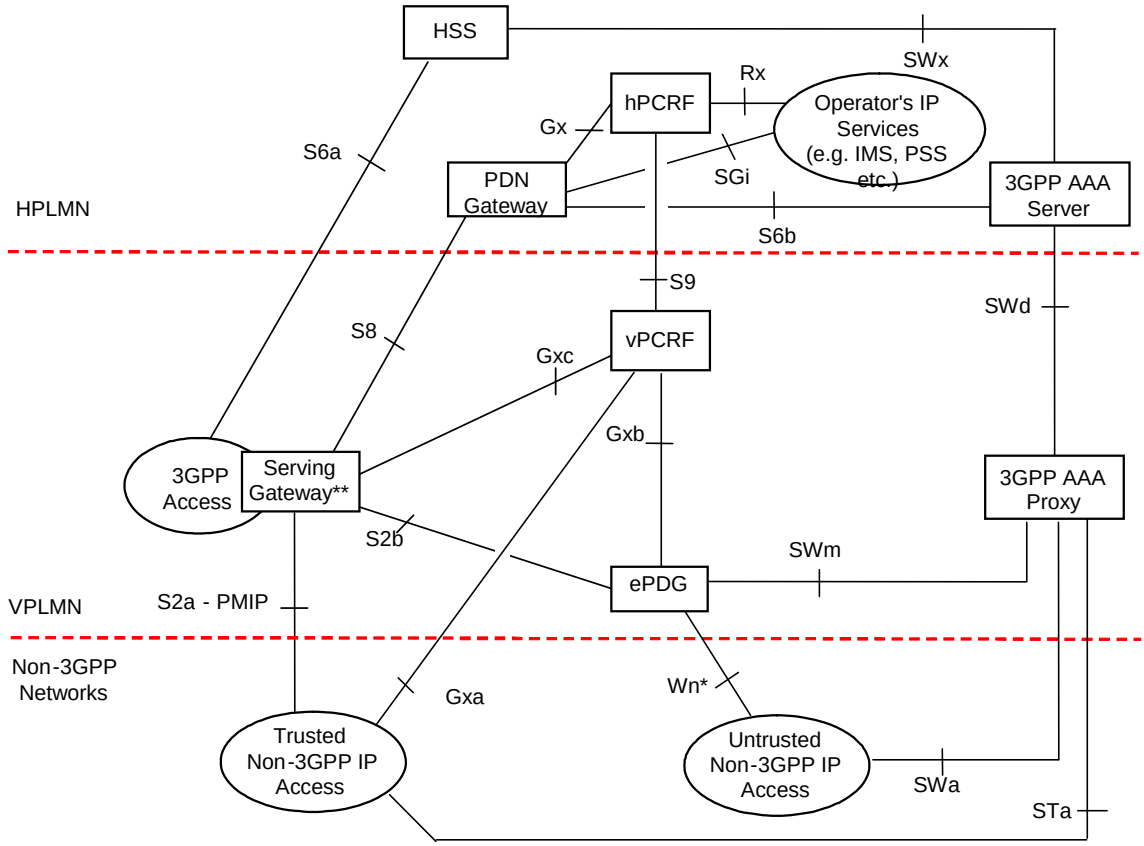


Figure 4.2.3-2: Roaming Architecture for EPS using PMIP-based S8, S2a, S2b (Chained PMIP-based S8-S2a/b) - Home Routed

** Chained S2a/S2b and S8 used when VPLMN has business relationship with Non-3GPP Networks and S-GW in VPLMN includes local non-3GPP Anchor.

NOTE 1: AAA, mobility, and QoS policy and event reporting related optimizations (e.g. signalling reduction and information hiding towards the HPLMN) for PMIP-based S8-S2a/b chaining are not specified within this Release of the specification.

NOTE 2: GTP-based S8-S2b chaining is not specified within this Release of the specification.

The following are some additional considerations in this case:

- Gxc is used only in the case of PMIP-based S8 and for 3GPP access.

NOTE 3: If QoS enforcement on PMIP-based S8 is required by the Serving Gateway for Un-trusted Non-3GPP IP Accesses, static policies will be used in this Release of the specification.

- Gxc is not required for Trusted Non-3GPP IP Access; Gxa is used instead to signal the QoS policy and event reporting.

NOTE 4: For S2a using a Trusted WLAN access, refer to clause 16.

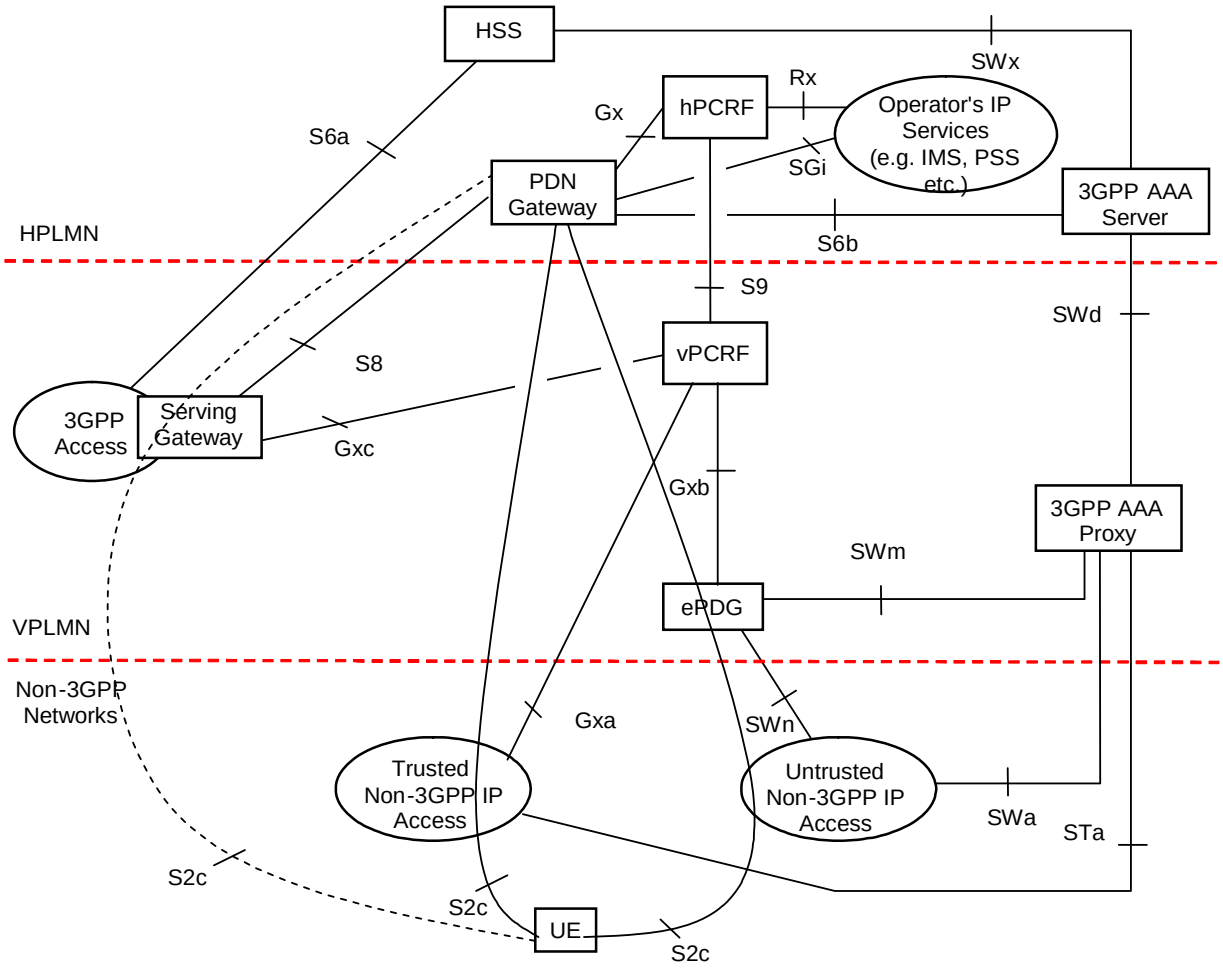


Figure 4.2.3-3: Roaming Architecture for EPS using S8 – S2c - Home Routed

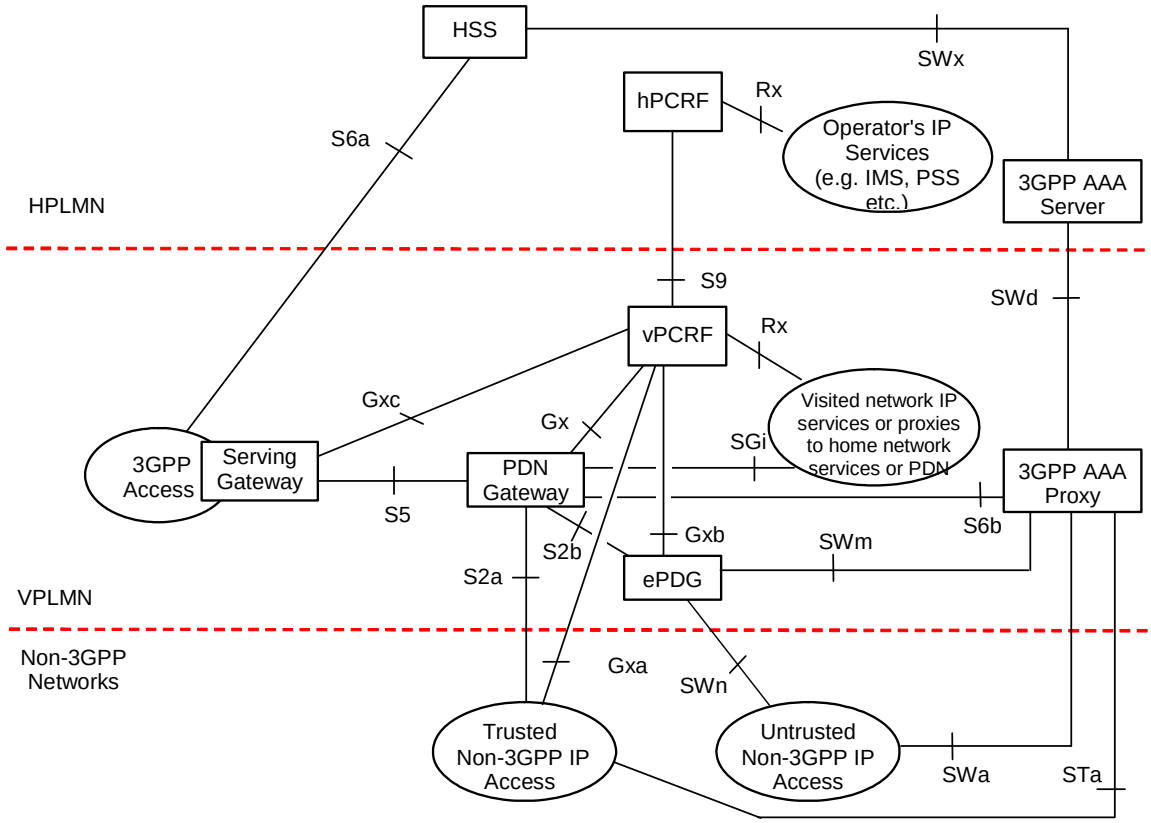


Figure 4.2.3-4: Roaming Architecture for EPS using S5, S2a, S2b – Local Breakout

NOTE 5: The two Rx instances in Figure 4.2.3-4 apply to different application functions in the HPLMN and VPLMN.

NOTE 6: For S2a using a Trusted WLAN access, refer to clause 16.

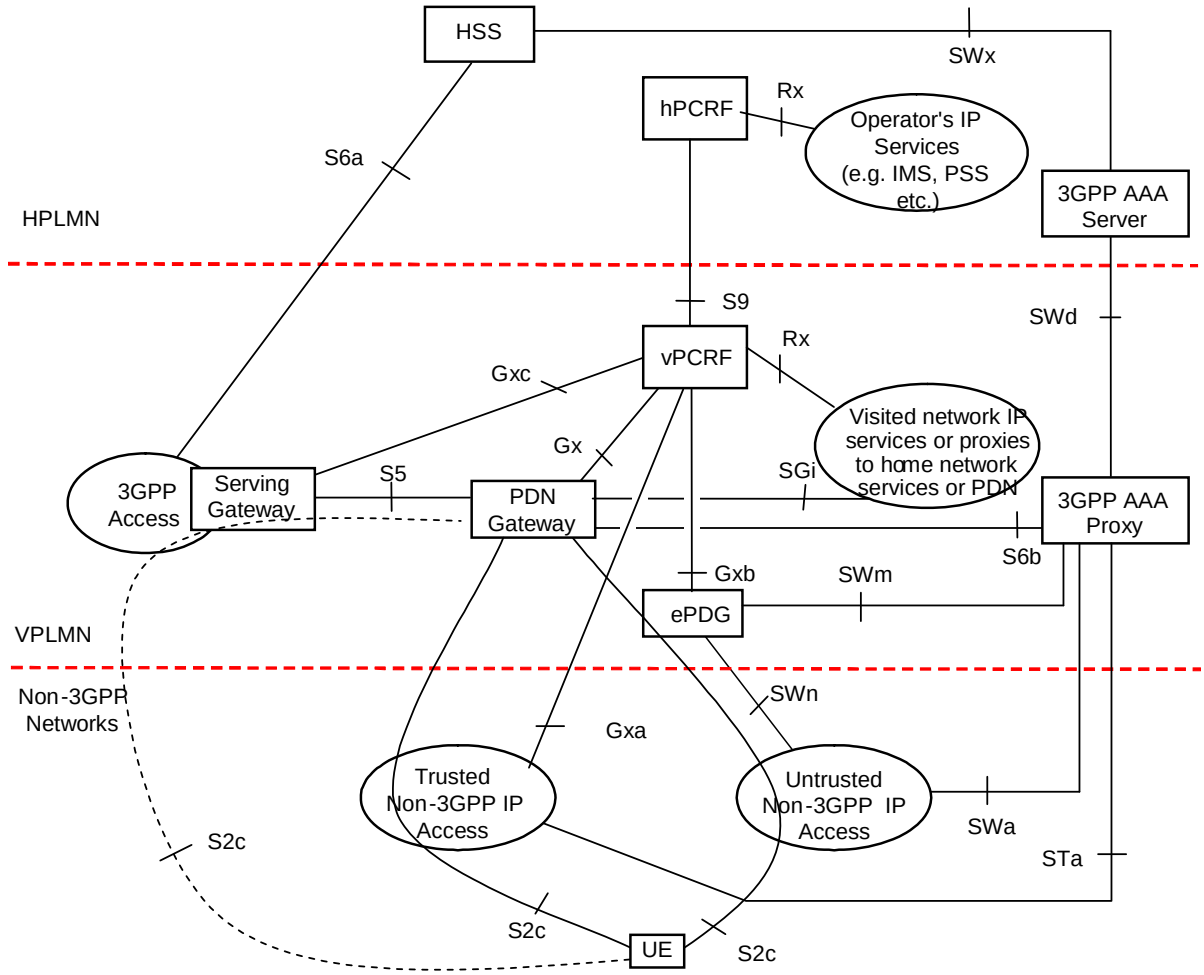


Figure 4.2.3-5: Roaming Architecture for EPS using S5, S2c – Local Breakout

NOTE 7: The two Rx instances in Figure 4.2.3-5 apply to different application functions in the HPLMN and VPLMN.

4.3 Network Elements

4.3.1 Access Networks

4.3.1.1 E-UTRAN

E-UTRAN is described in detail in TS 36.300 [6] with additional functions listed in TS 23.401 [4].

4.3.1.2 Trusted and Untrusted Non-3GPP Access Network

Trusted and Untrusted Non-3GPP Access Networks are IP access networks that use access technology whose specification is out of the scope of 3GPP.

Whether a Non-3GPP IP access network is Trusted or Untrusted is not a characteristic of the access network.

In non-roaming scenario it is the HPLMN's operator decision if a Non-3GPP IP access network is used as Trusted or Untrusted Non-3GPP Access Network.

In roaming scenario, the HSS/3GPP AAA Server in HPLMN makes the final decision of whether a Non-3GPP IP access network is used as Trusted or Untrusted non-3GPP Access Network. The HSS/3GPP AAA Server may take the VPLMN's policy and capability returned from the 3GPP AAA Proxy or roaming agreement into account.

For supporting multiple PDNs, the same trust relationship shall apply to all the PDNs the UE connects to from a certain Non-3GPP Access Network, i.e. it shall not be possible to access one PDN using the non-3GPP access network as Trusted, while access to another PDN using the same non-3GPP access network as Untrusted.

4.3.2 MME

The details of functionality of MME are described TS 23.401 [4].

The following are additional MME functions:

- HRPD access node (terminating S101 reference point) selection and maintenance for handovers to HRPD.
- Transparent transfer of HRPD signalling messages and transfer of status information between E-UTRAN and HRPD access, as specified in the pre-registration and handover flows.
- Forwarding the GRE key for uplink traffic to the target S-GW in case of CN node relocation.
- Transparent transfer of SON Information between E-UTRAN and HRPD access.

4.3.3 Gateway

4.3.3.1 General

Two logical Gateways exist:

- Serving GW (S-GW)
- PDN GW (P-GW)

The functional split of PDN GW and Serving GW is described in TS 23.401 [4].

4.3.3.2 Serving GW

The functionality of the Serving GW is described in TS 23.401 [4]. In addition to the functions described in TS 23.401 [4] the Serving GW includes the following functionality:

- A local non-3GPP anchor for the case of roaming when the non-3GPP IP accesses connected to the VPLMN.
- Event reporting (change of RAT, etc.) to the PCRF.
- Uplink and downlink bearer binding towards 3GPP accesses as defined in TS 23.203 [19].
- Uplink bearer binding verification with packet dropping of "misbehaving UL traffic".

NOTE 1: The term 'Uplink bearer binding verification' is defined in TS 23.401 [4].

- Mobile Access Gateway (MAG) according to PMIPv6 specification, RFC 5213 [8], if PMIP-based S5 or S8 is used. The MAG function shall be able to send UL packets before sending the PBU or before receiving the PBA.
- Decide if packets are to be forwarded (uplink towards PDN or downlink towards UE) or if they are locally destined to the S-GW (e.g. Router Solicitation).
- DHCPv4 (relay agent) and DHCPv6 (relay agent) functions if PMIP-based S5 or S8 is used.
- Handling of Router Solicitation and Router Advertisement messages as defined in RFC 4861 [38], if PMIP based S5 and S8 is used.
- Handling of Neighbour Solicitation and Neighbor Advertisement messages as defined in RFC 4861 [38], if PMIP based S5 and S8 is used.
- Allocation of downlink GRE key for each PDN connection within the Serving GW, which is used by the PDN GW to encapsulate downlink traffic to the Serving GW on the PMIP-based S5/S8 interface.
- If PMIP-based S8-S2a/b chaining is used:

- the Serving GW acts as a LMA towards the MAG function of the Trusted Non-3GPP IP Access or the ePDG;

- the Serving GW allocates uplink GRE key for each PDN connection within the Serving GW, which is used to encapsulate uplink traffic on PMIPv6-based S2a/S2b interface.

NOTE 2: The Serving GW does not require full MAG and full LMA functionally.

- the Serving GW includes functionality to interwork the PMIPv6 signalling towards the PDN GW and PMIPv6 signalling towards the MAG function of the Trusted Non-3GPP IP Access or the ePDG. In this case the Serving GW also acts as a MAG towards the PDN GW;

- the Serving GW includes functionality to link the user-plane of the PMIPv6 tunnel towards the PDN GW and the user-plane of the PMIPv6 tunnel towards the MAG function of the Trusted Non-3GPP IP Access or the ePDG.

4.3.3.3 PDN GW

PDN GW functionality is described in TS 23.401 [4] for 3GPP accesses connected to the EPC via GTP-based and PMIP-based S5/S8 interface. The PDN GW supports functionality specified in TS 23.401 [4] that is common to both PMIP-based and GTP-based S5/S8 interfaces also for access to EPC via non-3GPP accesses.

Additionally, the PDN GW is the user plane anchor for mobility between 3GPP access and non-3GPP access. For this, the PDN GW includes the following functionality:

- A LMA according to the PMIPv6 specification, RFC 5213 [8], if PMIP-based S5 or S8, or if PMIP-based S2a or PMIP-based S2b is used. The LMA function shall be able to accept UL packets from any trusted MAG without enforcing that the source IP address must match the CoA in the MN BCE.

- A DSMIPv6 Home Agent, as described in RFC 5555 [10], if S2c is used.

- Allocation of uplink GRE key for each PDN connection within the PDN GW, which is used to encapsulate uplink traffic to the PDN GW on the PMIP-based S5/S8, or PMIP-based S2a or PMIP based S2b interface.

- A MIPV4 Home Agent, if S2a with MIPv4 FA CoA mode is used.

- GPRS Tunnelling Protocol for the control plane and the user plane to provide PDN connectivity to UEs using non-3GPP accesses, if GTP-based S2a or GTP-based S2b is used.

4.3.4 ePDG

The functionality of ePDG includes the following:

- Allocation of a remote IP address as an IP address local to the ePDG which is used as CoA when S2c is used;

- Functionality for transportation of a remote IP address as an IP address specific to a PDN when S2b is used;

- Routing of packets from/to PDN GW (and from/to Serving GW if it is used as local anchor in VPLMN) to/from UE; if GTP based S2b is used, this includes routing of uplink packets based on the uplink packet filters in the TFTs assigned to the S2b bearers of the PDN connection;

- Routing of downlink packets towards the SWu instance associated to the PDN connection;

- De-capsulation/Encapsulation of packets for IPSec and, if network based mobility (S2b) is used, for GTP or PMIPv6 tunnels;

- Mobile Access Gateway (MAG) according to the PMIPv6 specification, RFC 5213 [8], if PMIP based S2b is used;

- Tunnel authentication and authorization (termination of IKEv2 signalling and relay via AAA messages);

- Local mobility anchor within untrusted non-3GPP access networks using MOBIKE (if needed);

- Transport level packet marking in the uplink;

- Enforcement of QoS policies based on information received via AAA infrastructure;

- Lawful Interception.
- Allocation of downlink GRE key for each PDN connection within the ePDG, which is used to encapsulate downlink traffic to the ePDG on the PMIPv6-based S2b interface.
- Accounting for inter-operator charging according to charging principles specified in TS 32.240 [61].
- Interfacing OFCS through reference points TS 32.251 [62] for EPC nodes.

4.3.5 PCRF

The functionality of PCRF is described in TS 23.203 [19] with additional functionality listed in TS 23.401 [4]. In the non-roaming scenario, additionally, the PCRF terminates the Gxa, Gxb and Gxc reference points with the appropriate IP-CANs.

In roaming scenarios, the difference from TS 23.401 [4], is that the vPCRF exists for the UE for the scenario of roaming with home-routed traffic in addition to the scenario in TS 23.401 [4] of roaming with local breakout.

4.3.5.1 Home PCRF

In addition to the h-PCRF functionality listed in TS 23.401 [4], in this document the Home PCRF

- Terminates the Gx reference point for roaming with home routed traffic;
- Terminates the Gxa, Gxb or Gxc/S9 reference points as appropriate for the IP-CAN type.

4.3.5.2 Visited PCRF

In addition to the v-PCRF functionality listed in TS 23.401 [4], in this document the Visited PCRF

- Terminates the Gxa, Gxb or Gxc reference points as appropriate for the IP-CAN type;
- Terminates the S9 reference point.

4.4 Reference Points

4.4.1 List of Reference Points

The description of the reference points:

S1-MME, S1-U, S3, S4, S10, S11: these are defined in TS 23.401 [4].

S2a It provides the user plane with related control and mobility support between trusted non 3GPP IP access and the Gateway.

S2b It provides the user plane with related control and mobility support between ePDG and the Gateway.

S2c It provides the user plane with related control and mobility support between UE and the Gateway. This reference point is implemented over trusted and/or untrusted non-3GPP Access and/or 3GPP access.

S5 It provides user plane tunnelling and tunnel management between Serving GW and PDN GW. It is used for Serving GW relocation due to UE mobility and in case the Serving GW needs to connect to a non collocated PDN GW for the required PDN connectivity.

S6a This interface is defined between MME and HSS for authentication and authorization. It is defined in TS 23.401 [4].

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

Gx It provides transfer of (QoS) policy and charging rules from PCRF to Policy and Charging Enforcement Function (PCEF) in the PDN GW.

Gxa It provides transfer of (QoS) policy information from PCRF to the Trusted Non-3GPP accesses.

Gxb This interface is not specified within this Release of the specification.

Gxc It provides transfer of (QoS) policy information from PCRF to the Serving Gateway

PMIP-based S8 It is the roaming interface in case of roaming with home routed traffic. It provides the user plane with related control between Gateways in the VPLMN and HPLMN.

S9 It provides transfer of (QoS) policy and charging control information between the Home PCRF and the Visited PCRF in order to support local breakout function. In all other roaming scenarios, S9 has functionality to provide dynamic QoS control policies from the HPLMN.

SGi It is the reference point between the PDN Gateway and the packet data network. Packet data network may be an operator external public or private packet data network or an intra operator packet data network, e.g. for provision of IMS services. This reference point corresponds to Gi for 3GPP accesses.

SWa It connects the Untrusted non-3GPP IP Access with the 3GPP AAA Server/Proxy and transports access authentication, authorization and charging-related information in a secure manner.

STa It connects the Trusted non-3GPP IP Access with the 3GPP AAA Server/Proxy and transports access authentication, authorization, mobility parameters and charging-related information in a secure manner.

SWd It connects the 3GPP AAA Proxy, possibly via intermediate networks, to the 3GPP AAA Server.

SWm This reference point is located between 3GPP AAA Server/Proxy and ePDG and is used for AAA signalling (transport of mobility parameters, tunnel authentication and authorization data). This reference point also includes the MAG-AAA interface functionality, RFC 5779 [43] and Mobile IPv6 NAS-AAA interface functionality, RFC 5447 [44].

SWn This is the reference point between the Untrusted Non-3GPP IP Access and the ePDG. Traffic on this interface for a UE-initiated tunnel has to be forced towards ePDG.

SWu This is the reference point between the UE and the ePDG and supports handling of IPSec tunnels. The functionality of SWu includes UE-initiated tunnel establishment, user data packet transmission within the IPSec tunnel and tear down of the tunnel and support for fast update of IPSec tunnels during handover between two untrusted non-3GPP IP accesses.

SWx This reference point is located between 3GPP AAA Server and HSS and is used for transport of authentication, subscription and PDN connection related data.

S1 interface for E-UTRAN is the same for both the architectures.

Protocol assumption:

- S2a interface is based on current or future IETF RFCs. S2a is based on Proxy Mobile IP version 6. For Trusted WLAN, S2a may also be based on GTP. To enable access via Trusted Non 3GPP IP accesses that do not support GTP and PMIPv6, S2a also supports Client Mobile IPv4 FA mode.

- S2b interface is based on GTP or Proxy Mobile IP version 6.

- S2c is based on DSMIPv6 [10].

- The PMIP-based S5, PMIP-based S8, PMIP-based S2a and PMIP-based S2b interfaces are based on the same protocols and differences shall be minimized. The S5 interface is based on the PMIPv6 specification, RFC 5213 [8].

- The GTP-based S5/S8, GTP-based S2a and GTP based S2b interfaces are based on the GTP protocol (TS 29.274 [57]). The GTP variant of S5 interface is described in TS 23.401 [4].

- PMIPv6-based S8 interface is based on the PMIPv6 specification, RFC 5213 [8]. The GTP variant interface is described in TS 23.401 [4].

- The PMIPv6-based interfaces (S5, S8, S2a, and S2b) shall support Generic Routing Encapsulation (GRE) RFC 2784 [23] including the Key field extension RFC 2890 [24]. The Key field value of each GRE packet header should enable the unique identification of the UE PDN connection that the GRE packet payload is associated with. These keys are exchanged using GRE Options extension to PMIPv6 Proxy Binding Update and Proxy Binding Ack messages on PMIPv6-based interfaces.

- In case of CN node relocation, the GRE key for uplink traffic is forwarded to the target S-GW over S10/S11 reference point.

- SWu interface is based on IKEv2 [9] and MOBIKE [18].

The EPS shall allow the operator to configure a type of access (3GPP or non-3GPP) as the "home link" for Client Mobile IP purposes.

NOTE: Redundancy support on reference points PMIP-based S5 and PMIP-based S8 should be taken into account.

4.4.2 Reference Point Requirements

4.4.2.1 S5 Reference Point Requirements

Both the GTP and PMIP variants of the S5 reference point shall satisfy the following architectural principles:

- There shall be only one radio interface protocol stack defined, common for both S5 variants, including both radio layer and Non-Access Stratum protocols.

- There shall be only one S6a interface defined common to both S5 variants. There may be a need for different information elements specific to PMIP-based or GTP-based variants of S5 but differences due to the S5 variants should be minimized.

- In the non-roaming case, there shall be only one Gx interface defined for transfer of policy and charging rules, common to both S5 variants. There may be a need for different information elements specific to PMIP-based or GTP-based variants of S5 but differences due to the S5 variants should be minimized.

- Differences between S5 variants in terms of functional split between the endpoints should be minimized.

The S5 reference point shall fulfil the following requirements:

- S5 shall allow access to multiple PDNs. It shall be possible to allow an UE to connect to different packet data networks. It shall also be possible to support a UE with concurrent connections to several packet data networks.

- S5 shall allow multiple PDN connections for a given APN and UE.

- S5 shall be able to transport both IPv4 and IPv6 user plane traffic independent of IP version of the underlying IP transport network.

- S5 shall support fault handling. There should be mechanisms to identify and signal faults for groups of mobiles – e.g., if a large node handling millions of terminals goes down.

NOTE: As further development of the architecture takes place as well as when additional functionality such as MBMS, LCS etc. are addressed, further requirements will be needed.

4.4.2.2 Void

4.4.2.3 Void

4.4.2.4 Void

4.5 High Level Functions

4.5.1 PDN GW Selection Function for Non-3GPP Accesses for S2a and S2b

PDN Gateway selection for non-3GPP accesses uses similar mechanisms as defined in TS 23.401 [4], with the following modification:

- The PDN Gateway selection function interacts with the 3GPP AAA Server or 3GPP AAA Proxy and uses subscriber information provided by the HSS to the 3GPP AAA Server. To support separate PDN GW addresses at a PDN GW for different mobility protocols (PMIP, MIPv4 or GTP), the PDN GW Selection function takes mobility protocol type into account when deriving PDN GW address by using the Domain Name Service function.

During the initial authorization, PDN Gateway selection information for each of the subscribed PDNs is returned to the ePDG or the Trusted Non-3GPP Access Network. The PDN Gateway selection information includes:

- The PDN GW identity, which is a logical name (FQDN) or IP address and an APN; or

- an APN and an indication whether the allocation of a PDN GW from the visited PLMN is allowed or a PDN GW from the home PLMN shall be allocated.

This enables the entity requiring the IP address of the PDN Gateway to proceed with selection as per the procedures defined in TS 23.401 [4], clause 4.3.8.1. Once the selection has occurred, the PDN Gateway registers its association with a UE and the APN with the AAA/HSS by sending PDN GW identity, that is either its IP address (e.g. if it has a single IP address for all the mobility protocols it supports or if it only supports one mobility protocol) or its FQDN (e.g. if it has multiple IP addresses for the mobility protocols it supports), as well as information that identifies the PLMN in which the PDN GW is located, to the 3GPP AAA Server or AAA Proxy only when the Access Technology Type is non-3GPP. For 3GPP access types, the MME/S4-SGSN updates the HSS with the selected PDN GW identity, as well as information that identifies the PLMN in which the PDN GW is located, according to TS 23.401 [4]/TS 23.060 [21]. This permits the HSS and 3GPP AAA Server or Proxy to provide the association of the PDN Gateway identity and the related APN for the UE subsequently.

NOTE 1: The format of the information that identifies the PLMN in which the PDN GW is located is defined in stage 3 specifications.

In the case that a UE already has assigned PDN Gateway(s), the PDN GW identity for each of the already allocated PDN Gateway(s), as well as information that identifies the PLMN in which the PDN GW is located, are returned by the 3GPP AAA Server or Proxy during the authorization step. This eliminates the need to repeat PDN Gateway selection for the PDNs the UE is already connected with. The information about the PLMN in which the PGW is located allows the receiving entity to determine an appropriate APN-OI. The ePDG may use this information to determine the S2b protocol type (PMIP or GTP). The TWAN may also use this information to determine the S2a protocol type (PMIP or GTP).

Upon mobility between 3GPP and non-3GPP accesses, PDN Gateway selection information for the subscribed PDNs the UE is not yet connected with is returned to the target access system as done during initial attachment. For the PDNs the UE is already connected with transfer of PDN GW information takes place as defined below:

- If a UE attaches to a non-3GPP access and it already has assigned PDN Gateway(s) due to a previous attach in a 3GPP access, the HSS provides the PDN GW identity, as well as information that identifies the PLMN in which the PDN GW is located, for each of the already allocated PDN Gateway(s) with the corresponding PDN information to the 3GPP AAA server over the SWx reference point.

- If a UE attaches to a 3GPP access and it already has an assigned PDN Gateway(s) due to a previous attach in a non-3GPP access, the HSS provides the PDN GW identity, as well as information that identifies the PLMN in which the PDN GW is located, for each of the already allocated PDN Gateway(s) with the corresponding PDN information to the MME over the S6a reference point and/or S4-SGSN over the S6d reference point.

The HSS receives the PDN GW identity for each of the selected PDN GWs and the corresponding PDN information for a given UE, from both the 3GPP AAA Server and also from the MME/S4-SGSN, depending on the currently in-use access. The HSS is responsible for the storage of the selected PDN GW identity as described in clause 12.

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 (PMIP or/and GTP) from the Domain Name Service function.

The TWAN may be configured with the S2a protocol variant(s) on a per HPLMN granularity, or may retrieve information regarding the S2a protocol variants supported by the PDN GW (PMIP or/and GTP) from the Domain Name Service function.

NOTE 2: The location of the PDN GW selection function depends upon the type of S2 interface used for attachment and the IP mobility mechanism being used.

- For PMIPv6 on S2a/b, the entity requesting the PDN Gateway is the entity acting as Mobile Access Gateway (MAG).
- For GTP on S2b, the entity requesting the PDN Gateway is the ePDG.
- For GTP on S2a, the TWAG, described in clause 16.1.2, is requesting the PDN Gateway.
- For the PMIP-based S8-S2a/b chained cases, the PDN GW information is sent together with the selected Serving GW address from the 3GPP AAA proxy to the entity acting as MAG in the non-3GPP access network during access authentication and authorization. The PDN GW selection mechanism is the same as in the unchained case. The MAG function of the non-3GPP access network conveys the PDN GW address to the Serving GW as part of the PMIPv6 PBU message.
- For MIPv4 FA mode on S2a, the entity requesting the PDN Gateway is the entity that plays the role of the FA.

4.5.1a PDN GW Selection Function for eHRPD with SIPTO support

In order to select the appropriate PDN GW for SIPTO in eHRPD access via HSGW, the PDN GW selection function needs to support DNS mechanism that allows selection of a PDN GW which is close to the HSGW for the UE. Details related to SIPTO support for eHRPD access is defined in 3GPP2 X.S0057 [51].

4.5.2 PDN GW Selection Function for S2c

For the S2c reference point, the UE needs to know the IP address of the PDN Gateway for the PDN the UE wants to connect to. This address is made known to the UE using one of the following methods:

1) Via PCO at the attach procedure or UE requested PDN Connectivity procedure, for 3GPP access (as defined in TS 23.401 [4]) or trusted non-3GPP access (if supported).
2) Via IKEv2 during tunnel setup to ePDG. For a UE's initial Attach, during the IKEv2 tunnel establishment procedure on the SWu interface (between UE and ePDG):
   - For non-roaming case, the 3GPP AAA Server selects the HA (PDN GW) which is close to the ePDG and sends the HA (PDN GW) FQDN or IP address to the ePDG;
   - For roaming with local breakout case, the 3GPP AAA Proxy selects the HA (PDN GW) which is close to the ePDG and sends the HA (PDN GW) FQDN or IP address to the ePDG;

   The HA (PDN GW) FQDN or IP address are then forwarded to the UE by the ePDG.

   NOTE 1: Whether the selected PDN GW is closer to the UE than other PDN GW depends on the network configurations and operations, it may be geographically/topologically closer or less IP hops.
3) If the IP address of the PDN GW is not received using options 1-2 above and if the UE knows that the HA is in the PDN where the UE is attached to then the UE shall request a PDN Gateway address via DHCP IETF RFC 6611 [41].
4) If the IP address of the PDN GW is not delivered using options 1-3 above the UE can interact directly with the Domain Name Service function by composing a FQDN corresponding to the PDN.

For the S2c reference point, the network can force a reallocation of the PDN Gateway selected upon initial DSMIPv6 bootstrapping for the PDN the UE wants to connect to. This may happen if one of the following situations occurs:

- The UE has done initial network attachment on an access system supporting network-based mobility, but the PDN Gateway discovered by the UE for the S2c reference point is different from the PDN Gateway allocated at initial network attachment. In this case, to enable IP address preservation based on DSMIPv6 upon inter-system mobility, the network must trigger a PDN Gateway reallocation for the S2c reference point, to re-direct the UE to the PDN Gateway that was selected upon initial network attachment.

- The UE has done initial network attachment over S2c and, relying on DNS, has discovered a sub-optimal PDN Gateway. In this case, based on operator's policies, the network can optionally trigger a PDN Gateway reallocation to re-redirect the UE to a PDN Gateway that can provide better performance.

PDN Gateway reallocation for the S2c reference point is triggered by the AAA/HSS during DSMIPv6 bootstrapping. For a UE's initial Attach, if the UE has selected a initial PDN GW and initiated DSMIPv6 bootstrapping:

- In non-roaming scenario, the PDN GW reports the UE Care of Address (allocated by the WLAN AN or ePDG) to the 3GPP AAA Server. According to the UE CoA and the pre-configuration, the 3GPP AAA Server finds there are other PDN GW(s) which are close to the UE, then it can initiate a PDN GW reallocation procedure (Clause 6.10 "PDN GW reallocation upon attach on S2c") to redirect the UE to the other PDN GW.

- In roaming with local breakout scenario, the PDN GW reports the UE Care of Address (allocated by the WLAN AN or ePDG) to the 3GPP AAA Proxy. According to the UE CoA and the pre-configuration, the 3GPP AAA Proxy finds there are other PDN GW(s) which are close to the UE, then it can initiate a PDN GW reallocation procedure (clause 6.10 "PDN GW reallocation upon attach on S2c") to redirect the UE to the other PDN GW.

NOTE 2: Whether the selected PDN GW is closer to the UE than other PDN GW depends on the network configurations and operations, it may be geographically/topologically closer or less IP hops.

NOTE 3: This reallocation is initiated only if the UE has not yet successfully established a binding with the selected PDN GW.

The HSS receives the values of identity(ies) of all allocated PDN GWs and the corresponding PDN information for a given UE from the 3GPP AAA. The HSS is responsible for the storage of PDN GW identity information.

4.5.3 Serving GW Selection Function for Non-3GPP Accesses

The S-GW selection function allocates an S-GW that acts as a local anchor for non-3GPP access in the case of S8-S2a/b chained roaming. Whether S8-S2a/b chaining should be used is decided by 3GPP AAA Proxy based on per-HPLMN configuration.

The Serving GW selection function is located in 3GPP AAA Proxy. If an S-GW is needed for non-3GPP access in the visited network, the 3GPP AAA proxy will select an S-GW for the UE during initial attach or handover attach. The 3GPP AAA proxy shall send the selected S-GW address to the MAG function of the Trusted non-3GPP IP access or ePDG in the chained S8-S2a/b scenarios.

There is no mechanism standardized for S-GW address preservation for handover between 3GPP and non-3GPP in S2/S8 chained case within this Release of the specification.

4.5.4 ePDG Selection

4.5.4.1 General

The UE performs ePDG selection based on a set of information configured by the HPLMN in the UE, and based on the UE's knowledge of the PLMN it is attached to.

A UE connected to one or multiple PDN GWs uses a single ePDG.

4.5.4.2 ePDG FQDNs Construction

When the UE attempts to construct an FQDN for selecting an ePDG in a certain PLMN-x (either a VPLMN or the HPLMN), then the UE shall construct one of the following FQDN formats:

- Operator Identifier FQDN: The UE constructs the FQDN by using the PLMN-x ID as the Operator Identifier.

- Tracking/Location Area Identity FQDN: The UE constructs the FQDN by using the identity of the Tracking Area/Location Area it is located in (i.e. based on PLMN-x ID and TAC/LAC). The Tracking/Location Area Identity FQDN is used to support location-specific ePDG selection within a PLMN.

The ePDG FQDN formats are specified in TS 23.003 [16].

The UE selects one of the above FQDN formats as follows:

a) If the UE attempts to select an ePDG in the registered PLMN and the UE is configured to use for this PLMN the Tracking/Location Area Identity FQDN as defined in point 2) of clause 4.5.4.3; and

b) the UE knows the TAI/LAI of the area the UE it is located in (e.g. the TAI/LAI from the most recent Attach or TAU/LAU),

then the UE constructs a Tracking/Location Area Identity FQDN. Otherwise the UE constructs the Operator Identifier FQDN.

Also, the UE constructs the Operator Identifier FQDN as a fallback in the case of failure of DNS resolution of a Tracking/Location Area Identity based FQDN.

4.5.4.3 UE Configuration By HPLMN

The UE may be configured (e.g. via H-ANDSF, USIM, etc.) by the HPLMN with the following configuration, whose usage is defined in clause 4.5.4.4:

1) ePDG identifier configuration: It contains the FQDN or IP address of an ePDG in the HPLMN.

NOTE: The FQDN in the ePDG identifier configuration may have a different format than the one described in clause 4.5.4.2.

2) ePDG selection information: It contains a prioritized list of PLMNs which are preferred for ePDG selection. It also indicates if selection of an ePDG in a PLMN should be based on Tracking/Location Area Identity FQDN or on Operator Identifier FQDN, as specified in clause 4.5.4.4. The list of PLMNs may include the HPLMN.

The PLMNs included in the ePDG selection information are PLMNs that have roaming agreements with HPLMN for interworking with untrusted WLANs.

The ePDG selection information may include an "any PLMN" entry, which matches any PLMN the UE is attached to except the HPLMN. If the ePDG selection information contains both the "any PLMN" and the PLMN the UE is attached to, the UE shall give precedence to the latter.

4.5.4.4 UE ePDG Selection Procedure

The UE shall perform ePDG selection by executing the steps below. Unless otherwise specified, when the UE attempts to select an ePDG, the UE shall construct an FQDN for this ePDG as specified in clause 4.5.4.2 and shall use the DNS server function to obtain the IP address(es) of this ePDG.:

1) The UE shall attempt to determine the country it is located in. This is determined by implementation-specific methods not defined in this specification. If the UE cannot determine the country it is located in, the UE shall stop the ePDG selection.

2) If the UE determines to be located in its home country, then:

   a) The UE shall select an ePDG in the HPLMN. If the ePDG selection information contains the HPLMN, the UE shall construct an FQDN as specified in clause 4.5.4.2. If the ePDG selection information does not contain the HPLMN and the UE is configured with the ePDG identifier defined in bullet 1) of clause 4.5.4.3, then the UE shall either use the configured FQDN and use the DNS server function to obtain the IP address(es) of the ePDG(s) in the HPLMN, or the UE shall use the configured IP address. Otherwise, the UE shall construct an Operator Identifier FQDN and shall use the DNS server function to obtain the IP address(es) of the ePDG(s) in the HPLMN.

   b) If the UE cannot select an ePDG in the HPLMN, then the UE shall stop the ePDG selection.

3) If the UE determines to be located in a country other than its home country (called the visited country), then:

a) If the UE is registered via 3GPP access to a PLMN and this PLMN matches an entry in the ePDG selection information, then the UE shall select an ePDG in this PLMN. If the UE fails to connect to an ePDG in this PLMN, the UE shall select an ePDG by performing the DNS procedure specified in clause 4.5.4.5.

b) In all other cases, (e.g. when the UE is not configured with the ePDG selection information, or the UE is registered via 3GPP access to a PLMN but this PLMN does not match an entry in the ePDG selection information, or the UE is not registered via 3GPP access to any PLMN), the UE shall select an ePDG by performing the DNS procedure specified in clause 4.5.4.5.

4.5.4.5 ePDG Selection with DNS-based Discovery of Regulatory Requirements

The UE shall perform ePDG selection according to the following procedure when the UE determines to be located in a country other than its home country (called the visited country) and when the conditions defined in clause 4.5.4.4 apply.

The UE shall perform a DNS query to determine if the visited country mandates the selection of ePDG in this country as specified below.

1) If the DNS response contains no records, then the UE determines that the visited country does not mandate the selection of ePDG in this country. In this case:

   a) If the ePDG selection information contains one or more PLMNs in the visited country, the UE shall select an ePDG in one of these PLMNs. The UE shall consider these PLMNs based on their priorities in the ePDG selection information. If the UE fails to connect to an ePDG in one or more of these PLMNs, the UE shall select an ePDG in the HPLMN according to bullet 1b below.

   b) Otherwise, including the case when the UE fails to connect to an ePDG according to bullet 1a above, the UE shall select an ePDG in the HPLMN. If the UE is configured with the ePDG identifier defined in bullet 1) of clause 4.5.4.3, then the UE shall either use the configured FQDN and use the DNS server function to obtain the IP address(es) of the ePDG(s) in the HPLMN, or the UE shall use the configured IP address. Otherwise, the UE shall construct an Operator Identifier FQDN as specified in clause 4.5.4.2 and shall use the DNS server function to obtain the IP address(es) of the ePDG(s) in the HPLMN.

2) If the DNS response contains one or more records, then the UE determines that the visited country mandates the selection of ePDG in this country. Each record in the DNS response shall contain the identity of a PLMN in the visited country which may be used for ePDG selection. In this case:

   a) If the UE is registered via 3GPP access to a PLMN which is included in the DNS response, then the UE shall select an ePDG in this PLMN. If the UE fails to connect to an ePDG in this PLMN, then the UE shall select an ePDG in one of the other PLMNs included in the DNS response as specified in bullet 2b below.

   b) If the UE is registered via 3GPP access to a PLMN which is not included in the DNS response or the UE is not registered via 3GPP access to any PLMN or the UE fails to connect to an ePDG according to bullet 2a above, then the UE shall select an ePDG in one of the PLMNs included in the DNS response as follows:

      The UE shall select one of the PLMNs included in the DNS response based on the prioritized list of PLMNs in the ePDG selection information (i.e. the UE shall select first the highest priority PLMN in the ePDG selection information that is contained in the DNS response). If the ePDG selection information does not contain any of the PLMNs in the DNS response or the UE is not configured with the ePDG selection information, or the UE was not able to connect to an ePDG in the PLMNs included in the ePDG selection information and in the DNS response, then the UE shall select a PLMN included in the DNS response based on its own implementation means.

   c) If the UE cannot select an ePDG in any of the PLMNs included in the DNS response, then the UE shall stop the ePDG selection.

3) If the UE does not receive a DNS response, then the UE shall stop the ePDG selection.

After the UE selects a PLMN for ePDG selection as specified above, UE shall construct an Operator Identifier FQDN for the selected PLMN and shall use the DNS server function to obtain the IP address(es) of the ePDG(s) in this PLMN.

4.5.4a ePDG selection for emergency bearer services

4.5.4a.1 General

The UE may select an ePDG for emergency bearer services either using configured information as specified in clause 4.5.4a.2 or using dynamically created FQDN generated by the UE as specified in clause 4.5.4a.3. The UE shall first attempt ePDG selection based on configured information as described in clause 4.5.4a.2. If configured information is not available in the UE, the UE shall try to select ePDG as described in clause 4.5.4a.3.

NOTE: The UE stops the establishment of emergency calls if it is unable to select an ePDG for emergency bearer services.

4.5.4a.2 Static selection

It shall be possible to configure the UE (e.g. H-ANDSF, USIM, etc) with an ePDG address that supports emergency bearer services in its HPLMN. The ePDG address can take the format of:

1) An FQDN; or

2) An IP address.

The ePDG configuration information for emergency services shall be separate from the configuration for regular services and exclusively used for the ePDG selection of emergency services.

When the UE is statically configured with the IP address of an ePDG that supports emergency bearer services, the UE initiates the IPsec tunnel establishment towards this IP address.

If an FQDN is configured the UE employs the DNS server function to obtain the IP address(es) of the ePDG(s). If the DNS server responds with:

a) At least one IP address: the UE selects an IP address from the list returned in the DNS response, and the UE initiates the IPsec tunnel establishment towards this IP address, If it fails it repeats the attempts to set-up a SWu tunnel with the other IP addresses received from the DNS until it either succeeds or there is no more available IP address; or

b) No IP address is returned then the UE shall stop the selection of an ePDG for emergency services.

If the UE is not configured with an ePDG address for emergency services then the UE shall use dynamic ePDG selection as described in clause 4.5.4a.3.

4.5.4a.3 Dynamic selection.

The UE shall use the dynamically created HPLMN Operator Identifier FQDN as described in clause 4.5.4.2, with the addition that the FQDN constructed shall also contain an indication that the UE requires an ePDG that supports emergency bearer services. This FQDN is defined in TS 23.003 [16].

For the FQDN format of ePDG address, the UE shall use the DNS server function to obtain the IP address(es) of the ePDG(s). If the DNS query fails or does not provide an IP address the UE shall stop the establishment of emergency call.

4.5.5 PCRF Selection

In addition to the PDN-GW and AF being served by one or more PCRF nodes in a HPLMN and, where applicable , in VPLMN as in TS 23.401 [4], the following nodes in this specification also are served by PCRF:

- Serving GW;
- Elements in trusted non-3gpp access;
- ePDG.

Selection of a PCRF by nodes served by PCRF in this specification, is the same as that in specified in TS 23.203 [19].

4.5.6 DSMIPv6 Home Link Detection Function

The DSMIPv6 Home Link Detection Function is used by the UE to detect if, for a specific PDN, an access interface is the Home Link from a DSMIPv6 perspective.

It is up to the UE configuration to decide when to trigger the home link detection function for a specific PDN connection, except that homelink detection for an access interface shall be performed before sending any DSMIPv6 Binding Update via that access interface.

The UE detects the home link comparing the IPv6 prefix associated with a specific access system of the UE , and the Home Network Prefix (HNP) associated with the PDN connection. If there is a match, the UE detects it is in the home link for this specific PDN over the access interface. Otherwise, the UE detects it is not in the home link for this specific PDN over the access interface.

Home Network Prefix (HNP) may be assigned in a 3GPP access via PCO during 3GPP attach, if supported by the UE, or via IKEv2.

NOTE: The UE knows the IPv6 prefix associated with a specific access system interface via IP address allocation mechanisms applied in that access system.

The UE knows the HNP associated with a specific PDN from the IPsec security association bootstrap (see clause 6.3, step 4) or from PCO received in 3GPP attach.

4.5.7 IMS Emergency Session Support

4.5.7.1 Overview

Support for IMS Emergency Session for E-UTRAN access connected to the EPC with GTP-based S5/S8 is covered in TS 23.401 [4]. Corresponding changes that apply for PMIP-based S5/S8 interface are covered in clause 5 of this specification.

For this Release of the specification, IMS Emergency Session Support for non-3GPP accesses connected to EPC is limited to:

- Support of handover of emergency sessions from E-UTRAN access to HRPD access and is covered in clause 9 of this specification with an overview provided in clause 9.2.2.

NOTE: Support for IMS emergency sessions over HRPD access connected to EPC is not covered in this specification.

- Support of IMS Emergency Session Support over WLAN access to EPC as described in clause 4. 5.7.2

4.5.7.2 IMS Emergency Session Support over WLAN access to EPC

4.5.7.2.1 Introduction

This clause provides an overview about the EPC functionality for emergency PDN connections used to support IMS Emergency Session over WLAN un trusted access to EPC defined in TS 23.167 [83]. The specific functionality is described in the affected procedures and functions of this specification. For discrepancies between this overview clause and the detailed procedure and function descriptions the latter take precedence.

UEs request a PDN Connection for emergency services (also called an emergency PDN connection) when they are aware they need to establish an IMS emergency session.

In this Release of the specification, to support emergency sessions over WLAN access to EPC,

1. EPC procedures are only defined for Untrusted WLAN access to EPC (S2b)
2. An UE issues an Emergency session over WLAN access to EPC as a last resort (e.g. impossibility to use 3GPP access) and when it does not know it is roaming
3. Only UEs that have a valid EPC subscription and that are authenticated and authorized for EPC service are allowed to request an emergency PDN connection

4. For emergency PDN connection, no mechanisms are defined to support mobility between WLAN and 3GPP accesses.

5. No specific mechanisms are defined to select a specific WLAN AP for emergency services

6. No specific mechanisms are defined to support the roaming case: if an UE that is roaming sets up an emergency PDN connection, an ePDG and a PDN GW in the Home PLMN are used.

To get EPC access for emergency services the UE shall select an ePDG that supports emergency services. This is defined in clause 4.5.4a. Then the UE executes the procedure of Initial attach for S2b emergency services described in clause 7.2.5

An ePDG that supports emergency services is configured with Emergency Configuration Data that are applied to all PDN Connections for emergency services. The Emergency Configuration Data contain the Emergency APN which is used to derive a PDN GW, may contain the statically configured PDN GW for the Emergency APN, and may also contain information on the default QoS to apply to a PDN Connection for emergency services (as defined in clause 4.5.7.2.4).

The following procedures apply for emergency PDN connections:

- procedures defined in clause 7.4.3 ("UE/ePDG-initiated Detach Procedure and UE-Requested PDN Disconnection");

- procedures defined in clause 7.9.2 ("PDN GW initiated Resource Allocation Deactivation");

- procedures defined in clause 7.10 ("Dedicated S2b bearer activation");

- procedures defined in clause 7.11.1 ("PDN GW initiated bearer modification").

As part of these procedures, the UE local IP address and optionally UDP source port number (if NAT is detected) are reported from ePDG to the PDN GW. When Access Network Information reporting has been set by the PCRF, the UE local IP address is reported to the PCRF.

NOTE: The UE local IP address is used by the UE for sending all IKEv2 [9] messages and as the source address on the outer header of the IPsec tunnel to the ePDG.

The UE establishes only one PDN connection for emergency services. Thus procedures for "UE-initiated Connectivity to Additional PDN" in clause 7.6 do not apply to emergency PDN connections.

The emergency PDN connection is not a subscribed service. Thus procedures related with HSS Initiated Subscribed QoS Modification in clause 7.11.2 or procedures related with "HSS/AAA-initiated Detach Procedure" in clause 7.4.4 do not apply to emergency PDN connections.

The procedures defined in clause 8 do not apply to emergency PDN connections.

Procedures related with S2c do not apply to emergency PDN connections. Procedures related with S2a do not apply to emergency PDN connections.

4.5.7.2.2 Architecture Reference Model for Emergency Services

In this Release of the specification, only the non-roaming architecture defined in Figure 4.2.2-1 applies for emergency services.

4.5.7.2.3 PDN GW selection function for Emergency Services

The PDN GW selection does not depend on subscriber information in the HSS since emergency service support is not a subscribed service but a local service. Upon reception from the UE indication that a PDN connection for emergency services needs to be established, the ePDG looks up it configured Emergency Configuration Data. The Emergency Configuration Data contains the Emergency APN to be used to derive a PDN GW, or may also contain the statically configured PDN GW for the Emergency APN.

When a PDN GW is selected based on the Emergency APN, the PDN GW selection function described in clause 4.3.8.1 of TS 23.401 [4] for normal bearer services is applied to the Emergency APN. The PDN GW selection function shall always derive a PDN GW in the local PLMN.

This functionality is used by the Initial Attach procedure for emergency services as described in clause 7.2.5

4.5.7.2.4 QoS for Emergency Services

The Default QoS values used over S2b for establishing emergency PDN connections are configured in the Emergency Configuration Data.

NOTE: The WLAN network may support traffic priority management based on DSCP marking or may support WFA WMM profile specification, however the mapping between the 3GPP PCC QoS and the DSCP marking in ePDG and the control of QoS marking by UE for uplink traffic are not defined in this release of the specification.

4.5.7.2.5 PCC for Emergency Services

The same mechanisms than defined for 3GPP access in clause 4.3.12.6 of TS 23.401 [4] apply.

4.5.7.2.6 IP Address Allocation

The same mechanisms than defined for 3GPP access in clause 4.3.12.8 of TS 23.401 [4] apply.

4.5.7.2.7 Handling of PDN Connections for Emergency Bearer Services

The same mechanisms than defined for 3GPP access in clause 4.3.12.9 of TS 23.401 [4] apply with the only difference is that it is the ePDG (and not the MME) that shall reject any additional emergency PDN Connection requests.

4.5.7.2.8 Network provided WLAN Location Information

When as part of procedures for Authentication and Authorization on an Access Point based on USIM credentials, the WLAN Access Network provides WLAN Access Network location information to the 3GPP AAA server that it considers as network provided location, the 3GPP AAA server stores this information and provides it to the ePDG at the SWm Authentication and or Autorization procedure or upon request of the ePDG.

NOTE 1: It is up to local 3GPP AAA server policies to decide whether location information received from the WLAN access network may be considered as network provided location. The definition of the policies used by 3GPP AAA server is outside the scope of 3GPP.

This location information is called WLAN Location Information and contains the same information as is contained in the TWAN Identifier defined in clause 16.1.7. The Age of the WLAN Location information is provided in conjunction with the WLAN Location information.

NOTE 2: In cases where an UE may within an area move between AP(s) without the 3GPP AAA server being notified of this mobility, the WLAN Location Information can only refer to the first AP used by the UE within the area.

The 3GPP AAA server shall update its storage of WLAN Location Information associated with an UE when it receives WLAN Access Network location information from a WLAN AN that it considers as trustworthy for network provided location. The 3GPP AAA server shall remove its storage of WLAN Location Information associated with an UE when it becomes aware that the WLAN session of the UE is terminated or when it receives WLAN Access Network location information from a WLAN AN that it considers as not trustworthy for network provided location.

The ePDG shall store WLAN Location Information associated with an UE when it receives WLAN Access Network location information from the 3GPP AAA server. The ePDG shall remove its storage of WLAN Location Information associated with an UE when it receives from the 3GPP AAA server an indication that no WLAN Access Network location information is available for this UE.

The WLAN Location Information information and its Age, when available, are propagated by the ePDG to the PDN GW and then via PCC as defined in TS 23.203 [19]. This takes place at the UE-initiated connectivity to an initial PDN connection (Attach Procedure), at the UE-initiated connectivity to an additional PDN connection or, as described below, when the ePDG needs to send User Location Information about an already established PDN connection.

When the AAA server has sent WLAN Location Information at the UE-initiated connectivity to an initial (Attach Procedure) or additional PDN connection, and when later the ePDG needs to send User location Information towards

the PDN GW over S2b, the ePDG may initiate a WLAN Location Information Request to fetch the most up to date WLAN Location Information in conjunction with the age of this Information.

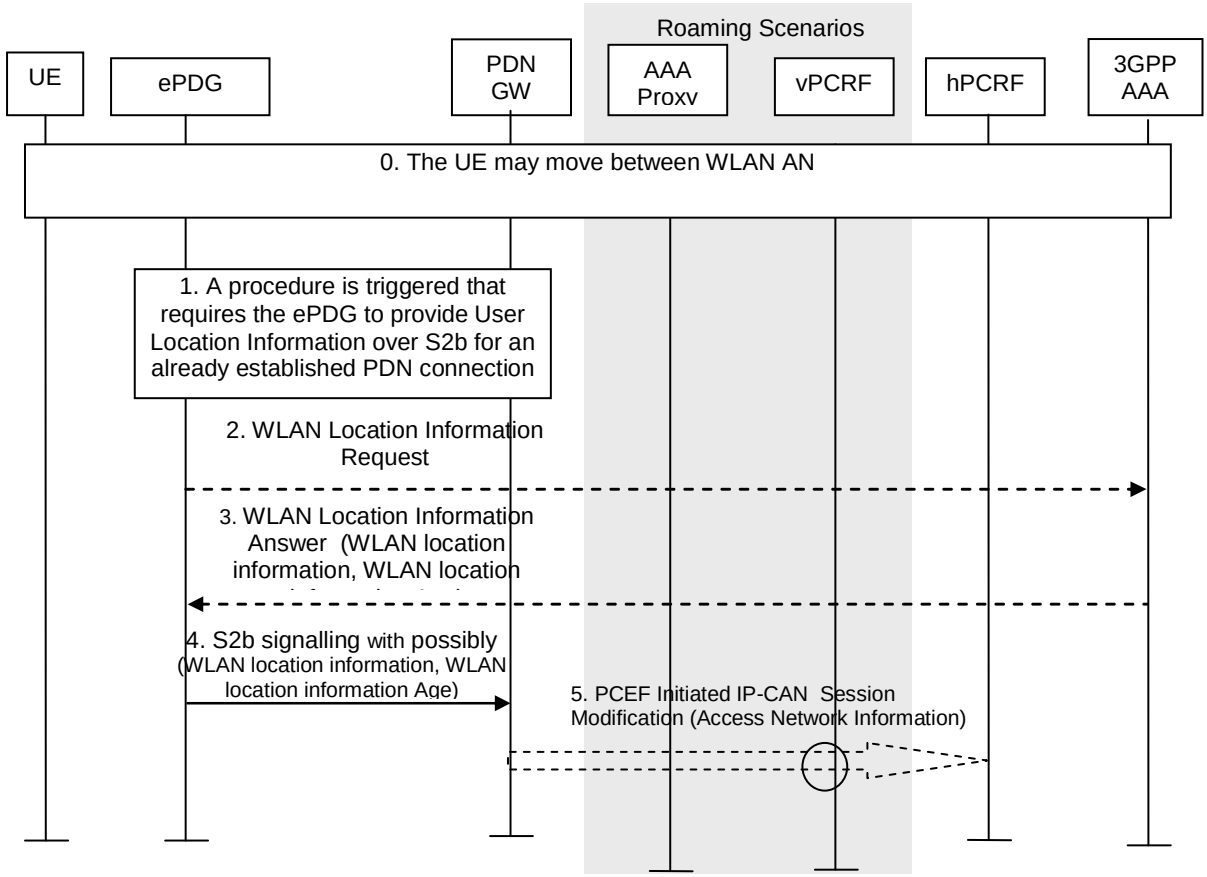


Figure 4.5.7.2.8-1: EPDG retrieval of WLAN Location Information

0) When the 3GPP AAA server detects that the UE has moved between WLAN AN, it locally updates or removes the WLAN Location Information information and its Age it stores for the UE.

1) A procedure is triggered that requires the ePDG to provide User Location Information over S2b for an already established PDN connection. The corresponding procedures are:

   - 7.4.3 UE/ePDG-initiated Detach Procedure and UE-Requested PDN Disconnection with GTP on S2b.
   - 7.9.2 PDN GW initiated Resource Allocation Deactivation with GTP on S2b.
   - 7.10 Dedicated S2b bearer activation with GTP on S2b.
   - 7.11 S2b bearer modification with GTP on S2b.

2) When the AAA server has sent WLAN Location Information at the set-up of a SWm session and the ePDG has detected a change of the outer IP address of the UE, the ePDG initiates a WLAN Location Information Request (IMSI) towards the 3GPP AAA server.

3) The 3GPP AAA server provides a WLAN Location Information Answer that may contain WLAN location information and WLAN location information Age or an indication that no WLAN location information is available. The ePDG replaces any WLAN location information andWLAN location information Age it may have stored beforehand by the information received from the 3GPP AAA server. When the WLAN Location Information Answer contains an indication that no WLAN location information is available, the ePDG removes any WLAN location information and WLAN location information Age it may have stored beforehand about the UE.

4) The ePDG issues S2b signalling with User Location Information. The User Location Information shall include UE local IP address and optionally UDP source port number (if NAT is detected). The User Location Information includes WLAN Location Information (and its Age) only when the ePDG has such information

currently available about the UE. When the PDN GW receives no WLAN Location Information from the ePDG it shall delete any such information it may have stored for the PDN connection.

5) If requested by the PCRF the PDN GW forwards to the PCRF following information extracted from User Location Information it may have received from the ePDG:

   - The UE local IP address.

   - WLAN location information in conjunction with the Age of this information,

   When the PCRF receives no WLAN location information from the PDN GW within User Location Information the WLAN location information is considered as not any longer valid.

4.5.8 APN congestion Control Function for eHRPD

The PDN GW may provide mechanisms for avoiding and handling overload situations for eHRPD over S2a. These include the rejection of PDN connection requests from UEs.

When performing overload control the PDN GW shall operate as specified in clause 4.3.7.5 of TS 23.401 [4].

NOTE: The words of "Bearer" in clause 4.3.7.5 of TS 23.401 [4] are replaced by "PDN connection" for eHRPD.

When receiving the rejection from the PDN GW, the HSGW shall operate as specified in clause 4.13 of the 3GPP2 X.S0057 [51].

4.5.9 GTP-C signalling based Load and Overload Control for trusted and untrusted WLAN

4.5.9.1 GTP-C load control

GTP-C Load Control feature is an optional feature which allows a GTP control plane node to send its Load Control Information to a peer GTP control plane node which the receiving GTP control plane peer node uses to augment existing PDN GW selection procedure.

GTP-C Load Control feature allows the PDN GW to send its Load Control Information to the TWAN/ePDG (for enhanced load balancing across PDN GWs during Attach or new PDN connectivity request scenarios).

This feature is supported over S2a and S2b interfaces via GTPv2 control plane protocol.

The same concepts as described in TS 23.401 [4], clause 4.3.7.1a.1 for PGW Load Control apply with the TWAN/ePDG playing a similar role as the MME/SGSN.

NOTE: Refer to clause 12 of TS 29.274 [57] for the details, such as exact format of the Load Control Information, mechanisms to discover the support of the feature by the peer node, interfaces for which this feature is applicable, APN level load control, etc.

4.5.9.2 GTP-C overload control

GTP-C Overload Control feature is an optional feature. Nodes using GTP control plane signalling may support communication of Overload Control Information in order to mitigate overload situation for the overloaded node through actions taken by the peer node(s).

This feature is supported over S2a and S2b interfaces via GTPv2 control plane protocol.

The Overload Control Information may convey information regarding the node itself and/or regarding specific APN(s) status.

GTP-C Overload Control feature allows the PDN GW to send its Overload Control Information to the TWAN/ePDG.

GTP-C Overload Control feature allows the TWAN/ePDG to send its Overload Control Information to the PDN GW.

An ePDG may apply certain restrictions towards PDN GW that have indicated overload, e.g.:

- reject PDN connection requests from the UE (e.g. Initial Attach, UE-initiated Connectivity to Additional PDN, Attach and PDN Connectivity Request at handover to Untrusted WLAN) and locally set a back-off timer. As long as the back-off timer is running, the ePDG shall reject the subsequent PDN connection requests from the UE;

- reduce/throttle messages towards the PDN GWs indicating overload status;

- apply other implementation specific mechanisms, which are outside the scope of 3GPP specifications.

A TWAN may during access authentication in Transparent Single-Connection Mode, Single-Connection Mode and during WLCP procedures in Multi-Connection Mode apply certain restrictions towards PDN GW that have indicated overload, e.g.:

- reject PDN connection requests from the UE (e.g. Initial Attach with PDN Connectivity, UE Initiated PDN connectivity request, Attach and PDN Connectivity Request at handover to Trusted WLAN) as follows:

  - for Transparent Single-Connection Mode, locally set a back-off timer and prevent the UE from accessing the SSID. For any further request for the same UE and the same SSID, as long as the back-off timer is running, the TWAN prevents the UE from accessing the SSID.

    NOTE 1: Some UE(s) may black-list an AP when they fail to authenticate on this AP. The following mechanisms can help lowering the risk of having to reject an attempt to access TWAN in Transparent Single-Connection Mode:

      - The TWAN reselects another PDN GW to retry PDN connection establishment, if more than one PDN GW supports the target APN,

      - If possible, the TWAN rejects UEs in Single-Connection Mode and Multi-Connection Mode before rejecting UEs in Transparent Single-Connection Mode when the PDN GW(s) have indicated overload.

  - for Single-Connection Mode, reject EPC access requests from the UE with a Session Management back-off timer that instructs the UE to not request new PDN connectivity to the same APN for the indicated time.

  - for Multi-Connection Mode, reject WLCP PDN connection requests for the same APN from the UE with a Session Management back-off timer that instructs the UE to not request new PDN connectivity to the same APN for the indicated time.

- reduce/throttle messages towards the PDN GWs indicating overload status;

- apply other implementation specific mechanisms, which are outside the scope of 3GPP specifications.

The same concepts as described in TS 23.401 [4] clause 4.3.7.1a.2 for PGW Overload Control apply with the TWAN/ePDG playing a similar role as the MME/SGSN.

NOTE 2: Refer to clause 12 of TS 29.274 [57] for the details, such as exact format of the Overload Control Information, mechanisms to discover the support of the feature by the peer node, interfaces for which this feature is applicable, APN level overload control, etc.

If the UE has received a Session Management back-off timer over non-3GPP access from the TWAG, the UE shall not send any Session Management requests related to that APN to the network via WLAN as long as the Session Management back-off timer is running.

A Session Management back-off timer received over non-3GPP access has no impact on the UE behaviour in 3GPP access. A Session Management back-off time received over 3GPP access has no impact on the UE behaviour in non-3GPP access.

NOTE 3: For ePDG, since a Session Management back-off timer is not provided to the UE, the UE may retry its request. This results in repeated signaling towards the ePDG before the network rejects the request from UE. Hence, it may cause the overload of the ePDG.

A PDN GW may apply certain restrictions towards TWAN/ePDG that have indicated overload, e.g. apply similar policies as those described in TS 23.401 [4] clause 4.3.7.1a.2 in the case of an MME or an SGW has indicated overload.

4.6 Identities

4.6.1 User Identification

In order to access the 3GPP Evolved Packet Core from non-3GPP accesses, and get Authentication, Authorization and Accounting services from the Evolved Packet Core, the NAI RFC 4282 [15] based user identification defined in TS 23.003 [16] shall be used.

In order to support network-based and client-based mobility related services from the evolved packet core, the NAI RFC 4282 [15] based user identification as defined in TS 23.003 [16] shall be used by the network and mobility clients. The username part of NAI shall be based on IMSI. For emergency attached UEs to the HRPD access which do not have authenticated IMSI, the username part of the MN NAI shall be based on IMEI as defined in TS 23.003 [16] for S2a and S101 reference points (see clause 9). IMSI shall be used for user identification on the GTP based S2b interface.

User identification in non-3GPP accesses may require additional identities that are out of the scope of 3GPP. These user identities, if not compliant to TS 23.003 [16], are however not sufficient to identify a user in the 3GPP Evolved Packet Core.

4.6.2 EPS bearer identity with GTP based S2b/S2a

With GTP based S2b an EPS Bearer ID uniquely identifies an S2b bearer between an ePDG and a PDN GW for one UE accessing via non 3GPP access (see clause 4.10.3). This EPS Bearer ID is allocated by the ePDG and is not known to the UE.

With GTP based S2a an EPS Bearer ID uniquely identifies an S2a bearer between a TWAN and a PDN GW for one UE accessing via trusted WLAN access. This EPS Bearer ID is allocated by the TWAN and is not known to the UE.

The EPS Bearer IDs assigned for a specific UE on S2b are independent of the EPS Bearer IDs assigned for the same UE on S5/S8 and may overlap in value.

The EPS Bearer IDs assigned for a specific UE on S2a are independent of the EPS Bearer IDs assigned for the same UE on S5/S8 and may overlap in value.

NOTE 1: In MAPCON scenario with one PDN connection over 3GPP access and another PDN connection over untrusted non-3GPP access, the possibly identical EPS Bearer ID used simultaneously on S2b and S5/S8 designates two distinct traffic flow aggregates.

NOTE 2: When a PDN connection is handed over between 3GPP access and untrusted non-3GPP access, the possibly identical EPS Bearer ID on the source and target side may designate distinct traffic flow aggregates.

4.7 IP Address Allocation

4.7.1 IP Address Allocation with PMIP-based S5/S8

The IP address allocation mechanisms described in clause 5.3.1.1 of TS 23.401 [4] are also valid for the PMIP based S5/S8. This clause is complementary to clause 5.3.1 of TS 23.401 [4] and describes the differences in the IP Address allocation when PMIP-based S5/S8 is used.

For IP address allocation with PMIP-based S5/S8, the following clarifications apply:

- If the PDN Type associated with the PDN connection is IPv4:
  - If initial and handover attach and deferred IPv4 address allocation is not used, the IPv4 address is allocated via default bearer activation. This case does not present any architecture differences from the GTP based S5/S8 described in clause 5.3.1.2.1 of TS 23.401 [4]. In this case, the Serving GW shall request IPv4 address in the Proxy Binding Update. Then the IPv4 address is assigned by the PDN GW and returned to the Serving Gateway in the Proxy Binding Acknowledgement.
  - If initial and handover attach and deferred IPv4 address allocation is used, the IPv4 address allocation and IPv4 parameter configuration via DHCPv4 according to RFC 2131 [28] and RFC 4039 [29] procedure does

not present any architecture differences from the GTP based S5/S8 described in TS 23.401 [4], clause 5.3.1.2.4, except that the Serving GW shall have DHCPv4 relay agent functionality. The Serving GW shall request IPv4 address in the Proxy Binding Update. Then the IPv4 address is assigned by the PDN GW and returned to the Serving Gateway in the Proxy Binding Acknowledgement. The PDN GW shall also send the DHCPv4 Address Allocation Procedure Indication in the same Proxy Binding Acknowledgement message. In this case, the UE IPv4 address assigned by the PDN GW is not provided as part of the default bearer activation procedures to the UE. The Serving GW replaces the IPv4 address assigned by the PDN GW to 0.0.0.0 in the response message to the MME. The MME then forwards the 0.0.0.0 address to the UE. After the default bearer establishment procedure is completed, the UE uses the connectivity with the EPS and initiates the IPv4 address allocation on its own using DHCPv4 as specified in figure 4.7.1-1. The IPv4 address provided to the UE by DHCPv4 procedure shall correspond to the value provided in the Proxy Binding Acknowledgement message.

  - If the IPv4 address is allocated by using DHCPv4 procedure, then at any time after the UE releases the IPv4 address using DHCPv4 or the IPv4 address lease time expires, the PDN GW initiates the "PDN-GW initiated PDN-disconnection" procedure for the given PDN connection. The same IPv4 address shall not be allocated to another UE immediately.

- If the PDN Type associated with the PDN connection is IPv6:

  - IPv6 network prefix allocation via IPv6 Stateless Address auto-configuration: The IPv6 network prefix is assigned by the PDN GW and returned to the Serving Gateway in the Proxy Binding Acknowledgement. The Serving GW shall advertise the same information as the PDN GW would advertise with GTP based S5/S8. To ensure that link-local address generated by the UE does not collide with the link-local address of the Serving GW, the PDN GW shall provide an interface identifier to the UE and the UE shall use this interface identifier to configure its link-local address. For stateless address auto-configuration however, the UE can choose any interface identifier to generate IPv6 address, other than link-local, without involving the network. The PDN GW shall also provide a link-local address to the Serving GW and the Serving GW shall use the link-local address on the access link shared with the UE. In the case of PMIP-S5/S8 because any prefix that the Serving GW will advertise to the UE is unique, there is no need for the UE to perform Duplicate Address Detection for global uniqueness for any IPv6 address configured from the allocated IPv6 network prefix. However, the Serving GW shall respond with Neighbor Advertisement upon receiving Neighbor Solicitation messages from a given UE. For example, the UE may perform Neighbor Unreachability Detection towards the Serving GW, the Serving GW supports the DAD related functionality similar to that supported by PDN GW in the case of GTP based S5/S8 described in TS 23.401 [4], clause 5.3.1.2.2. Otherwise the PDN GW has the same functions as it is defined in TS 23.401 [4], clause 5.3.1.2.2.

  - IPv6 parameter configuration via Stateless DHCPv6 procedure does not present any architecture differences from the GTP based S5/S8 described in TS 23.401 [4], clause 5.3.1.2.3, except that the Serving GW shall have DHCPv6 relay agent functionality. The P-GW notifies the UE with the same DNSv6 information as was provided via PCO during the PDN connection establishment procedure, e.g. Attach, if DHCPv6 procedure is performed by the UE.

  - If sent, the router solicitation from the UE comes subsequent to the Attach procedure, as shown in Figure 4.7.1-2. The IPv6 network prefix assigned in the PMIP Binding Acknowledgement is sent in the Router Advertisement.

- If the PDN type associated with the PDN connection is IPv4v6:

  - The IPv6 network prefix allocation via IPv6 Stateless Address auto-configuration procedure and IPv6 parameter configuration via Stateless DHCPv6 procedure are the same as for PDN type IPv6 defined in pervious bullets.

  - If initial attach and deferred IPv4 address allocation is used, the Serving GW shall request both IPv6 network prefix and IPv4 address in the Proxy Binding Update. In this case no IPv4 address is assigned by the PDN GW during the attach procedure. Only IPv6 network prefix is returned to the Serving Gateway in the Proxy Binding Acknowledgement. The PDN GW shall also send the DHCPv4 Address Allocation Procedure Indication in the same PBA message. Then the Serving GW shall respond to the UE by setting the IPv4 PDN Address to 0.0.0.0. The UE may obtain an IPv4 address subsequently, by initiating DHCPv4 procedure as specified in figure 4.7.1-1.

  - If initial attach and deferred IPv4 address allocation is not used, the Serving GW shall request both IPv6 network prefix and IPv4 address in the Proxy Binding Update. In this case IPv4 address is assigned by the

PDN GW during the attach procedure. IPv6 network prefix and IPv4 address is returned to the Serving Gateway in the Proxy Binding Acknowledgement. The Serving GW shall deliver IPv4 address to the UE.

- For handover attach (i.e. Request Type set to "handover"), the Serving GW shall request both IPv6 network prefix and IPv4 address in the Proxy Binding Update, irrespective of whether the UE requested deferred IPv4 address or not. The previously assigned IPv6 network prefix and/or IPv4 address are returned to the Serving Gateway in the Proxy Binding Acknowledgement during the handover attach procedure. If deferred IPv4 address allocation is used for this PDN connection, the PDN GW shall also send the DHCPv4 Address Allocation Procedure Indication in the same PBA message. In this case, the UE IPv4 address is not provided as part of the default bearer activation procedures to the UE. The Serving GW shall respond to the MME by setting the PDN Address to 0.0.0.0. The MME then forwards the 0.0.0.0 address to the UE. After the default bearer establishment procedure is completed, the UE uses the connectivity with the EPS and may renew the IPv4 address allocation using DHCPv4. The IPv4 Address provided to the UE by subsequent DHCPv4, when initiated by the UE, must correspond to the value provided in the PBA.

- If the IPv4 address is provided to the UE by using DHCPv4 procedure, then at any time after the UE releases the IPv4 address using DHCPv4 or IPv4 address lease time expires, the PDN GW initiates the "PDN Gateway initiated IPv4 address Delete" procedure to delete the IPv4 address from the PDN connection and bearer contexts. The same IPv4 address shall not be allocated to another UE immediately.

- If an external PDN Address Allocation is needed, the PDN GW follows the same procedures defined in TS 23.401 [4] to obtain the external IP address after the PBU is received and before the PBA is sent.

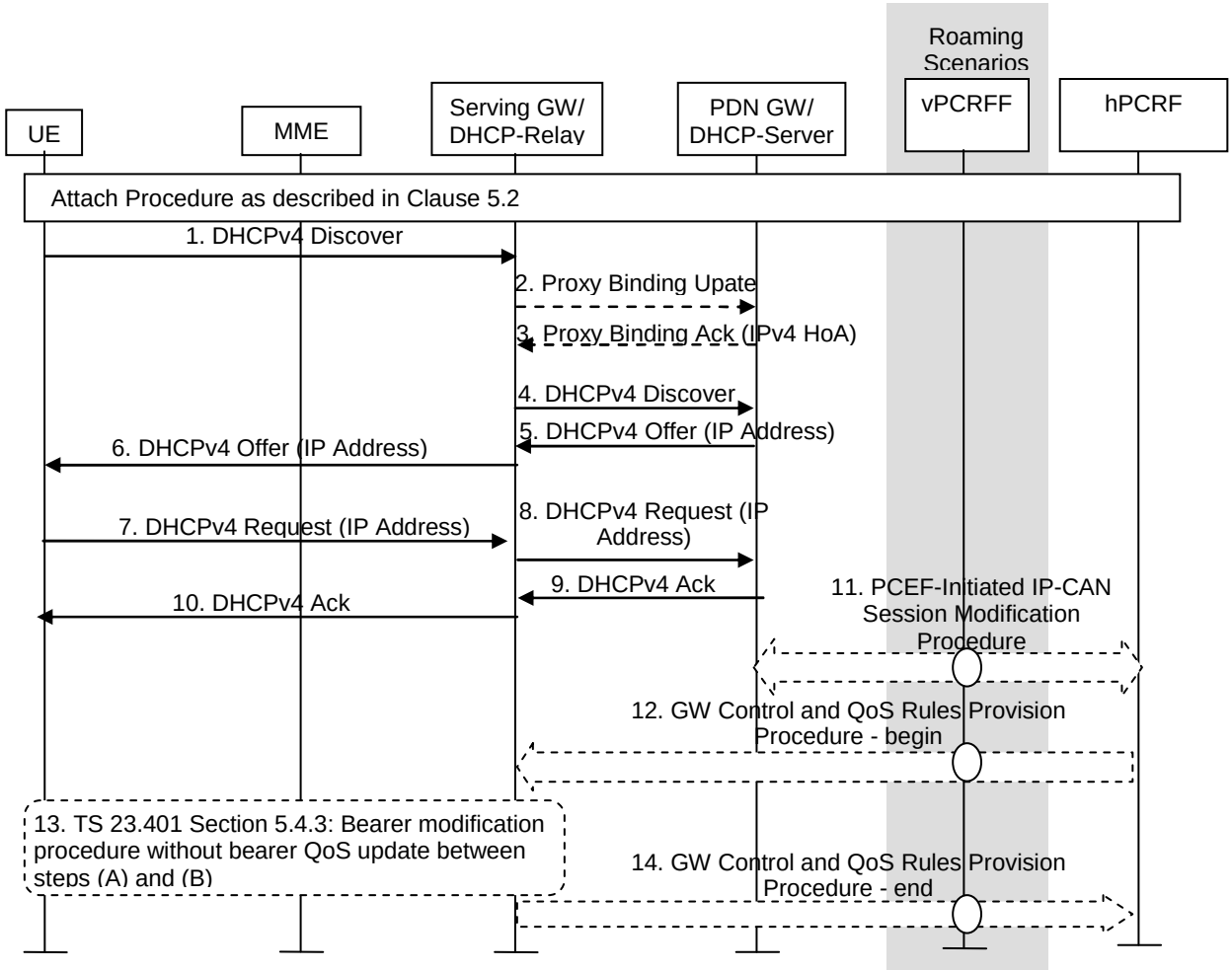


Figure 4.7.1-1: IPv4 Address Allocation using DHCP with DHCP Server Collocated with the PDN GW and DHCP Relay in the Serving GW

1. If the PDN type associated with the PDN connection is IPv4v6 or IPv4, after the default bearer is setup, the UE sends a DHCPv4 Discovery message in broadcast to the network to find available servers.

Steps 2-3 and 11-14 are only executed if the PDN type is IPv4v6 and IPv4 address was not allocated by the PDN GW in the initial attach procedure. The interaction of PBU messages (2-3) with DHCPv4 related messages (1, 4-10) is based on RFC 5844 [17].

2. The Serving GW sends a Proxy Binding Update (MN NAI, APN, UE Address Info) to the PDN GW in order to request the new IPv4 address and update the current registration. The MN NAI identifies the UE for whom the message is being sent. To request for IPv4 address for the UE, the UE Address Information should contain IPv4 address option set to 0.0.0.0, and the HNP shall be set to the HNP of the IP-CAN Session.

3. The PDN GW responds with a PMIPv6 Binding Acknowledgement (MN NAI, UE Address Info) message to the Serving GW. The MN NAI is identical to the MN NAI sent in the Proxy Binding Update. The PDN GW takes into account the request from Serving GW and the policies of operator when the PDN GW allocates the UE Address Info. The UE address info returns the assigned IPv4 Address and/or IPv6 prefix previously assigned to the UE during attach, if one was requested in the PMIPv6 Proxy Binding Update message. Otherwise, the PDN GW validates the addresses and returns in the UE Address Info IE the IPv4 address and/or IPv6 prefix received in the Proxy Binding Update message.

4. Upon receiving the DHCPv4 Discovery message, the Serving GW acting as a relay agent shall add its address in the GIADDR option and add the assigned UE IPv4 address (received from PDN GW at the PBA message), if available in the "Address Request" option, and relay the message in unicast within the PMIPv6 tunnel to PDN GW acting as a DHCPv4 server.

5. When receiving the DHCPv4 Discovery message, the PDN GW should verify the GIADDR option. Then the PDN GW uses "Address Request" option and/or the PMIPv6 tunnel on which the DHCPv4 message is received to identify the UE binding and update it with the 'client identifier' and 'chaddr' combination for subsequent DHCPv4 procedure. After that the PDN GW extends an IPv4 lease offer and sending the DHCPv4 Offer with the assigned UE IPv4 address.

6. The Serving GW acting as DHCPv4 relay agent relays the DHCPv4 message to the UE.

7. When the UE receives the lease offer, it sends a DHCPREQUEST message containing the received IPv4 address.

8. The Serving GW acting as DHCPv4 relay agent relays the DHCPv4 message to the PDN GW.

9. When the PDN GW receives the DHCPREQUEST message from the UE, it sends a DHCPACK packet to the UE. This message includes the lease duration and any other configuration information that the client might have requested.

10. The Serving GW acting as DHCPv4 relay agent relays the DHCPv4 message to the UE.

    When receiving the DHCPACK message, the UE completes TCP/IP configuration process.

11. In case a new IPv4 address is allocated, the PDN-GW initiates the PCEF initiated IP-CAN session modification procedure as described in TS 23.203 [19] to inform the PCRF of the IPv4 address allocated to the UE. If PCC rules have changed the PCRF provides the updated PCC rules to the PDN-GW as part of this procedure.

12. In case QoS rules have to be modified, e.g. change of SDF filters, the PCRF initiates a GW Control and QoS rules provision procedure as described in TS 23.203 [19] to inform the S-GW of the updated QoS rules.

13. The S-GW initiates the "Bearer Modification Procedure without bearer QoS update" as described in TS 23.401 [4], clause 5.4.3, between steps (A) and (B).

14. The S-GW informs the PCRF of the success of the QoS rules enforcement, thus ending the GW Control and QoS rules provision procedure described in TS 23.203 [19].

    The PDN GW shall discard the unicast DHCPv4 Discovery or Request message with an empty or unknown GIADDR option, if the assigned UE IPv4 address is not delivered to the UE yet.

NOTE 1: The DHCPv4 client may skip DHCPv4 Discovery phase, and send DHCPv4 Request message in broadcast as the first message. In this case, the Serving GW acting as a relay agent shall add its address in the GIADDR option and add the assigned UE IPv4 address (received from PDN GW in the PBA message) in the "Address Request" option if one was provided in the attach procedure, and relay the message in unicast within the PMIPv6 tunnel to PDN GW acting as a DHCPv4 server.

NOTE 2: After releasing the IPv4 address using DHCPv4 Release procedure, UE can request an IPv4 address for the same PDN connection subsequently.

NOTE 3: Allocation of IP address from an external PDN using Radius or Diameter requires the "Proxy Binding Update" of PMIPv6 to carry the relevant PCO that is transported by GTP.

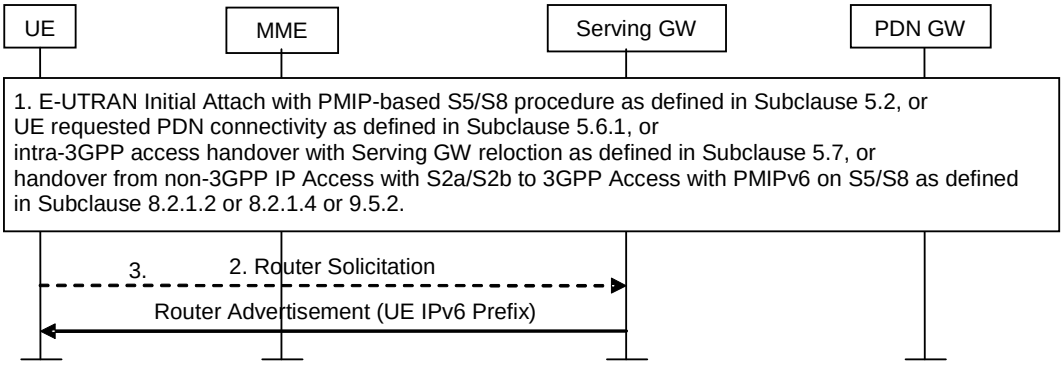


Figure 4.7.1-2: IPv6 Prefix allocation after the PDN connection setup procedure

1. A PDN connection is setup over 3GPP access, after the E-UTRAN initial Attach with PMIP-based S5/S8 procedure as defined in clause 5.2, UE requested PDN connectivity as defined in clause 5.6.1, or intra-3GPP access handover with Serving GW relocation as defined in clause 5.7, or handover from non-3GPP IP Access with S2a/S2b to 3GPP Access with PMIPv6 on S5/S8 as defined in clause 8.2.1.2 or 8.2.1.4.

2. If the PDN type associated with the PDN connection is IPv4v6 or IPv6, the UE may send a Router Solicitation message to the network to solicit a Router Advertisement message.

3. Upon receiving the Route Solicitation message or after the PDN connection setup procedure, the Serving GW shall send an IPv6 Router Advertisement message as specified in IETF RFC 4862 [58] to the UE for PDN connection type IPv4v6 or IPv6 (i.e. the Serving GW acts as an advertising interface as specified in IETF RFC 4861 [59] for the PDN connection type IPv4v6 or IPv6). The Router Advertisement messages shall contain the assigned IPv6 prefix received in the PMIPv6 Binding Acknowledgement message. After the UE has received the Router Advertisement message, it constructs a full IPv6 address via IPv6 Stateless Address autoconfiguration in accordance with IETF RFC 4862 [58]. However, the UE shall not use any identifiers defined in TS 23.003 [16] as the basis for generating the interface identifier. For privacy, the UE may change the interface identifier used to generate full IPv6 address, as defined in TS 23.221 [60] without involving the network.

NOTE 4: In order to renew the allocated IPv6 prefix, the Serving GW sends an IPv6 Router Advertisement (solicited or unsolicited) to the UE i.e. the Serving GW acts as an advertising interface as specified in IETF RFC 4861 [59] for the PDN connection type IPv4v6 or IPv6.

When sending the IPv6 Router Advertisement message, the Serving GW may trigger the paging (e.g. by sending a Downlink Data Notification message to the MME) if the UE is in idle state.

4.7.2 IP Address Allocation in Trusted Non-3GPP IP Access using PMIPv6 on S2a

IP address is allocated to the UE when connectivity to new PDN is initiated. The IP address can be provided by either PDN GW or external PDN. Access GW in trusted non-3GPP access system is responsible for delivering the IP address to the UE. Based on the signalling between the UE and the non-3GPP IP access system the UE should be able to know the connected PDN identity (APN). This enables the UE to uniquely associate each allocated IP address with the PDN from where it was allocated.

The trusted non-3GPP Access shall support at least one of the following functionalities in order to successfully allocate IP address to the UE in the EPC:

- Support of DHCPv4 relay agent functionality for IPv4 parameter configuration and IP address allocation as specified in RFC 2131 [28] and RFC 4039 [29] and described in clause 4.7.1 for the Serving GW. This

functionality is used to support DHCPv4 based IPv4 address allocation mechanism in the UE. For this case the following applies:

- At initial attach or handover attach, if the PDN type is IPv4 only, the trusted non-3GPP IP Access shall request IPv4 address in the Proxy Binding Update. The Protocol Configuration Options in the Proxy Binding Update includes the Address Allocation Preference to indicate that deferred IPv4 address allocation was requested by the UE. In the same way as it is defined in clause 4.7.1, the IPv4 address is assigned by the PDN GW during the initial attach procedure and the IPv4 address is returned in the Proxy Binding Acknowledgement. The DHCPv4 Address Allocation Procedure Indication is included in the Proxy Binding Acknowledgement to indicate that IPv4 address allocation using DHCPv4 is allowed. The MAG shall not deliver the assigned IPv4 address to the UE before the DHCPv4 address allocation. After the PMIPv6 tunnel is set up between the trusted non-3GPP Access and the PDN GW, the trusted non-3GPP Access may relay the DHCPv4 messages between the UE and the PDN GW for IPv4 parameter configuration and IPv4 address allocation as specified for the Serving GW in figure 4.7.1-1.

- At initial attach and handover attach, if the PDN type is IPv4v6 and deferred IPv4 address allocation is used, the trusted non-3GPP IP Access shall request both IPv6 network prefix and IPv4 address in the Proxy Binding Update. The Protocol Configuration Options in the Proxy Binding Update includes the Address Allocation Preference to indicate that deferred IPv4 address allocation was requested by the UE. In the same way as it is defined in clause 4.7.1, if deferred IPv4 address allocation is allowed, no IPv4 address is assigned by the PDN GW during the initial attach procedure, only IPv6 network prefix is returned in the Proxy Binding Acknowledgement. The DHCPv4 Address Allocation Procedure Indication is included in the Proxy Binding Acknowledgement to indicate that IPv4 address allocation using DHCPv4 is allowed. After the PMIPv6 tunnel is set up between the Trusted Non-3GPP IP Access and the PDN GW, when the UE requests the IPv4 address via DHCPv4, the trusted non-3GPP Access and PDN GW perform steps 2 and 3 in Figure 4.7.1-1, and then the non-3GPP Access may relay the DHCPv4 messages between the UE and the PDN GW for IPv4 parameter configuration and IPv4 address allocation as specified in figure 4.7.1-1.

- Any time after the UE releases the IPv4 address using DHCPv4 or IPv4 address lease time expires, and if the PDN Type is IPv4, the PDN GW initiates "PDN-GW-initiated PDN-disconnection" procedure for the given PDN connection. The same IPv4 address shall not be allocated to another UE immediately.

- Any time after the UE releases the IPv4 address using DHCPv4 or IPv4 address lease time expires, and if the PDN Type is IPv4v6, the PDN GW initiates the "PDN GW initiated IPv4 address Delete Procedure" procedure to delete the IPv4 address from the PDN connection and from bearer contexts. The same IP address shall not be allocated to another UE immediately.

- Support of DHCPv4 server functionality for IPv4 parameter configuration and IP address allocation as specified in RFC 2131 [28] and RFC 4039 [29]. This functionality is used to support DHCPv4 based IPv4 address allocation mechanism in the UE. For this case the following applies:

  - At initial attach and handover attach, if the PDN type is IPv4v6 and deferred IPv4 address allocation is used, the trusted non-3GPP IP Access shall request both IPv6 network prefix and IPv4 address in the Proxy Binding Update. The Protocol Configuration Options in the Proxy Binding Update includes the Address Allocation Preference to indicate that deferred IPv4 address allocation was requested by the UE. In the same way as it is defined in clause 4.7.1, if deferred IPv4 address allocation is allowed, no IPv4 address is assigned by the PDN GW during the initial attach procedure, only IPv6 network prefix and the DHCPv4 Address Allocation Procedure Indication are returned in the Proxy Binding Acknowledgement. After the PMIPv6 tunnel is set up between the Trusted Non-3GPP IP Access and the PDN GW, when the UE requests the IPv4 address via DHCPv4, the MAG in Trusted Non-3GPP IP Access requests the IPv4 address for the UE from the PDN GW via PMIPv6 signalling as it is described in Figure 4.7.2-1.

NOTE 1: At initial attach and handover attach, if the PDN type is IPv4, the trusted non-3GPP IP Access requests IPv4 address in the Proxy Binding Update and the PDN GW returns an IPv4 address in the Proxy Binding Acknowledgement. In this case the PDN GW is not aware of how and when the IPv4 address is delivered to the UE.

- Any time after the UE releases the IPv4 address using DHCPv4 or IPv4 address lease time expires, and if the PDN Type is IPv4, the trusted non-3GPP access system will initiate "Trusted Non-3GPP IP Access requested PDN Disconnection Procedure with PMIPv6" procedure for the given PDN connection. The same IP address shall not be allocated to another UE immediately.

- Any time after the UE releases the IPv4 address using DHCPv4 or IPv4 address lease time expires, and if the PDN Type is IPv4v6, the non-3GPP access may initiate "Non-3GPP access initiated IPv4 address Delete

Procedure" procedure to delete the IPv4 address from the PDN connection and bearer contexts. The same IP address shall not be allocated to another UE immediately.

- Support of DHCPv6 (relay agent or server) functionality for IPv6 parameter configuration as specified in RFC 3736 [30]. This functionality is required to support DHCPv6 based parameter configuration mechanism in the UE.

- Support of prefix advertisement for IPv6 prefix received from PDN GW in PMIPv6 Proxy Binding Acknowledgement.

- Support for IPv4 Address allocation that is received from PDN GW from PMIPv6 Proxy Binding Acknowledgement using access specific mechanisms.

NOTE 2: Configuration parameters are received from the PDN GW by using DHCPv4/v6 (the non-3GPP Access GW acting as DHCPv4/v6 relay towards the PDN GW) or PMIPv6 PCO in the PBA message.

NOTE 3: When DHCPv4/v6 is used between the non-3GPP Access GW and PDN GW, the DHCPv4/v6 messages are sent within the PMIPv6 tunnel.

NOTE 4: After releasing the IPv4 address using DHCPv4 Release procedure, UE can request an IPv4 address for the same PDN connection subsequently.

- Support of static IP address allocation. The non-3GPP access may receive a static IP address (i.e. a static IPv4 address and/or a static IPv6 prefix) from HSS/AAA during access authentication and authorization procedure. Then the non-3GPP access should forward the static IP address to the PDN GW.

NOTE 5: For static address allocation, a static PDN GW is selected by either having the APN configured to map to a given PDN GW, or the PDN GW identity provided by the HSS/AAA indicates the static PDN GW.

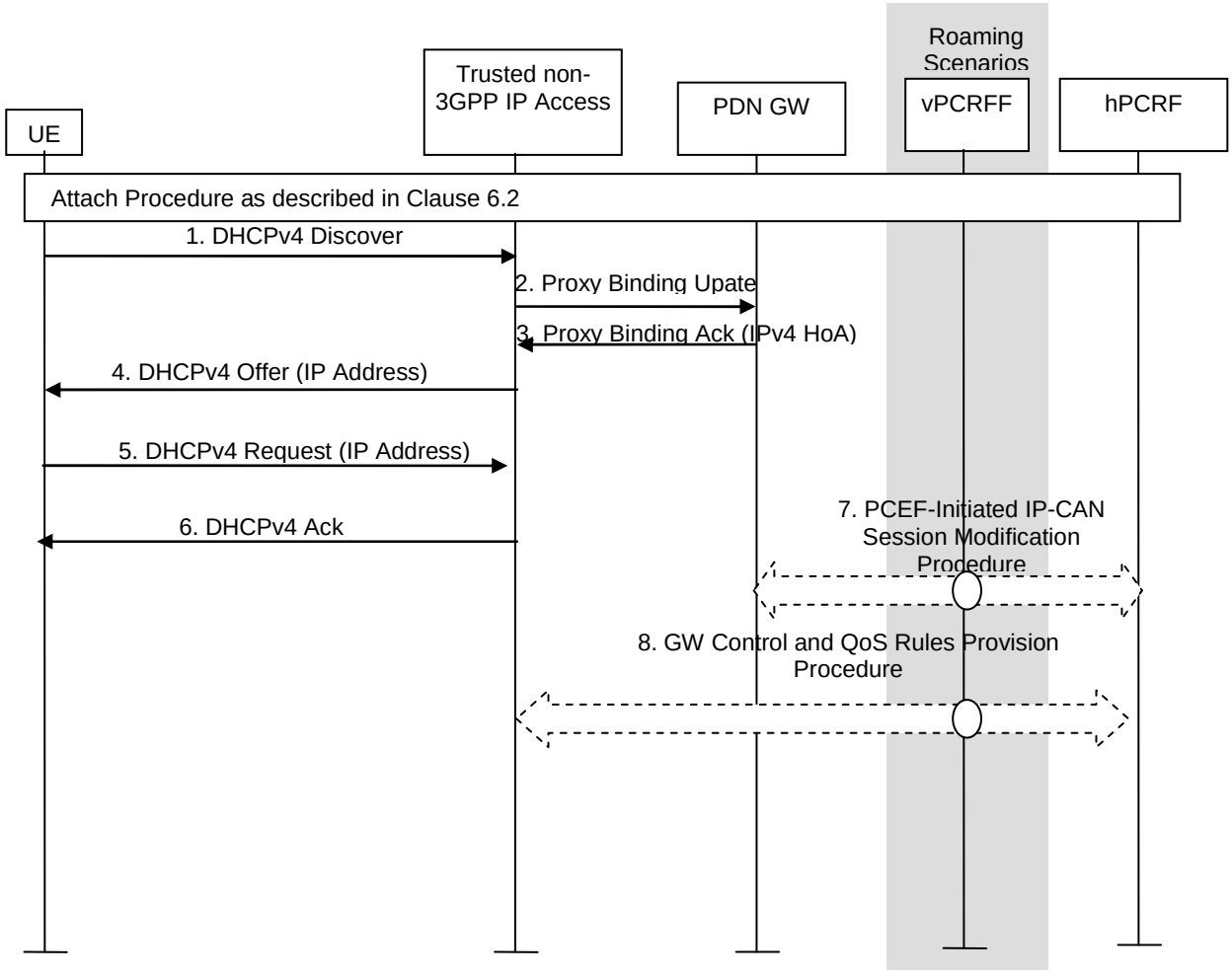


Figure 4.7.2-1: IPv4 Address Allocation using DHCP with DHCP Server Collocated with the MAG when PDN type is IPv4v6

1. If the PDN type associated with the PDN connection is IPv4v6, after the PDN connection establishment, the UE sends a DHCPv4 Discovery message in broadcast to the network to find available servers.

2. The MAG in the Trusted Non-3GPP IP Access sends a Proxy Binding Update (MN NAI, APN, UE Address Info) to the PDN GW in order to request the new IPv4 address and update the current registration. The MN NAI identifies the UE for whom the message is being sent. To request for IPv4 address for the UE, the UE Address Information should contain IPv4 address option set to 0.0.0.0, and the HNP shall be set to the HNP of the PDN connection.

3. Upon receiving the PBU message from the Trusted Non-3GPP IP Access the PDN GW allocates an IPv4 address for the UE in accordance with the operator's policies. The PDN GW responds with a PMIPv6 Binding Acknowledgement (MN NAI, UE Address Info) message to the Trusted Non-3GPP IP Access. The MN NAI is identical to the MN NAI sent in the Proxy Binding Update. The UE address info returns the assigned IPv4 Address and IPv6 prefix previously assigned to the UE during attach.

4. The Trusted Non-3GPP IP Access acting as a DHCPv4 server sends the DHCPv4 Offer with the assigned UE IPv4 address received in the PBA message in step 3.

5. When the UE receives the lease offer, it sends a DHCPREQUEST message containing the received IPv4 address.

6 The MAG in the Trusted Non-3GPP IP Access acting as DHCPv4 server sends a DHCPACK packet to the UE. This message includes the lease duration and any other configuration information that the client might have requested.

   When receiving the DHCPACK message, the UE completes TCP/IP configuration process.

7. In case a new IPv4 address is allocated, the PDN-GW initiates the PCEF initiated IP-CAN session modification procedure as described in TS 23.203 [19] to inform the PCRF of the IPv4 address allocated to the UE. If PCC rules have changed the PCRF provides the updated PCC rules to the PDN-GW as part of this procedure. This step can happen any time after step 3.

8. In case QoS rules have to be modified, e.g. change of SDF filters, the PCRF initiates a GW Control and QoS rules provision procedure as described in TS 23.203 [19] to inform the S GW of the updated QoS rules.

NOTE 6: The DHCPv4 client may skip DHCPv4 Discovery phase, and send DHCPv4 Request message in broadcast as the first message.

NOTE 7: After releasing the IPv4 address using DHCPv4 Release procedure, UE can request an IPv4 address for the same PDN connection subsequently.

4.7.3 IP Address Allocation in Untrusted Non-3GPP IP Access using PMIPv6 or GTP on S2b

When an Untrusted Non-3GPP IP access is used two types of IP address are allocated to the UE:

- An IP address, which is used by the UE within the Untrusted Non-3GPP IP Access Network to get IP connectivity towards the ePDG.

- One or more IP address(es), which is used by the UE towards the external PDNs via the allocated PDN GW(s).

The IP address that is allocated by the Untrusted Non-3GPP IP Access Network is used as the end point of the IPSec SAs between the UE and the ePDG. The allocation of this IP address is out of the scope of this specification.

The IP address(es) that are allocated by the PDN GW(s) are allocated to the UE when connectivity to a new PDN is initiated. The IP address(es) can be provided by either PDN GW or external PDN as it is specified in clause 5.3.1.1 of TS 23.401 [4]. The ePDG receives the allocated IP address(es) within the PMIP Proxy Binding Acknowledgement or GTP Create Session Response and the ePDG is responsible for delivering the IP address(es) to the UE. The ePDG shall provide the UE with connected PDN information (APN), so that the UE can uniquely associate each allocated IP address with the PDN from where it was allocated.

The ePDG may receive a static IP address (i.e. a static IPv4 address and/or a static IPv6 prefix) from HSS/AAA during IKEv2 tunnel establishment procedure. Then the ePDG should forward the static IP address to the PDN GW.

NOTE: For static address allocation, a static PDN GW is selected by either having the APN configured to map to a given PDN GW, or the PDN GW identity provided by the HSS/AAA indicates the static PDN GW.

4.7.4 IP Address Allocation using S2c

Prior the use of S2c an IP address which will be used as a care-of address shall be allocated to the UE.

When a Trusted Non-3GPP Access Network is used one or more IP addresses are allocated to the UE by the Trusted Non-3GPP Access Network. One of these IP addresses is used by the UE as care-of address within DSMIPv6. The allocation of these IP addresses is out of the scope this specification.

When an Untrusted Non-3GPP Access Network is used one or more IP addresses are allocated to the UE by the Untrusted Non-3GPP Access Network. The allocation of these IP addresses is out of the scope of 3GPP. One of these IP addresses is used by the UE as the IP address towards the ePDG when IPSec SAs are established. During the IPSec SA establishment the ePDG allocates and delivers an IP address to the UE, which IP address is used by the UE as care-of address within DSMIPv6. This IP address is allocated by the ePDG either by using an internal address pool or using an external server, such as DHCP. The allocation of this IP address is implementation specific.

When a UE is connecting to a PDN via S2c, address allocation for that PDN takes place as follows.

During IKEv2 exchange for bootstrapping the DSMIPv6 security association (see clause 6.3) the following parameters can be negotiated between the UE and the PDN GW/HA:

- The IPv6 prefix to which the IPv6 Home Address belongs, also called the "Home Network Prefix" and the PDN associated with the IPv6 prefix (PDN is indicated with APN);
- The UE's IPv6 Home Address;
- The DNS server address for that PDN.

The UE may request additional configuration parameters by running stateless DHCP as defined in RFC 4039 [29] and RFC 3736 [30] over the DSMIPv6 tunnel.

The UE may also request an IPv4 home address using DSMIPv6 signalling, as defined in RFC 5555 [10].

The PDN GW/HA may receive a static IP address (i.e. a static IPv4 address and/or a static IPv6 prefix) from HSS/AAA during the authentication and authorization procedure. Then the PDN GW/HA shall assign the static IP address to the UE, as indicated above.

NOTE: The UE selects a PDN GW as specified in clause 4.5.2. In case the PDN GW selected by the UE is different from the static PDN GW stored in the HSS, the PDN GW reallocation procedure (see clause 6.10) shall be performed.

4.7.5 IPv6 Prefix Delegation using S2c

Optionally a single network prefix shorter than a /64 prefix may be assigned to a PDN connection (TS 23.401 [4]). When S2c is used to access a PDN, the UE acting as a Mobile Router may request delegation of one or more IPv6 prefix(es) via DHCPv6 Prefix Delegation signalling as described in RFC 6276 [56]. The UE does not need to explicitly register these additional prefixes using S2c signaling as implicit mode registration is used.

4.7.6 IPv6 Prefix Delegation using PMIP-based S5/S8

Optionally a single network prefix shorter than the default /64 prefix may be assigned to a PDN connection as specified in 3GPP TS 23.401 [4]. When PMIP-based S5/S8 is used, the UE may request delegation of one or more IPv6 prefix(es) via DHCPv6 Prefix Delegation signalling as described in RFC 7148 [82]. In this case, the Serving GW shall support DHCPv6 relay agent functionality for intercept the related DHCPv6 message. The UE uses DHCPv6 to request additional IPv6 prefixes (i.e. prefixes in addition to the default prefix) from the PDN GW after completing stateless IPv6 address autoconfiguration procedures as specified in figure 4.7.6-1.

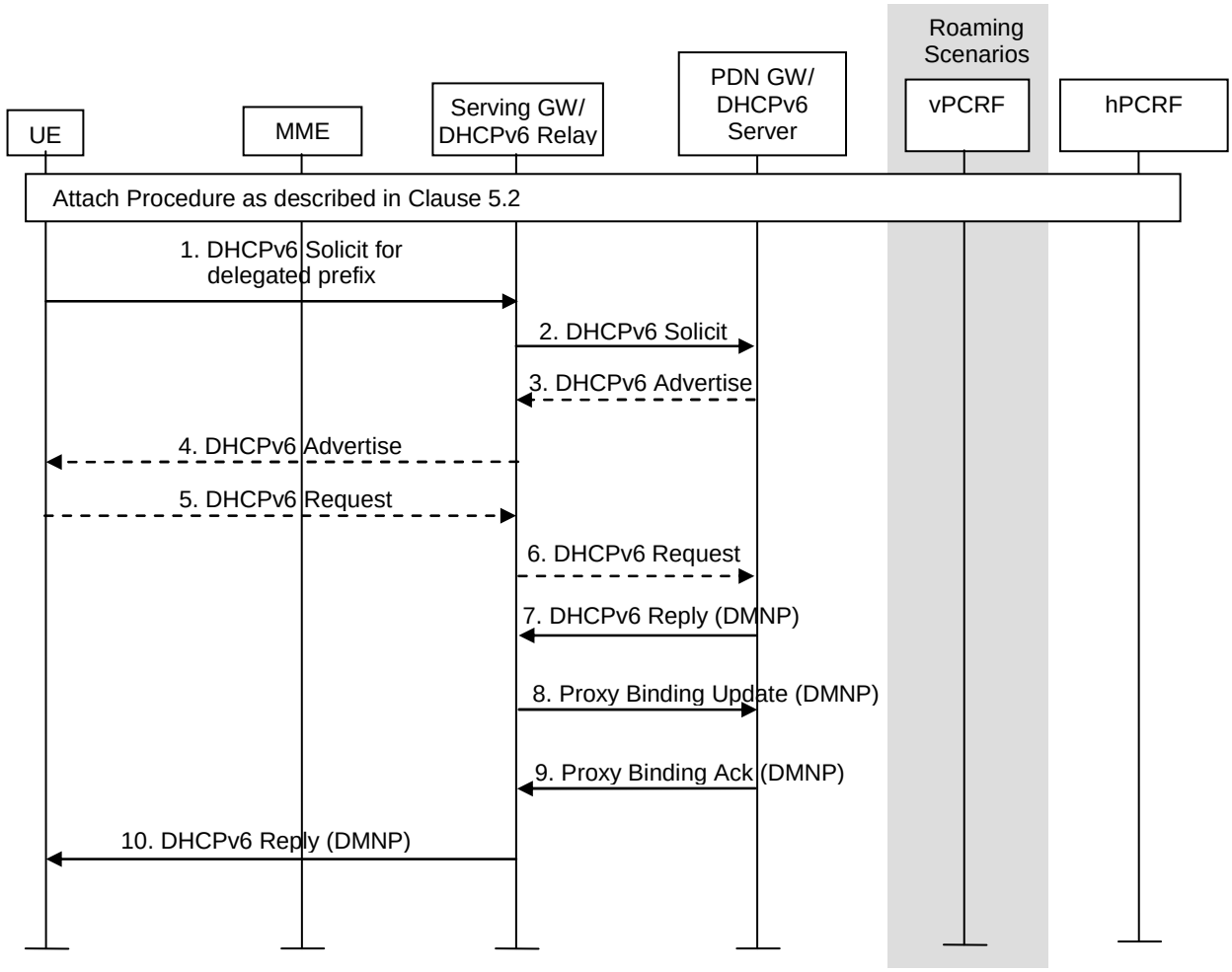


Figure 4.7.6-1: Prefix Delegation with DHCP Server Collocated with the PDN GW and DHCP Relay in the Serving GW when using PMIP-based S5/S8

1. If the PDN type associated with the PDN connection is IPv4v6 or IPv6, after the PMIPv6 tunnel is setup, the UE sends a DHCPv6 Solicit message including the IA_PD option to the Serving GW to acquire a network prefix shorter than a /64 prefix.

2. The DHCPv6 relay agent in the Serving GW shall relay the DHCPv6 solicit message within the PMIPv6 tunnel to PDN GW acting as a DHCPv6 server.

3-7. The DHCPv6 procedures is then completed as described in RFC 3633 [81] ending with the delegating router sending a Reply message conveying the delegated prefixes.

8. Once the Serving GW receives the set of delegated prefixes from the delegating router function running on thePDN GW, the Serving GW shall send the delegated prefixes in a Proxy Binding Update.

9. On reception of the PBU the PDN GW returns the assigned prefix in the DMNP option carried by a PBA to the Serving GW. The PDN GW shall add the assigned prefix to the binding cache which is extended as specified in RFC 7148 [82].

10. The Serving GW acting as DHCPv6 relay agent relays the DHCPv6 Reply message with deleageted prefix to the UE.

NOTE: Steps 3 to 6 can be skipped if DHCPv6 Rapid Commit is used.

4.8 Network Discovery and Selection

4.8.0 General Principles

Access network selection and traffic steering between 3GPP access and WLAN is supported using ANDSF and is also supported using RAN rule procedures without ANDSF. Clause 4.8 focuses on Network Discovery and Selection using ANDSF. Access network selection and traffic steering using RAN rules when ANDSF is not applied is described in TS 23.401 [4], clause 4.3.23 and TS 23.060 [21], clause 5.3.21, as well as in E-UTRAN and UTRAN specifications as referenced therein. Coexistence between ANDSF and RAN rules is described in clause 4.8.6.4.

The following principles apply when the UE is registered in the Home PLMN or in a PLMN which is equivalent to the home PLMN and when both 3GPP and non-3GPP accesses are available or when multiple non-3GPP accesses are available:

- The EPS network may provide the UE with assistance data/policies about available accesses located in the Home PLMN or in a PLMN equivalent to the Home PLMN, to allow the UE to scan for accesses and select an access.

- If the UE is capable of routing different IP flows to the same PDN connection through different access networks (see TS 23.261 [55]), the EPS network shall allow the operator to influence the access where a specific IP flow shall be routed.

- If the UE is capable of routing different simultaneously active PDN connections through different access networks, the EPS network shall allow the operator to influence the access where a specific PDN connection shall be routed.

- Assistance data/policies are provided only after establishing secure communication, as specified in TS 33.402 [45].

- The assistance data/policies provided to UE may depend on the UE's subscription data.

- The EPS network allows the operator to influence the access that the UE shall handover to (when in active mode) or re-select (when in idle mode).

- Multi-access network discovery and selection works for both single-radio and multiple- radio terminals. For the case of multiple-radio terminals, multi-access network discovery and selection works without requiring all radios supported by the UE to be switched on.

- No architectural impact is foreseen for network selection upon initial network attachment.

- The UE may provide information to the network for the retrieval of the assistance data/policies.

The following principles apply when the UE is registered in a Visited PLMN (VPLMN) and when both 3GPP and non-3GPP accesses are available or when multiple non-3GPP accesses are available:

- The VPLMN shall be able to provide Access Network Discovery information only for 3GPP and non-3GPP access networks that provide connectivity to the VPLMN or to a PLMN equivalent to the VPLMN, or to both.

- The VPLMN shall be able to provide to a roaming UE Inter-System Mobility Policies and/or Inter System Routing Policies (see clause 4.8.2.1). Such policies shall be valid only in the VLPMN or in a PLMN equivalent to the VPLMN, as per roaming agreements.

- The Home PLMN (HPLMN) shall be able to provide to a roaming UE Access Network Discovery information for 3GPP and non-3GPP access networks that provide connectivity to the HPLMN or to a PLMN equivalent to the HPLMN, or to both.

- The HPLMN shall be able to provide to a roaming UE Inter-System Mobility Policies and/or Inter System Routing Policies.

- When the UE receives Inter System Routing Policies from the HPLMN and the VPLMN, it shall select the active rule according to clause 4.8.2a.1.

- When the UE receives Inter System Mobility Policies from the HPLMN and the VPLMN, it shall select the active rule according to clause 4.8.2a.1.

- The VPLMN shall not provide Inter-APN Routing Policies, and the UE shall ignore any Inter-APN Routing Policy, which is delivered by a VPLMN.

The multi-access network discovery and selection mechanism shall not interfere with the existing 3GPP PLMN selection mechanisms used for the 3GPP Access Technologies (specified in TS 23.122 [53]) and with the existing 3GPP2 network selection mechanisms. The multi-access network discovery and selection procedures defined in this document include a WLAN access selection procedure and a PLMN selection procedure for WLAN access (see clause 4.8.2b), which are different from and shall not be used in conjuction with the procedures for I-WLAN access (specified in TS 23.234 [5]). For WLAN access selection and PLMN selection, the procedures defined in the present document replace I-WLAN procedures specified in TS 23.234 [5].

The ANDSF's policy and the UE implementation shall ensure that PLMN changes are not conducted more often than the time stored in the USIM (in EF_{HPPLMN}, see TS 31.102 [46]) for the "periodic network selection attempts" specified in TS 22.011 [47].

NOTE: A change between the HPLMN and another PLMN equivalent to the HPLMN can be triggered by the ANDSF, but is not considered a PLMN reselection.

4.8.1 Architecture for Access Network Discovery Support Functions

The following architecture may be used for access network discovery and selection. The support and the use of these functions and interfaces are optional.

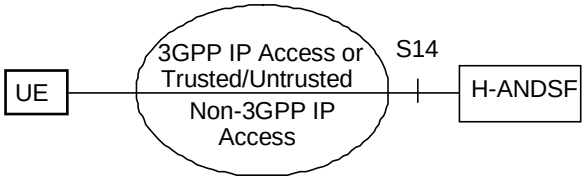


Figure 4.8.1.1-1: Non-Roaming Architecture for Access Network Discovery Support Functions

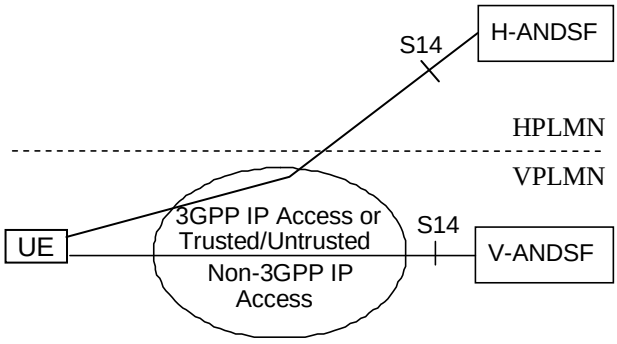


Figure 4.8.1.1-2: Roaming Architecture for Access Network Discovery Support Functions

The architecture is based on a new network element called Access Network Discovery and Selection Function (ANDSF). An ANDSF element located in the home PLMN of a UE is referred to as the Home-ANDSF (H-ANDSF) for this UE, whereas an ANDSF element located in the visited PLMN of a UE is referred to as the Visited-ANDSF (V-ANDSF) for this UE. Unless otherwise specified, the term ANDSF is used to refer to both an H-ANDSF and a V-ANDSF. Details about the ANDSF functionality and its interaction with the UE are provided in clause 4.8.2.1.

The ANDSF is an optional element in the network architecture and thus a UE may or may not be able to interact with an H-ANDSF and/or with a V-ANDSF.

The UE-ANDSF interaction can take place via non-seamless WLAN offload (see clause 4.1.5) or via any 3GPP or non-3GPP access technology that can be used by the UE to access EPC.

NOTE: ANDSF push interactions might not always be possible via non-seamless WLAN offload.

4.8.2 Network Elements

4.8.2.1 Access Network Discovery and Selection Function (ANDSF)

4.8.2.1.1 General

The ANDSF contains data management and control functionality necessary to provide network discovery and selection assistance data as per operators' policy. The ANDSF shall respond to UE requests for access network discovery information (pull mode operation) and may be able to initiate data transfer to the UE (push mode operation), based on network triggers or as a result of previous communication with the UE.

NOTE 1: In this Release, the OMA DM Push mechanism may not work in all possible scenarios and the ANDSF may not always be able to initiate a session to the UE.

NOTE 2: The usage of ANDSF capabilities is intended for scenarios where access-network level solutions are not sufficient for the UE to perform Network Discovery and Selection of non-3GPP technologies according to operator policies.

The ANDSF shall comply with regulatory requirements pertaining to the privacy and confidentiality of user location information.

Subject to operator's configuration, the ANDSF may obtain the permanent UE identity, e.g. based on the security solution specified in TS 33.402 [45].

The H ANDSF in the subscriber's home operator network may interact with other databases such as the HSS user profile information residing in subscriber's home operator network. Details of such interaction with these databases are not described in this Release of the specifications.

The ANDSF shall be able to provide various types of information, e.g. inter-system mobility policy, network access discovery information, etc. These types of information are specified in the following clauses.

The ANDSF may provide to UE all types of information or only one of them.

The H-ANDSF selects the types of information to be delivered to the UE according to the operator requirements and the roaming agreements. If the permanent UE identity is known to the H-ANDSF, and subject to operator's configuration, the available subscription data (e.g. the list of access networks, or access technology types, the UE is authorized to use, etc.) may also be used by the H-ANDSF for selecting the inter-system mobility policies, the access network discovery information, the inter-system routing policies and the inter-APN routing policies.

The V-ANDSF selects the types of information to be delivered to the UE according to the operator requirements and the roaming agreements. However, the V-ANDSF shall not deliver IARP policy (see clause 4.8.2.1.5) to a roaming UE.

The ANDSF shall be able to limit the amount of information provided to the UE based e.g. on the UE's current location, UE capabilities, etc. The ANDSF shall be able to limit the load caused by the UE initiated requests towards the ANDSF.

The information provided by ANDSF may also be pre-configured by the home operator on the ME or provisioned on the UICC. The UE shall use the ANDSF information in the following order:

1) ANDSF information provided by the ANSDF server to the ME;

2) ANDSF information configured on the UICC;

3) ANDSF information pre-configured on the ME.

The visited operator cannot pre-configure ANDSF information in the UE.

4.8.2.1.2 Inter-System Mobility Policy

The Inter-System Mobility Policy (ISMP) is a set of operator-defined rules that affect the inter-system mobility decisions taken by the UE. The UE uses the inter-system mobility policy when it can route IP traffic only over a single

radio access interface at a given time (e.g. is neither IFOM nor MAPCON capable or its IFOM and MAPCON capabilities are disabled) in order to select the most preferable access technology type or access network that should be used to connect to EPC.

The inter-system mobility policy may be provisioned in the UE and may be updated by the ANDSF based on network triggers or after receiving a UE request for network discovery and selection information.

Each ISMP rule includes the following information:

- Validity conditions, i.e. conditions indicating when the rule is valid (such conditions may include e.g. a time duration, a location area, etc.).
- A prioritized list of access technologies or access network that indicate the order in which they are preferred or restricted for EPC connectivity.
- A rule priority that indicates the priority of this rule with respect to other ISMP rules provided by the same PLMN.

For example, an ISMP rule may indicate that 3GPP access is preferable to WLAN access for EPC connectivity. When this rule is applied, inter-system handover from 3GPP access to WLAN access is not allowed. The rule may also indicate e.g. that WiMAX access is more preferable to WLAN access.

NOTE: The inter-system mobility policy does not indicate the most preferable access network or access technology type that should be used to access CS services.

The home operator may provide ISMP rules to UE via the H-ANDSF or may pre-configure the UE with ISMP rules. The ISMP rules provided to UE via the H-ANDSF shall take precedence over the pre-configured ISMP rules in the UE.

4.8.2.1.3 Access Network Discovery Information

Upon UE request, the ANDSF may provide a list of access networks available in the vicinity of the UE for all the access technology types requested by the UE (if any requested).

The ANDSF provides information for access networks that are available to the UE including:

- the access technology type (e.g. WLAN, WiMAX).
- the radio access network identifier (e.g. the SSID of a WLAN).
- other technology specific information, e.g. one or more carrier frequencies.
- validity conditions, i.e. conditions indicating when the provided access network discovery information is valid (such conditions may include e.g. a location).

The UE may retain and use the access network discovery information provided by the ANDSF until new/updated information is retrieved.

4.8.2.1.4 Inter-System Routing Policy

The Inter-System Routing Policy (ISRP) is a set of operator-defined rules that determine how the UE should route IP traffic across multiple radio access interfaces. The ANDSF may provide a list of ISRP rules to the UE independently of the UE capability to route IP traffic simultaneously over multiple radio access interfaces. The UE uses the ISRP rules when it can route IP traffic simultaneously over multiple radio access interfaces (e.g. it is an IFOM capable UE with the IFOM capability enabled or a MAPCON capable UE with the MAPCON capability enabled) in order to meet the operator routing / offload preferences by:

(i) deciding when an access technology type / access network is restricted for a specific IP traffic flow and/or a specific APN; and

(ii) selecting the most preferable access technologies / access networks which should be used by the UE when available to route IP traffic that matches specific criteria (e.g. all traffic to a specific APN, or all traffic belonging to a specific IP flow, or all traffic of a specific application, etc).

The inter-system routing policy may be provisioned in the UE and may be updated by the ANDSF based on network triggers or after receiving a UE request for network discovery and selection information.

Each ISRP rule includes the following information:

- Rules for IFOM: Each one of these rules identifies a prioritised list of access technologies / access networks which should be used by the UE when available to route traffic that matches specific IP traffic filters on a specific APN or on any APN. A rule for IFOM can also identify which radio accesses are restricted for traffic that matches specific IP traffic filters on aspecific APN (e.g. WLAN is not allowed for RTP/RTCP traffic flows on APN-x) or on any APN;

    - Each rule for IFOM contains one or more IP traffic filters (to match specific IP traffic), a prioritised list of access technologies / access networks, a rule priority and, optionally, validity conditions that indicate when the rule is valid. Each IP traffic filter may identify traffic based on destination address, transport protocol, destination/source port numbers, DSCP or Traffic Class, destination domain name and application identity.

NOTE 1: IP traffic filters in ANDSF policies are applied in the UE for uplink traffic. Thus the source port in this context is the source port within the IP packet sent by the UE; the destination address and port are the destination address and port in the IP packets sent by the UE.

- Rules for MAPCON: Each one of these rules identifies a prioritised list of access technologies / access networks which should be used by the UE when available to route PDN connections to specific APNs. A rule for MAPCON can also identify which radio accesses are restricted for PDN connections to specific APNs (e.g. WLAN is not allowed for PDN connection to APN-x);

    - Each rule for MAPCON contains an APN value, a prioritised list of access technologies / access networks, a rule priority and, optionally, validity conditions that indicate when the rule is valid. When no APN value is contained, the rule applies to any APN.

- Rules for Non-seamless WLAN Offload (NSWO) specified in clause 4.1.5: Each one of these rules identifies which traffic shall or shall not be non-seamlessly offloaded to a WLAN when available. It shall be possible to restrict certain traffic from using non-seamless WLAN offload only in specific WLAN access networks or in all WLAN access networks. Similarly, it shall be possible to permit certain traffic to use non-seamless WLAN offload only in specific WLAN access networks or in all WLAN access networks.

    - Each rule for NSWO contains one or more IP traffic filters (to match specific IP traffic), a rule priority and, optionally, validity conditions that indicate when the rule is valid. Each IP traffic filter may identify traffic based on destination address, transport protocol, destination/source port numbers, DSCP or Traffic Class, destination domain name and application identity.

The prioritised list of access technologies included in the rules for IFOM and MAPCON may contain 3GPP access, WLAN access as well as specific 3GPP RATs such as GERAN, UTRAN and E-UTRAN. The order of the access technologies in this list allows the operator to prioritize specific 3GPP RATs with respect to WLAN access. The UE shall use the prioritised list of access technologies in these rules only for IP routing and PDN connection establishment. The UE shall not use this prioritised list for 3GPP RAT selection.

NOTE 2: For example, if the UE camps on UTRAN and the prioritised list of access networks in the active IFOM rule indicates that E-UTRAN has the highest priority for an IP flow, this rule does not trigger the UE to re-select to E-UTRAN for routing the IP flow.

If more than one valid rule for IFOM and non-seamless WLAN offload match a specific IP traffic flow, the UE applies the rule with the highest rule priority.

The home operator may provide ISRP rules to UE via the H-ANDSF or may pre-configure the UE with ISRP rules. The ISRP rules provided to UE via the H-ANDSF shall take precedence over the pre-configured ISRP rules in the UE.

4.8.2.1.5 Inter-APN Routing Policy

The Inter-APN Routing Policy (IARP) is a set of operator-defined rules that determine which traffic should be routed across different PDN connections and which traffic should be non-seamlessly offloaded to WLAN (as defined in clause 4.1.5). These rules can be provisioned by the H-ANDSF only. If the UE receives IARP rules from the V-ANDSF, the UE shall ignore them. An Inter-APN routing capable UE selects an existing IP interface to route IP flows based on the received / provisioned IARP rules and user preferences. This IP interface is either associated with a specific APN or is used for non-seamless WLAN offload (NSWO).

NOTE 1: IP interfaces not associated with an APN and not used for NSWO are considered outside the scope of IARP. Such interfaces could include e.g. an IP interface to a tethering device connected to UE over USB, or an IP interface corresponding to an enterprise VPN connection over WLAN, etc. The scenario where multiple IP interfaces are associated with the same APN is also considered outside the scope of IARP.

Each IARP rule includes the following information:

- Rules for APN: Each one of these rules identifies a prioritised list of APNs which should be used by the UE to route traffic that matches specified IP traffic filters. A rule for APN can also identify which APNs are restricted for traffic that matches specified IP traffic filters.

  - Each rule for APN contains one or more IP traffic filters (to match specific IP traffic), a prioritized list of APNs, a rule priority and, optionally, validity conditions that indicate when the rule is valid. Each IP traffic filter may identify traffic based on destination address, transport protocol, destination/source port numbers, DSCP or Traffic Class, destination domain name and application identity. The rule priority indicates the priority of the rule for APN with respect to other rules inside the same IARP rule.

- Rules for NSWO: Each one of these rules identifies which traffic shall or shall not be non-seamlessly offloaded to a WLAN when available. It shall be possible to restrict certain traffic from using non-seamless WLAN offload only in specific WLAN access networks or in all WLAN access networks. Similarly, it shall be possible to permit certain traffic to use non-seamless WLAN offload only in specific WLAN access networks or in all WLAN access networks.

  - Each rule for NSWO contains one or more IP traffic filters (to match specific IP traffic), a rule priority and, optionally, validity conditions that indicate when the rule is valid. Each IP traffic filter may identify traffic based on destination address, transport protocol, destination/source port numbers, DSCP or Traffic Class, destination domain name and application identity. The rule priority indicates the priority of the rule for NSWO with respect to other rules inside the same IARP rule.

An IARP for APN rule can be applied only when it steers IP traffic to an existing (i.e. already established) PDN connection. When no APN in the IARP for APN rule is associated with an existing PDN connection, then the rule shall not be applied.

When the UE has simultaneously an active IARP rule and an active ISRP rule, the UE evaluates first the rules for APN and for NSWO inside the active IARP rule (in priority order) to determine how to route an IP flow.

- If the IP flow matches a rule for NSWO inside the active IARP rule, then the IP flow is routed to an IP interface used for NSWO and the rules inside the active ISRP rule are not evaluated.

- If the IP flow matches a rule for APN inside the active IARP rule that prefers a certain APN, then the IP flow is routed to the IP interface corresponding to this APN. If IFOM procedures are applied on this IP interface, then the rules for IFOM inside the active ISRP rule are also evaluated and used to further route the flow. The rules for NSWO inside the active ISRP rule are not evaluated (thus the IP flow is not offloaded to WLAN if it also matches a rule for NSWO inside the active ISRP rule).

- If the IP flow matches a rule for APN inside the active IARP rule that forbids one or more APNs, then the UE evaluates the rules inside the active ISRP rule (in priority order) to determine how to route the IP flow. If the IP flow matches a rule for NSWO inside the active ISRP rule that forbids the use of the selected WLAN (or any WLAN) for routing the IP flow, then the UE may select, in an implementation dependent way, a non-forbidden APN to route the IP flow.

- If the IP flow does not match any rule inside the active IARP rule, then the UE evaluates the rules inside the active ISRP rule (in priority order) to determine how to route the IP flow.

The above order of rule evalution applies to both non-roaming and roaming scenarios and independently of whether the active IARP rule and the active ISRP rule are provided by the same or by different PLMNs.

The home operator may provide IARP rules to UE via the H-ANDSF or may pre-configure the UE with IARP rules. The IARP rules provided to UE via the H-ANDSF shall take precedence over the pre-configured IARP rules in the UE.

4.8.2.1.6 WLAN Selection Policy

The WLAN Selection Policy (WLANSP) is a set of operator-defined rules that determine how the UE selects and reselects a WLAN access network. The UE may be provisioned with WLANSP rules from multiple PLMNs.

Each WLANSP rule includes the following information:

- Validity conditions, i.e. conditions indicating when the provided rule is valid. The validity conditions can include the time of day, geolocation, network location (e.g. PLMN, Location Area), etc.

- One or more groups of WLAN selection criteria in priority order. Each group contains one or more criteria that should be fulfilled by a WLAN access network in order to be eligible for selection. Such criteria are based on the following and only the following WLAN attributes:

  a) Attributes defined in the HS2.0 Rel-2 specification [75]:

     - PreferredRoamingPartnerList,

     - MinimumBackhaulThreshold,

     - MaximumBSSLoad,

     - RequiredProtoPortTuple.

     - A list of SSIDs as defined in the SPExclusionList.

  b) Additional attributes:

     - PreferredSSIDList: A prioritized list of SSIDs preferred for selection.

     - HomeNetwork: When the HomeNetwork is set in a group of selection criteria, it indicates that the group of selection criteria applies only to WLAN access networks that directly interwork with the home operator. When the HomeNetwork is not set or is not present in a group of seletion criteria, it indicates that the group of selection criteria applies to all WLAN access networks. The UE determines which WLAN access networks directly interwork with the home operator by discovering which WLAN access networks advertise the HPLMN identity or the home network realm or a service provider realm equivalent to the HPLMN. The home network realm is derived by the UE from IMSI as specified in TS 23.003 [16] (e.g. wlan.mnc015.mcc234.3gppnetwork.org).

NOTE: If the HomeNetwork is set in a group of selection criteria then this group of selection criteria is not expected to include the PreferredRoamingPartnerList and the PreferredSSIDList.

For example, a WLANSP rule may include the following groups of selection criteria:

- Group of selection criteria with priority 1:

  - PreferredRoamingPartnerList = Priority 1: partner1.com, Priority 2: partner2.com

  - MaximumBSSLoad = 60

- Group of selection criteria with priority 2:

  - PreferredSSIDList = Priority 1: myoperator1, Priority 2: myoperator2

  - MinimumBackhaulThreshold = 2Mbps in the downlink

A WLAN access network meets a group of selection criteria when it concurrently fulfills all the criteria in the group.

The home operator may provide WLANSP rules to UE via the H-ANDSF or may pre-configure the UE with WLANSP rules. The WLANSP rules provided to UE via the H-ANDSF shall take precedence over the pre-configured WLANSP rules in the UE.

4.8.2.1.7 VPLMNs with preferred WLAN Selection Rules

The "VPLMNs with preferred WLAN Selection" Rules is a list of PLMNs that is used by the UE when roaming. When the UE is roaming to one of the PLMNs in the list, the UE is configured to prefer the WLANSP rules provided by this PLMN over the WLANSP rules provided by the HPLMN. When the UE is roaming to any other PLMN, the UE is configured to prefer the WLANSP rules provided by the HPLMN.

How the UE uses this list of PLMNs for WLAN selection is specified in more detail in clause 4.8.2a.1.

The home operator may provide "VPLMNs with preferred WLAN Selection" rules to UE via the H-ANDSF or may pre-configure the UE with "VPLMNs with preferred WLAN Selection" rules. The "VPLMNs with preferred WLAN Selection" rules provided to UE via the H-ANDSF shall take precedence over the pre-configured "VPLMNs with preferred WLAN Selection" rules in the UE.

4.8.2.1.8 Void

4.8.2.1.9 Home Network Preferences

The Home Network Preferences may be provided by the UE's home operator and include information that assists the UE to select a WLAN access network and to select a PLMN for 3GPP-based authentication over WLAN. The Home Network Preferences may be provided by the HPLMN or an equivalent HPLMN or may be statically provisioned in the UE. The UE shall ignore the Home Network Preferences if provided by any other PLMN.

The Home Network Preferences may contain the following information:

- Equivalent Home Service Providers (EHSP): Contains a list of service providers which are equivalent to the UE's HPLMN. Each service provider in EHSP is identified with a domain name, which may contain a PLMN identity (e.g. wlan.mncXYZ.mccABC.3gppnetwork.org) or may not contain a PLMN identity (e.g. example.com). The EHSP is used by the UE for PLMN selection over WLAN as specified in clause 4.8.2b.

- Preferred Service Provider List (PSPL): Contains a prioritized list of service providers which are preferred for WLAN roaming. Each service provider in PSPL is identified with a domain name, which may contain a PLMN identity (e.g. wlan.mncXYZ.mccABC.3gppnetwork.org) or may not contain a PLMN identity (e.g. example.com). The UE uses the PSPL for WLAN selection and PLMN selection as specified in clause 4.8.2b.

- "S2a connectivity preference": The "S2a connectivity preference" indicates if the home operator prefers the UE to establish PDN connections over WLAN by using the applicable S2a procedures specified in clause 16. It is used by the UE during the WLAN selection procedure as specified in clause 4.8.2b.

- "Prefer 3GPP RPLMN" indication: This indication specifies how a roaming UE selects a PLMN in order to perform 3GPP-based authentication over WLAN access. If the "prefer 3GPP RPLMN" indication is not set, the UE attempts to select the HPLMN, or a service provider included in EHSP, or a service provider included in PSPL for authentication over WLAN access. If the "prefer 3GPP RPLMN" indication is set, the UE attempts to select the Registered PLMN (RPLMN) or a service provider included in EVSP of the RPLMN (see clause 4.8.2.1.10) for authentication over WLAN access. Further details about the use of "prefer 3GPP RPLMN" indication are provided in clause 4.8.2b.

The home operator may provide Home Network Preferences to UE via the H-ANDSF or may pre-configure the UE with Home Network Preferences. The Home Network Preferences provided to UE via the H-ANDSF shall take precedence over the pre-configured Home Network Preferences in the UE.

4.8.2.1.10 Visited Network Preferences

The Visited Network Preferences may be provided by a PLMN-x, which is different from the UE's HPLMN and all equivalent HPLMNs. They include information that assists the UE (when roaming to PLMN-x) to select a PLMN for authentication over WLAN. The UE shall ignore the Visited Network Preferences if provided by HPLMN or any equivalent HPLMN.

The Visited Network Preferences may contain the following information:

- Equivalent Visited Service Providers (EVSP): Contains a list of service providers which are considered equivalent to the PLMN which provided the EVSP. Each service provider in EVSP is identified with a domain name, which may contain a PLMN identity (e.g. wlan.mncXYZ.mccABC.3gppnetwork.org) or may not contain a PLMN identity (e.g. example.com). The EVSP is used by the UE for PLMN selection over WLAN as specified in clause 4.8.2b.

NOTE: The list of Equivalent Visited Service Providers (EVSP) provided to UE by ANDSF is independent from the list of equivalent PLMNs (see TS 23.401 [4]) provided to UE via 3GPP access.

4.8.2a UE Procedures

4.8.2a.1 Selection of Active ANDSF Rules

The UE may be provisioned with multiple valid ISMP, ISRP, IARP and WLANSP rules (by the HPLMN and by the VPLMN when it is roaming). The UE does not apply all these valid rules but selects and applies only the "active" rules. Specifically:

- A UE that cannot simultaneously route IP traffic over 3GPP access and over WLAN access shall select an active ISMP rule, an active IARP rule and an active WLANSP rule, as specified below.

- A UE that can simultaneously route IP traffic over 3GPP access and over WLAN access shall select an active ISRP rule, an active IARP rule and an active WLANSP rule, as specified below.

When the UE is not roaming, it shall select the active ISMP/ISRP rule, the active IARP rule and the active WLANSP rule to apply from the valid rules provided by the HPLMN based on the individual priorities of these rules (or based on other criteria specified in TS 24.312 [73]). For example, the highest priority valid WLANSP rule is selected as the active WLANSP rule.

When the UE is roaming, it may have valid rules from both HPLMN and VPLMN. In this case, the UE shall select the active rules as follows:

1) The active IARP rule is selected from the valid IARP rules provided by the HPLMN.

2) The active ISMP/ISRP rule and the active WLANSP rule are selected based on the UE configuration as follows:

   a) The UE is configured to "prefer WLAN selection rules provided by the HPLMN" or not. This configuration can be done either by the user or by the H-ANDSF via the list of "VPLMNs with preferred WLAN Selection Rules" (see clause 4.8.2.1.7). User configuration takes precedence over the H-ANDSF configuration.

   b) If the UE is configured not to prefer WLAN selection rules provided by the HPLMN (i.e. the VPLMN to which the UE is registered is included in the list of "VPLMNs with preferred WLAN Selection Rules"), then the UE shall check the WLANSP rule of the VPLMN and shall determine if there are available WLAN access networks that match one or more groups of selection criteria in this rule.

      i) If there is at least one WLAN access network that matches one or more groups of selection criteria in the WLANSP rule of the VPLMN, then the UE shall select the active WLANSP rule and the active ISMP/ISRP rule from the valid rules provided by the VPLMN (based on their priority values).

      ii) If there is no WLAN access network that matches one or more groups of selection criteria in the WLANSP rule of the VPLMN, then the UE shall select the active WLANSP rule and the active ISMP/ISRP rule from the valid rules provided by the HPLMN. When the UE determines that at least one WLAN access network that matches one or more groups of selection criteria in the WLANSP rule of the VPLMN becomes available, it shall operate as in bullet i) above and may re-select to such WLAN access network.

   c) If the UE is configured to prefer WLAN selection rules provided by the HPLMN (i.e. the VPLMN to which the UE is registered is not included in the list of "VPLMNs with preferred WLAN Selection Rules"), then the UE shall check the WLANSP rule of the HPLMN and shall determine if there are available WLAN access networks that match one or more groups of selection criteria in this rule.

      i) If there is at least one WLAN access network that matches one or more groups of selection criteria in the WLANSP rule of the HPLMN, then the UE shall select the active WLANSP rule and the active ISMP/ISRP rule from the valid rules provided by the HPLMN (based on their priority values).

      ii) If there is no WLAN access network that matches one or more groups of selection criteria in the WLANSP rule of the HPLMN, then the UE shall select the active WLANSP rule and the active ISMP/ISRP rule from the valid rules provided by the VPLMN. When the UE determines that at least one WLAN access network that matches one or more groups of selection criteria in the WLANSP rule of the HPLMN becomes available, it shall operate as in bullet i) above and may re-select to such WLAN access network.

During power-up, while the UE has not registered to any PLMN, the UE shall consider the WLANSP rules provided by the HPLMN as valid and shall select an active WLANSP rule as described above (the one with the highest priority). Thus during power-up the UE can select a WLAN network based on the WLANSP rules provided by HPLMN.

4.8.2a.2 UE Behavior Based on the ANDSF Information

This clause specifies the UE behavior when it is provisioned with ANDSF information and has selected the active rules as described in the previous clause.

If the UE has received or has been provisioned with ANDSF information which indicates that there is an access network in its vicinity with higher priority than the currently selected access network(s), the UE should perform procedures for discovering and reselecting the higher priority access network, if this is allowed by user preferences.

NOTE 1: How frequently the UE performs the discovery and reselection procedure depends on the UE implementation.

(i) When the UE cannot simultaneously route IP traffic over multiple radio accesses:

- The UE shall select the most preferable available access network for EPC connectivity and inter-system mobility based on the active ISMP rule, the active WLANSP rule and the user preferences. The user preferences take precedence over the active rules.
- The UE shall not consider any ISRP rules it may have received from the ANDSF.
- When automatic access network selection is used, the UE shall not initiate a connection to EPC using an access network indicated as restricted in the active ISMP rule.
- When the UE selects a non-3GPP radio access based on the active ISMP and the active WLANSP rules, the UE may still use 3GPP access for CS services.

NOTE 2: The user may manually select the access technology type or access network that should be used by the UE; in such case the active ISMP and the active WLANSP rules are not taken into account.

- When the UE is connected to EPC over 3GPP access, the UE shall use the active IARP rule and the user preferences to determine if an IP flow should be routed inside a specific PDN connection.
- When the UE is connected to EPC over WLAN access, the UE shall use the active IARP rule and the user preferences to determine if an IP flow should be routed inside a specific PDN connection or if it should be non-seamlessly offloaded to the selected WLAN access network.
- The UE shall use the active ISMP rule to determine if EPC connectivity is preferred over WLAN access or over 3GPP access. The prioritized list of access networks in the active ISMP rule shall not be used for WLAN selection since WLAN selection is based on the active WLANSP rule and the user preferences.
- When EPC connectivity is preferred over WLAN access (i.e. the highest priority access in the active ISMP rule corresponds to WLAN access technology / network), the UE shall use the active WLANSP rule to determine the most preferred available WLAN access network (as specified in clause 4.8.2b).
- When the UE is connected to EPC over WLAN access, the UE should occasionally re-evaluate if the connected WLAN still meets the selection criteria in the active WLANSP rule. The rate of this re-evaluation is defined by the UE implementation. When the UE determines that the currently selected WLAN does not meet the selection criteria in the active WLASP rule for an implementation-specific duration, the UE should attempt to select another WLAN access network as specified in clause 4.8.2b.
- When the most preferred available WLAN access network has higher priority than 3GPP access (according to the prioritized accesses in the active ISMP rule), then the UE shall connect to EPC over the most preferred available WLAN access network. Otherwise, the UE shall connect to EPC over 3GPP access. For example:
  - If the prioritized access networks in the active ISMP rule are the following: WLAN-A priority 1, 3GPP priority 2, WLAN-B priority 3; then
  - Since the UE determines that one or more WLANs are preferred for EPC connectivity over 3GPP access, the UE uses the groups of selection criteria in the active WLANSP rule to determine the most preferred available WLAN access network (as specified in clause 4.8.2b).

- If the most preferred available WLAN access network has lower priority than 3GPP access according to the active ISMP rule (e.g. WLAN-B), then the UE shall connect to EPC over 3GPP access.

- If the most preferred available WLAN access network has higher priority than 3GPP access according to the active ISMP rule (e.g. WLAN-A), then the UE shall connect to EPC over the most preferred available WLAN access network.

NOTE 3: It is assumed that the active ISMP rule in the UE can always be used to determine the relative priority of the most preferred WLAN (selected based on the active WLANSP rule) over 3GPP access.

(ii) When the UE can simultaneously route IP traffic over multiple radio accesses:

- The UE shall not consider any ISMP rules it may have received from the ANDSF.

- The UE shall use the active WLANSP rule and the user preferences to select and connect to the most preferred available WLAN access network, as specified in clause 4.8.2b. User preferences take precedence over the active WLANSP rule. After that, the UE is simultaneously connected to 3GPP access and to the selected (most preferred) WLAN access network.

- After the UE selects and connects to a WLAN access network based on the active WLANSP rule (as specified in clause 4.8.2b), the UE should occasionally re-evaluate if the connected WLAN still meets the selection criteria in the active WLANSP rule. The rate of this re-evaluation is defined by the UE implementation. When the UE determines that the currently connected WLAN does not meet the selection criteria in the active WLASP rule for an implementation-specific duration, the UE should attempt to select another WLAN access network as specified in clause 4.8.2b.

- The prioritized lists of access networks in the active ISRP rule shall not be used for WLAN selection since WLAN selection is based on the active WLANSP rule and the user preferences.

- The UE shall use the active ISRP for MAPCON rules and the user preferences to determine if a PDN connection to a certain APN should be established over 3GPP access or over the selected WLAN access network.

  - When an ISRP for MAPCON rule is used for the PDN connection establishment, the UE shall determine if the selected WLAN access network has higher priority than 3GPP access and establishes the PDN connection accordingly. For example:

    - If the list of prioritized access networks in the ISRP for MAPCON rule are the following: WLAN-A priority 1, 3GPP priority 2, WLAN-B priority 3; then

    - If the UE has selected WLAN-B (or any WLAN network with lower priority than 3GPP access), it shall establish the PDN connection over 3GPP access.

    - If the UE has selected WLAN-A (or any WLAN network with higher priority than 3GPP access), it shall establish the PDN connection over WLAN access.

- The UE shall use the active ISRP for IFOM rules, the active ISRP for NSWO rules, the active IARP rule and the user preferences to determine how to route outgoing IP flows. Specifically:

  - The UE shall evaluate the above rules in priority order as specified in clause 4.8.2.1.5 (Inter-APN Routing Policy) and shall determine which rule to apply.

  - When the applied rule is an ISRP for IFOM rule, the UE determines that this flow is subject to IP flow mobility and selects an access network to route this flow based on the prioritized list of access networks in the ISRP for IFOM rule. For example:

    - If the prioritized list of access networks in the ISRP for IFOM rule are the following: WLAN-A priority 1, 3GPP priority 2, WLAN-B priority 3; then

    - If the UE has selected WLAN-B (or any WLAN network with lower priority than 3GPP access), it shall route the IP flow over 3GPP access.

    - If the UE has selected WLAN-A (or any WLAN network with higher priority than 3GPP access), it shall route the IP flow over WLAN access.

- When the applied rule is an ISRP for NSWO or an IARP for NSWO rule, the UE shall route this IP flow to the selected WLAN access network (outside any PDN connection) provided that the rule does not prohibit this IP flow over the selected WLAN access network.

- When the applied rule is an IARP for APN rule, the UE shall route this IP flow inside the PDN connection specified by this rule.

NOTE 4: It is assumed that the active ISRP rule in the UE can always be used to determine the relative priority of the selected WLAN access network over 3GPP access.

4.8.2b WLAN Selection based on WLANSP

When the UE has valid 3GPP subscription credentials (i.e. a valid USIM) and WLANSP policies, the UE shall perform WLAN selection based on these policies, the applicable user preferences and the corresponding procedures specified in this document. User preferences take precedence over the WLANSP policies.

The following text specifies how the UE determines the most preferred WLAN access network (and possibly connects to this network, as clarified in clause 4.8.2a.2), when a WLAN access network cannot be selected based on user preferences (e.g. when there are no user preferences or when there is no user-preferred WLAN access network available).

If the UE supports S2a connectivity (see clause 16), then:

- The UE shall be able to discovery WLANs that support S2a connectivity. This discovery shall be performed by using ANQP procedures (as specified in the HS2.0 Rel-2 specification [75]) to retrieve the 3GPP Cellular Network information advertised by WLANs. The 3GPP Cellular Network information (see IEEE 802.11-2012 [64]) advertised by a WLAN indicates the PLMNs that interwork with the WLAN. In addition, the 3GPP Cellular Network information indicates the PLMNs to which the WLAN supports S2a connectivity.

- The UE may decide to select a WLAN that supports S2a connectivity to HPLMN, RPLMN or both HPLMN and RPLMN. This decision is based on UE implementation specific mechanisms and the "S2a connectivity preference" provisioned in the UE by the home ANDSF. The "S2a connectivity preference" is either set or not set. The UE performs service provider selection after selecting a WLAN that has S2a connectivity with the UE's HPLMN, RPLMN or both HPLMN and RPLMN.

- When the "S2a connectivity preference" is set, it indicates that the home operator prefers the UE to establish PDN connections over WLAN by using the applicable S2a procedures specified in clause 16. In this case, when the UE attempts to select a WLAN and determines that a PDN connection will be required over this WLAN, the UE shall attempt to select a WLAN that supports S2a connectivity unless other procedures are applicable for this PDN connection (e.g. S2b or S2c procedures).

The UE shall use the active WLANSP rule, the Home Network Preferences and, if roaming, the Visited Network Preferences to determine the most preferred available WLAN access network. The WLAN selection shall be performed with the following steps.

i. Step 1: The UE constructs a prioritized list of the available WLANs by discovering the available WLANs and comparing their attributes / capabilities against the groups of selection criteria in the active WLANSP rule. When a group of selection criteria includes the HomeNetwork attribute and is set, then the UE (a) shall create a list of available WLANs that directly interwork with the home operator (as specified in clause 4.8.2.1.6) and (b) shall apply the group of selection criteria to all the WLANs in this list. Otherwise, when the HomeNetwork attribute is not set or is not present, the UE shall apply the group of selection criteria to all available WLANs. The UE may need to perform ANQP procedures (as specified in the HS2.0 Rel-2 specification [75]) or other procedures in order to discover the attributes / capabilities of the available WLANs. The WLAN(s) that match the group of selection criteria with the highest priority are considered as the most preferred WLANs, the WLAN(s) that match the group of selection criteria with the second highest priority are considered as the second most preferred WLANs, etc. For example, the UE may construct the following prioritized list:

   - WLAN-1 (most preferred)

   - WLAN-4, WLAN-2 (second most preferred)

   - WLAN-3 (third most preferred, supports S2a connectivity to PLMN-a and PLMN-b)

ii. Step 2: If the UE decides to select a WLAN that supports S2a connectivity to one or more PLMNs (as specified above), then from the prioritized list contructed in the previous step the UE shall select the highest priority WLAN that support S2a connectivity to these PLMNs (e.g. WLAN-3 in the example shown above). If the UE does not discover a WLAN that supports S2a connectivity, or the UE does not decide to select a WLAN that supports S2a connectivity, then from the prioritized list contructed in the previous step the UE shall select the most preferred WLAN without considering its capability to support S2a connectivity (e.g. WLAN-1 in the example shown above).

- If the UE cannot select a single WLAN in this step, i.e. when there are multiple WLANs that could be selected but all have the same priority, then the UE shall select one of these multiple WLANs as follows:

  a) If the UE is not roaming, or if the UE is roaming and the "prefer 3GPP RPLMN" indication is not set, then the UE shall select a WLAN in this order: (a) a WLAN that directly interworks with the HPLMN, (b) a WLAN that directly interworks with a service provider in EHSP, (c) a WLAN that directly interworks with the most preferred service provider in PSPL.

  b) If the UE is roaming and the "prefer 3GPP RPLMN" indication is set, then the UE shall select a WLAN in this order: (a) a WLAN that directly interworks with the RPLMN, (b) a WLAN that directly interworks with a service provider in EVSP. Otherwise the UE shall behave as specified in bullet a) above.

iii. Step 3: After selecting a single WLAN access network (as specified in steps 1 and 2), if the UE needs to perform 3GPP-based access authentication, the UE shall construct the NAI as follows:

  a) If the UE is not roaming, or if the UE is roaming and the "prefer 3GPP RPLMN" indication is not set, then:

  - If the UE has selected a WLAN that directly interworks with the HPLMN, then the UE shall use the root NAI.

  - If the UE has selected a WLAN that directly interworks with a service provider in EHSP list (see clause 4.8.2.1.9), then the UE shall construct a decorated NAI that includes the realm of this service provider.

  - Otherwise, the UE shall determine the most preferred service provider that interworks with the selected WLAN based on PSPL and shall construct a decorated NAI that includes the realm of this service provider.

  b) If the UE is roaming and the "prefer 3GPP RPLMN" indication is set, then:

  - If the UE has selected a WLAN that directly interworks with the RPLMN, then the UE shall construct a decorated NAI that includes the realm of RPLMN.

  - If the UE has selected a WLAN that directly interworks with a service provider in EVSP list provided by the RPLMN (see clause 4.8.2.1.10), then the UE shall construct a decorated NAI that includes the realm of this service provider and the realm of RPLMN.

  - Otherwise, the UE shall behave as specified in bullet a) above.

NOTE 1: The UE performs the WLAN selection based on the active WLANSP rule without taking into account real-time events associated with the active ISRP rule. As specified in clause 4.8.2a.2, the active ISRP rule is used only for routing decisions and does not impact the selection or reselection of the WLAN access network. For example, when a new IP flow in the UE matches an active ISRP rule in which the highest priority access network is a WLAN other than the selected WLAN, this event should not trigger WLAN re-selection. If the conditions for WLAN selection change every time a new application runs or when certain IP flows are detected, the WLAN selection in the UE will be complex and may lead to frequent WLAN re-selections that would negatively affect the user experience and the battery consumption.

NOTE 2: Events such as change of WLAN load information, change of UE location, change of time of day may lead to WLAN (re-)selection based on the WLANSP rule.

4.8.3 Reference Points

S14 This reference point is between UE and H-ANDSF / V-ANDSF for direct queries via pull. It enables dynamic provision of information to the UE for access NW discovery and selection procedures related to non-3GPP and 3GPP accesses. This dynamic provision shall be supported with Pull (UE-initiated session) and with Push (ANDSF-initiated session), if feasible. Communication over S14 is secured as specified in TS 33.402 [45].

Protocol assumption:

- S14 interface is realized above IP level.

4.8.4 ANDSF Discovery

In non-roaming scenario, the H-ANDSF is discovered through interaction with the Domain Name Service function or the DHCP Server function. The H-ANDSF address may also be provisioned to the UE.

In roaming scenario, the UE shall be possible to retrieve both the H-ANDSF and V-ANDSF addresses.

NOTE: The ANDSF may not be contactable in certain PDNs.

4.8.5 Void

4.8.6 Support of RAN Assistance Information

4.8.6.1 General

As specified in TS 36.331 [52] and TS 25.331 [78], an E-UTRAN or UTRAN (referred to as RAN) may provide RAN Assistance Information to UE. This RAN Assistance Information includes the following thresholds and parameters:

- 3GPP access thresholds;
- WLAN access thresholds; and
- An Offload Preference Indication (OPI) value.

The 3GPP access thresholds define low/high threshold values for some UTRA and/or E-UTRA radio parameters, such as low/high RSRP thresholds for E-UTRA, low/high CPICH Ec/No thresholds for UTRA, etc. The WLAN access thresholds define low/high threshold values for some WLAN access parameters, such as the low/high Beacon RSSI thresholds, the high/low UL/DL backhaul data rate thresholds and the low/high channel utilization thresholds. UL/DL backhaul data rate is defined in Hotspot 2.0 [75]. Channel utilization and Beacon RSSI are defined in IEEE 802.11-2012 [64]. How these thresholds are used in the ANDSF rules is specified in clause 4.8.6.2.

The OPI value provided by RAN is a bitmap (i.e. a one-dimensional bit array) that may be used by UEs in an E-UTRA or UTRA cell to determine when they should move certain traffic (e.g. certain IP flows) to WLAN access or to 3GPP access. The meaning of each bit in this bitmap is operator specific and is not defined in 3GPP specifications. How the OPI value is used in the ANDSF rules is specified in clause 4.8.6.2.

The thresholds and parameters provided to UE in a UTRA or E-UTRA cell may affect the validity of the ANDSF rules (as specified in clause 4.8.6.2) and thus make these rules subject to conditions set by the RAN in a given cell.

The user preferences on WLAN network selection and traffic routing shall take precedence over ANDSF rules and RAN rules.

4.8.6.2 ANDSF Rules Utilizing RAN Assistance Information

The 3GPP access thresholds, the OPI value and some of the WLAN access thresholds included in the RAN Assistance Information may be utilized by the following ANDSF rules:

- The Inter-System Routing Policy (ISRP) rules specified in clause 4.8.2.1.4, i.e. ISRP rules for IFOM, ISRP rules for MAPCON and ISRP rules for NSWO; and

- The Inter-APN Routing Policy (IARP) rules specified in clause 4.8.2.1.5, i.e. IARP rules for APN and IARP rules for NSWO.

In this release of the specification the ANDSF rules may use the low/high Beacon RSSI thresholds, the low/high WLAN channel utilization thresholds and the low/high UL/DL WLAN backhaul data rate thresholds included in the RAN Assistance Information. These thresholds subsequently referred to as "RAN provisioned WLAN access thresholds".

The ANDSF rules may also utilize low/high Beacon RSSI thresholds, low/high WLAN channel utilization thresholds and low/high UL/DL WLAN backhaul data rate thresholds provided by the ANDSF. These thresholds are subsequently referred to as "ANDSF provisioned WLAN access thresholds".

NOTE: The use of 3GPP access thresholds in the IARP for APN rules can enable routing policies such as "move certain traffic from a non-seamless WLAN connection to a given PDN connection over LTE access when the LTE radio strength and quality exceed the applicable thresholds provided by RAN".

An IARP/ISRP rule may utilize the 3GPP access thresholds, the RAN provisioned WLAN access thresholds and the OPI value included in the RAN Assistance Information and ANDSF provisioned WLAN access thresholds. When the rule utilizes any of these access thresholds and/or the OPI value, it shall be constructed as follows:

1. The IARP/ISRP rule shall contain RAN validity conditions, which indicate when the rule is valid or invalid based on the RAN Assistance Information.

2. The RAN validity conditions may contain one or more threshold conditions and one OPI condition.

3. Each threshold condition shall be associated either (i) with a 3GPP access threshold provided by RAN or (ii) with WLAN access threshold(s) provided by ANDSF, RAN, or both. A threshold condition shall be evaluated to true or false as specified in clause 4.8.6.3.

4. The OPI condition shall contain a provisioned OPI which is a bitmap assigned by ANDSF and is associated with the rule. The meaning of each bit in this bitmap is operator specific and is not defined in 3GPP specifications. The OPI condition shall be evaluated to true or false based on the provisioned OPI and the OPI value provided by RAN, as specified in clause 4.8.6.3.

5. The RAN validity conditions include an indicator which indicates if the rule may be valid either (a) when all threshold conditions are true or (b) when at least one threshold condition is true.

4.8.6.3 Evaluation of ANDSF Rules with RAN Validity Conditions

When the UE cannot simultaneously route IP traffic to both 3GPP access and WLAN, then

- When the UE has an IARP rule that contains RAN validity conditions, the UE shall evaluate the rule by ignoring all the RAN validity conditions that may be present, i.e. the UE shall consider these RAN validity conditions as true.

When the UE can simultaneously route IP traffic to both 3GPP access and WLAN access, then:

- When the UE has an IARP or ISRP rule that contains RAN validity conditions, the UE shall evaluate all included threshold conditions and the OPI condition, as specified below. The UE shall consider the RAN validity conditions as valid when the OPI condition is true and when either (a) all threshold conditions are true or (b) at least one threshold condition is true, according to the indicator described in bullet 5 of clause 4.8.6.2.

- When a threshold condition is associated with a 3GPP access threshold, the UE shall evaluate the threshold condition by comparing the associated 3GPP access threshold provided by RAN with the corresponding measured value. For example, when a threshold condition is associated with the low RSRP threshold, the UE shall evaluate the condition to true when the measured RSRP value is smaller to the low RSRP threshold. If the associated 3GPP access threshold is not available in the UE (e.g. it is not provided by RAN), then the UE shall consider the threshold condition as false.

- When a threshold condition is associated with only a RAN provisioned WLAN access threshold, the UE shall evaluate the threshold condition by comparing the associated RAN provisioned WLAN access threshold with the corresponding value received from the selected WLAN. For example, when a threshold condition is associated

with the low channel utilization threshold, the UE shall evaluate the condition to true when the channel utilization of the selected WLAN is smaller to the low channel utilization threshold. If the associated RAN provisioned WLAN access threshold is not available in the UE (e.g. it is not provided by RAN), then the UE shall consider the threshold condition as false.

- When a threshold condition is associated with only an ANDSF provisioned WLAN access threshold, the UE shall evaluate the threshold condition by comparing the ANDSF provisioned WLAN access threshold with the corresponding value received from the selected WLAN. For example, when a threshold condition is associated with a high DL/UL backhaul data rate threshold, the UE shall evaluate the condition to true when DL/UL backhaul data rate of the selected WLAN is higher than the high DL/UL backhaul data rate threshold.

- When a threshold condition is associated with both a RAN provisioned WLAN access threshold and an ANDSF provisioned WLAN access threshold, then it indicates that the threshold condition shall be evaluated by using only the RAN provisioned WLAN access threshold, if available (i.e. if included in the RAN Assistance Information). If the RAN provisioned WLAN access threshold is not available, the ANDSF provisioned WLAN access threshold shall be used.

- How often the UE re-evaluates the threshold and the OPI conditions to determine when each condition is true or false depends on the UE implementation.

- The UE shall evaluate an OPI condition by performing a bitwise 'AND' operation between the OPI value provided by RAN and the provisioned OPI contained in the rule. If the result of this operation in non-zero, the UE shall consider the OPI condition as true. If the OPI value is not available in the UE (e.g. it is not provided by RAN), then the UE shall consider the OPI condition as false.

- When the UE is roaming and applies IARP rules from HPLMN and/or ISRP rules from HPLMN, the UE shall ignore the RAN validity conditions that may be present in these rules, i.e. the UE shall consider these RAN validity conditions as true.

4.8.6.4 Co-existence with RAN Rules

Within a single PLMN, the WLAN access selection and the traffic routing behaviour of a UE shall be controlled either by the ANDSF rules specified in this specification or by the RAN rules specified in TS 36.304 [79] and TS 25.304 [80], not by any combination of them. The only exception is that when a UE applies the RAN rules, it shall be possible to simultaneously apply the IARP for APN rules provided by HPLMN, as further explained below.

When the UE has both ANDSF rules and RAN rules it shall select which rules to apply according to the following procedures.

When the UE can simultaneously route IP traffic to both 3GPP access and WLAN access:

- When the UE is not roaming or when the UE is roaming in a VPLMN not contained in the list of "VPLMNs with preferred WLAN Selection Rules" (see clause 4.8.2.1.7), then:

  - If the UE has a valid ISRP rule from HPLMN, the UE shall ignore the RAN rules and shall perform WLAN access selection and traffic routing based on the ANDSF procedures specified in clause 4.8.2a.

  - If the UE has no valid ISRP rule from HPLMN, the UE shall perform WLAN access selection and traffic routing based on the RAN rules. In this case, if the UE has a valid IARP rule from HPLMN, it shall apply the internal IARP for APN rules and shall ignore their RAN validity conditions if present.

- When the UE is roaming in a VPLMN contained in the list of "VPLMNs with preferred WLAN Selection Rules" (see clause 4.8.2.1.7) then:

  - If the UE has a valid ISRP rule from VPLMN, the UE shall ignore the RAN rules and shall perform WLAN access selection and traffic routing based on the ANDSF procedures specified in clause 4.8.2a.

  - If the UE has no valid ISRP rule from VPLMN, the UE shall perform WLAN access selection and traffic routing based on the RAN rules. In this case, if the UE has a valid IARP rule from HPLMN, it shall apply the internal IARP for APN rules and shall ignore their RAN validity conditions if present.

When the UE cannot simultaneously route IP traffic to both 3GPP access and WLAN access:

- When the UE is not roaming or when the UE is roaming in a VPLMN not contained in the list of "VPLMNs with preferred WLAN Selection Rules" (see clause 4.8.2.1.7), then:

- If the UE has at least one ISMP rule from HPLMN, the UE shall ignore the RAN rules and shall perform WLAN access selection and access selection for EPC connectivity based on the ANDSF procedures specified in clause 4.8.2a.

- If the UE has no ISMP rules from HPLMN, the UE shall apply the RAN rules or RCLWI command to determine when all PDN connections should be handed over to WLAN access or to 3GPP access. When the RAN rules indicate that all PDN connections should be handed over to WLAN access but at least one PDN connection is not allowed to be handed over to WLAN access (as specified in TS 23.401 [4]), the UE shall not handover any PDN connection. When all PDN connections are allowed to be handed over to WLAN access, the UE shall perform WLAN access selection based on the RAN rules and shall execute the applicable handover procedures specified in clause 8. In this case, if the UE has a valid IARP rule from HPLMN, it shall apply the internal IARP for APN rules and shall ignore their RAN validity conditions if present.

- When the UE is roaming in a VPLMN contained in the list of "VPLMNs with preferred WLAN Selection Rules" (see clause 4.8.2.1.7) then:

  - If the UE has at least one ISMP rule from VPLMN, the UE shall ignore the RAN rules and shall perform WLAN access selection and access selection for EPC connectivity based on the ANDSF procedures specified in clause 4.8.2a.

  - If the UE has no ISMP rules from VPLMN, the UE shall apply the RAN rules to determine when all PDN connections should be handed over to WLAN access or to 3GPP access. When the RAN rules indicate that all PDN connections should be handed over to WLAN access but at least one PDN connection is not allowed to be handed over to WLAN access (as specified in TS 23.401 [4]), the UE shall not handover any PDN connection. When all PDN connections are allowed to be handed over to WLAN access, the UE shall perform WLAN access selection based on the RAN rules and shall execute the applicable handover procedures specified in clause 8. In this case, if the UE has a valid IARP rule from HPLMN, it shall apply the internal IARP for APN rules and shall ignore their RAN validity conditions if present.

4.8.7 Support of LWA, LWIP and RCLWI

4.8.7.1 General

For WLAN access selection and traffic routing, in addition to the ANDSF procedures, the UE may also support:

- the LTE-WLAN Aggregation (LWA) procedures specified in TS 36.300 [6] and TS 36.463 [84];

- the LTE-WLAN Radio Level Integration with IPsec Tunnel (LWIP) procedures specified in TS 36.300 [6]; and

- the RAN controlled LTE-WLAN interworking (RCLWI) procedures specified in TS 36.300 [6].

As defined in TS 36.300 [6], the LWA, the LWIP and the RCLWI procedures are applicable only when the UE operates in ECM-CONNECTED mode (see TS 23.401 [4]). When the UE operates in ECM-IDLE mode (see TS 23.401 [4]), these procedures are not applied.

4.8.7.2 Co-existence with LWA and RCLWI

When the UE supports WLAN access selection and traffic routing based on the ANDSF procedures defined in this specification and based on the LWA/RCLWI procedures specified in TS 36.300 [6] and TS 36.463 [84], then the UE shall support co-existence between these procedures as well as co-existence between these procedures and the user preferences by applying the following behaviour:

1. When the UE has not selected a WLAN, the UE shall accept the LWA/RCLWI signalling and shall apply WLAN access selection and traffic routing based on the applicable LWA/RCLWI procedures.

2. When the UE has selected a WLAN based on user preferences, the UE shall ignore the LWA/RCLWI signalling.

3. When the UE has selected a WLAN based on ANDSF rules, the UE shall accept or shall ignore the LWA/RCLWI signalling based on the UE configuration. Specifically, the UE may be configured via the home ANDSF with an indication that specifies if the UE shall accept or ignore the LWA/RCLWI signalling in a specific PLMN and/or when connected to a specific WLAN access. Examples of such UE configuration include "always accept LWA/RCLWI signalling", "accept LWA/RCLWI signalling expect in PLMN-a", "accept

LWA/RCLWI signalling expect when connected to SSID-x" or "ignore LWA/RCLWI signalling expect in HPLMN, EHPLMN-a". If the UE is not configured via the home ANDSF with this indication, then the UE shall always accept the LWA/RCLWI signalling.

4. Based on implementation specific mechanisms, the UE shall limit the frequency of WLAN re-selection that may occur when the UE has an active ANDSF rule for WLAN selection (WLANSP rule) and it accepts the LWA/RCLWI signalling. For example, the UE may select one WLAN access in ECM-CONNECTED mode (see TS 23.401 [4]) based on LWA/RCLWI signalling and another WLAN access based on the active ANDSF rule in ECM-IDLE mode (see TS 23.401 [4]). The UE shall not trigger WLAN re-selection every time it transitions between ECM-CONNECTED and ECM-IDLE modes.

5. When the UE applies WLAN access selection and traffic routing based on the LWA/RCLWI procedures (i.e. in ECM-CONNECTED mode) the UE shall not apply WLANSP, ISRP and IARP for NWSO rules. However, if the UE has a valid IARP rule, it shall apply the internal IARP for APN rules in order to perform traffic routing across the established PDN connections.

4.8.7.3 Co-existence with LWIP

All the co-existence procedures between ANDSF and LWA defined in clause 4.8.7.2 are also applied for the co-existence between ANDSF and LWIP. If the UE is configured via the home ANDSF with an indication that specifies if the UE shall accept or ignore the LWA/RCLWI signalling in a specific PLMN and/or when connected to a specific WLAN access, then this configuration shall also be used by the UE to determine when it shall accept or ignore LWIP signalling.

4.9 Authentication and Security

4.9.1 Access Authentication in non-3GPP Accesses

Non-3GPP access authentication defines the process that is used for Access Control i.e. to permit or deny a subscriber to attach to and use the resources of a non-3GPP IP access which is interworked with the EPC network. Non-3GPP access authentication signalling is executed between the UE and the 3GPP AAA server/HSS. The authentication signalling may pass through AAA proxies.

3GPP based access authentication is executed across a SWa/STa reference point as depicted in the EPS architecture diagram. Following principles shall apply in this case:

- Transport of authentication signalling shall be independent of the non-3GPP IP Access technology.
- The 3GPP based access authentication signalling shall be based on IETF protocols, for e.g., Extensible Authentication Protocol (EAP) as specified in RFC 3748 [11].

The details of the access authentication procedure are defined in TS 33.402 [45].

4.9.2 Tunnel Authentication

Tunnel authentication refers to the procedure by which the UE and the ePDG perform mutual authentication during the IPsec tunnel establishment between the UE and the ePDG (SWu reference point).

Tunnel authentication is used only in case of Untrusted Non-3GPP Access and is executed across a SWm reference point as depicted in the EPS architecture diagram.

The details of the tunnel authentication procedure are defined in TS 33.402 [45].

4.10 QoS Concepts

4.10.1 General

The QoS model that is applied in conjunction with PMIP-based reference points does not use bearer IDs in user plane packets. Instead it is based on packet filters and associated QoS parameters (QCI, ARP, MBR, GBR) provided to the access system through off-path signalling.

The PCRF signals the same packet filters and associated QoS parameters over Gxa, Gxb and Gxc as over Gx; in other words the granularity of the QoS information that is passed over Gxa, Gxb and Gxc is the same as over Gx.

4.10.2 Void

4.10.3 The EPS Bearer with PMIP-based S5/S8 and E-UTRAN access

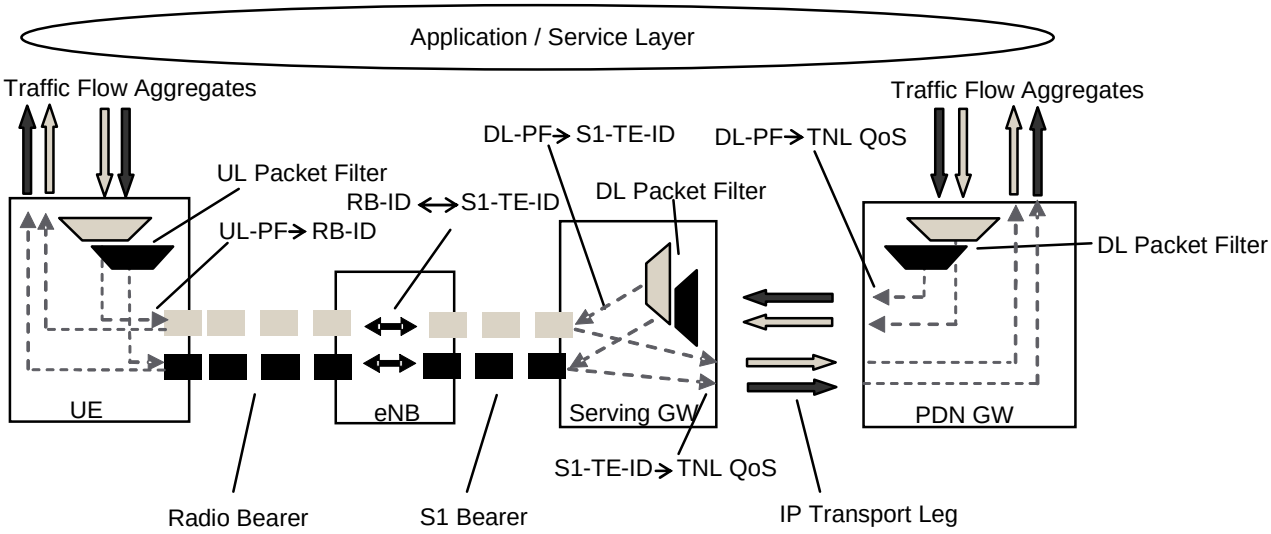


Figure 4.10.3-1: Two Unicast EPS bearers (PMIP-based S5/S8 and E-UTRAN access)

For PMIP-based S5/S8 and E-UTRAN access, an EPS bearer consists of the concatenation of one Radio Bearer and one S1 bearer. The PDN Connectivity Service between a UE and an external packet data network is supported through a concatenation of an EPS Bearer and IP connectivity between Serving GW and PDN GW. QoS control between a Serving GW and a PDN GW is provided at the Transport Network Layer (TNL).

The EPS bearer is realised by the following elements:

- In the UE, UL TFT maps a traffic flow aggregate to an EPS bearer in the uplink direction.
- In the Serving GW, the DL TFT maps a traffic flow aggregate to an EPS bearer in the downlink direction.
- A radio bearer transports the packets of an EPS bearer between a UE and an eNodeB. There is a one-to-one mapping between an EPS bearer and a radio bearer.
- An S1 bearer transports the packets of an EPS bearer between an eNodeB and a Serving GW. There is a one-to-one mapping between an EPS bearer and a S1 bearer.
- A per UE per PDN tunnel transports the packets of an EPS bearer between a Serving GW and a PDN GW. There is a many-to-one mapping between an EPS bearer and this per UE, per PDN tunnel.
- A UE stores a mapping between an uplink packet filter and a radio bearer to create the mapping between a traffic flow aggregate and a radio bearer in the uplink.

- An eNodeB stores a one-to-one mapping between a radio bearer and an S1 bearer to create the binding between a radio bearer and an S1 bearer in both the uplink and the downlink direction.
- A Serving GW stores a one-to-one mapping between a downlink packet filter and an S1 bearer to create the mapping between a traffic flow aggregate and an S1 bearer in the downlink.
- A PDN GW enforces APN-AMBR across all SDFs of the same APN that is associated with Non-GBR QCIs.

4.10.4 Application of PCC in the Evolved Packet System

EPS supports both static and dynamic PCC deployment options as specified in TS 23.401 [4].

NOTE 1: The local configuration of PCEF static policy and charging control functionality is not subject to standardization and is not based on subscription information.

In case of non-3GPP access that does not support an Gxa/b or S9 interface, static QoS policies (e.g. based on subscription QoS parameters for default connectivity) may be provided to the non-3GPP access through the AAA infrastructure. To perform policy enforcement according to the subscription QoS parameters for default connectivity, additional information may be provided to the PDN GW in one of the following ways:

- from the PCRF, if present and if the PDN GW supports the Gx interface;
- from the 3GPP AAA Server through the S6b interface in the form of a static QoS profile for the S2a, PMIP based S2b, and S2c reference points;
- from the ePDG through GTP based S2b in the form of a static QoS profile (Default EPS Bearer QoS), which the ePDG obtains from the 3GPP AAA Server through the SWm interface.

NOTE 2: In the two last cases, the PCEF may change the provided values based on interaction with the PCRF or based on local configuration.

When dynamic policy provisioning is not deployed, the PDN GW in case of PMIP or GTP based signalling uses the access type information (RAT Type in 3GPP access) contained in PMIP Proxy Binding Update messages or GTP Create Session Request messages for, e.g. charging. When dynamic policy provisioning is deployed, the PDN GW relies on the PCRF for indication of the handling required due to the access technology.

The behaviour of the system when PCC is deployed only in VPLMN or only in HPLMN is described in TS 23.203 [19].

For non-3GPP access that supports UEs with different Bearer Control Mode (BCM) capabilities, it should be possible for the UE to signal its BCM capabilities to the BBERF. It should also be possible for the BBERF to signal the selected BCM to the UE. How this information is exchanged between the UE and the BBERF is outside of the scope of 3GPP.

4.10.5 PDN connectivity service with GTP based S2b

For untrusted non-3GPP access to the EPC the PDN connectivity service is provided by IPsec connectivity between the UE and the ePDG concatenated with S2b bearer(s) between the ePDG and the PGW.

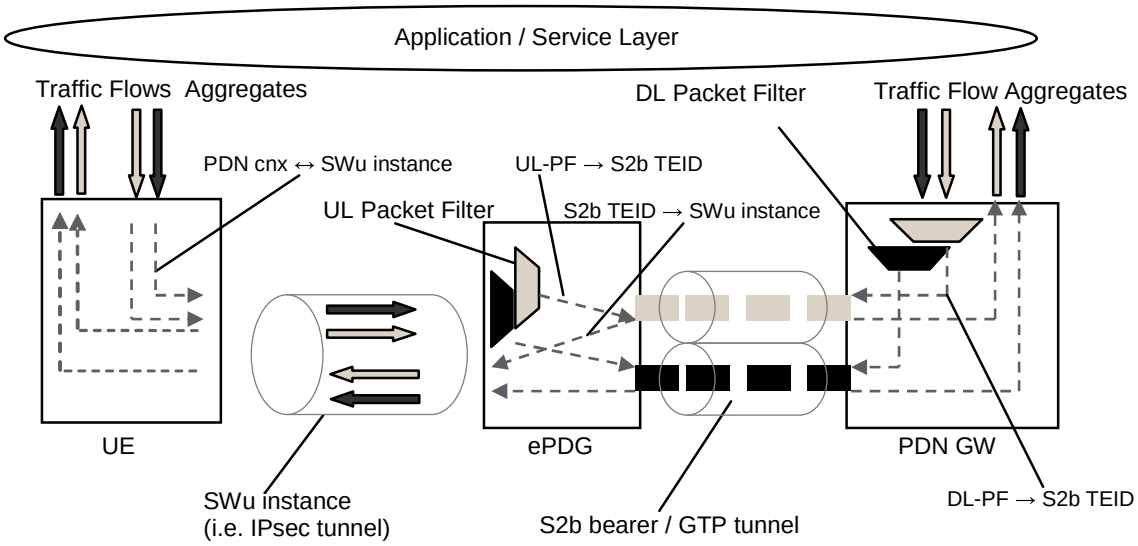


Figure 4.10.5-1: Two Unicast S2b bearers (GTP based S2b)

The SWu interface between the UE and the ePDG is identical for the GTP and PMIP variants of S2b. The UE establishes a separate SWu instance (i.e. a separate IPSec tunnel) for each PDN connection.

One default S2b bearer is established on the S2b interface when the UE connects to a PDN, and that remains established throughout the lifetime of the PDN connection to provide the UE with always-on IP connectivity to that PDN. Additional dedicated S2b bearers may be established on S2b for the same PDN connection depending on operator policy. The PGW establishes dedicated S2b bearers on S2b for the same PDN connection based on PCC decisions as specified in TS 23.203 [19].

The ePDG releases the SWu instance when the default S2b bearer of the associated PDN connection is released.

The S2b bearer is realized by the following elements:

- A GTP tunnel on S2b transports the packets of an S2b bearer between the ePDG and a PDN GW;
- The ePDG stores the mapping between uplink packet filters it receives from the PGW (e.g. in the Create Bearer Request message) and the corresponding S2b bearer;
- The PDN GW stores the mapping between downlink packet filters and an S2b bearer.

In support for the UE connectivity with the PDN:

- A SWu instance (i.e. a IPSec tunnel) transports the packets of all S2b bearer(s) for the same PDN Connection between the UE and the ePDG.

The ePDG routes uplink packets to the different bearers based on the uplink packet filters in the TFTs assigned to the bearers in the PDN connection, in the same way as a UE does for uplink traffic under 3GPP access. If no match is found, the uplink data packet shall be sent via the bearer that does not have any uplink packet filter assigned. If all bearers (including the default bearer for that PDN) have been assigned an uplink packet filter, the ePDG shall discard the uplink data packet.

The PDN GW routes downlink packets to the different bearers based on the downlink packet filters in in the TFTs assigned to the S2b bearers in the PDN connection, in the same way as the PDN GW does on GTP-based S5/S8 bearers (see TS 23.401 [4] clause 4.7.2.2).

4.11 Charging for Non-3GPP Accesses

The following are related to Non-3GPP accesses:

- Accounting information, e.g. the amount of data transmitted in uplink and downlink direction categorized with the QCI per UE, could be collected by components, if any, in the Non-3GPP access networks for inter-operator settlements.

NOTE: Specification of the above functionality is outside the scope of this TS.

4.12 Multiple PDN Support

General high level principles for the support of multiple PDNs are provided in TS 23.401 [4], clause 5.10.1. In addition, the following applies:

- Simultaneous exchange of IP traffic to multiple PDNs is supported in the EPS, when the network policies, non-3GPP access and user subscription allow it. UE Support for multiple overlapping IP address spaces is optional.

- Multiple PDN connections for a given APN and UE can be supported with the restrictions that all PDN connections for a given APN and UE shall use the same access network and shall all be moved to a new access network during handovers.

- If an additional PDN connection to the same APN occurs, and an existing PDN connection to that APN exists, the same PDN GW shall be selected.

- Multiple PDN connections to different APNs may use different access networks. The UE selects the access network where to route a specific PDN connection based on user preferences and operator's policies.

- A UE that is capable of routing different simultaneously active PDN connections through different access networks can do so if the UE is authorized by subscription to access each of the involved PDNs and each of the involved access networks.

- The access networks the UE can stay simultaneously connected with shall include no more than one 3GPP access and one and only one non-3GPP access.

NOTE: During the handover procedure the UE moves the PDN connections one-by-one, but the selective handover of the PDN connections to the same APN is not supported.

Once a specific IP mobility protocol is selected during initial attach for a specific non-3GPP access, it is not possible for the UE to use different mobility protocols for any of the PDNs that it obtains connectivity on the same non-3GPP access after initial attach. It is not possible for a UE that is connected to multiple PDNs over a 3GPP access to perform a handover to a non-3GPP access and then use different mobility protocols for the various PDNs that it connected with on the same non-3GPP access.

For the purpose of using MAPCON, the UE shall try to simultaneously connect to different APNs through different access networks only if the home network supports such simultaneous connectivity. The UE determines that the network supports such simultaneous connectivity over multiple accesses if the UE is provisioned with or has received per-APN inter-system routing policies (see clause 4.8.2.1) from the home network.

4.13 Detach principles

When a UE is attached to Evolved Packet Core via multiple access systems, the following principles shall apply during the detach procedure:

- A UE that is detaching from the Evolved Packet Core (e.g. a UE that is powering off) shall perform the UE initiated detach procedure on each of the access systems through which the UE is attached to Evolved Packet Core.
- A UE that is detaching from a specific access system and wants to preserve all or a subset of the active PDN connections that use that access system shall initiate UE initiated PDN disconnection procedure for each of the PDN connection which is not required to be preserved. The UE then shall initiate the applicable handover procedure to transfer to the access system through which the UE remains attached to the Evolved Packet Core each of the PDN connections to be preserved.
- When HSS initiates the detach procedure to delete the UE from the Evolved Packet Core (e.g. due to subscription expiry, etc), HSS/AAA initiated detach procedure should be performed towards each node registered for the UE.

5 Functional Description and Procedures for 3GPP Accesses with PMIP-based S5/S8

5.1 Control and User Plane Protocol Stacks

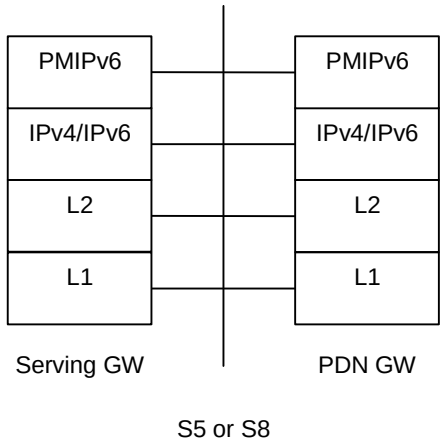
5.1.1 Void

5.1.2 General

TS 23.401 [4] defines the protocol stack for both the control plane and user plane for 3GPP accesses using GTP-based S5/S8. This clause defines the protocol stacks for 3GPP accesses using the PMIP-based S5/S8.

5.1.3 Control Plane

5.1.3.1 Serving GW - PDN GW



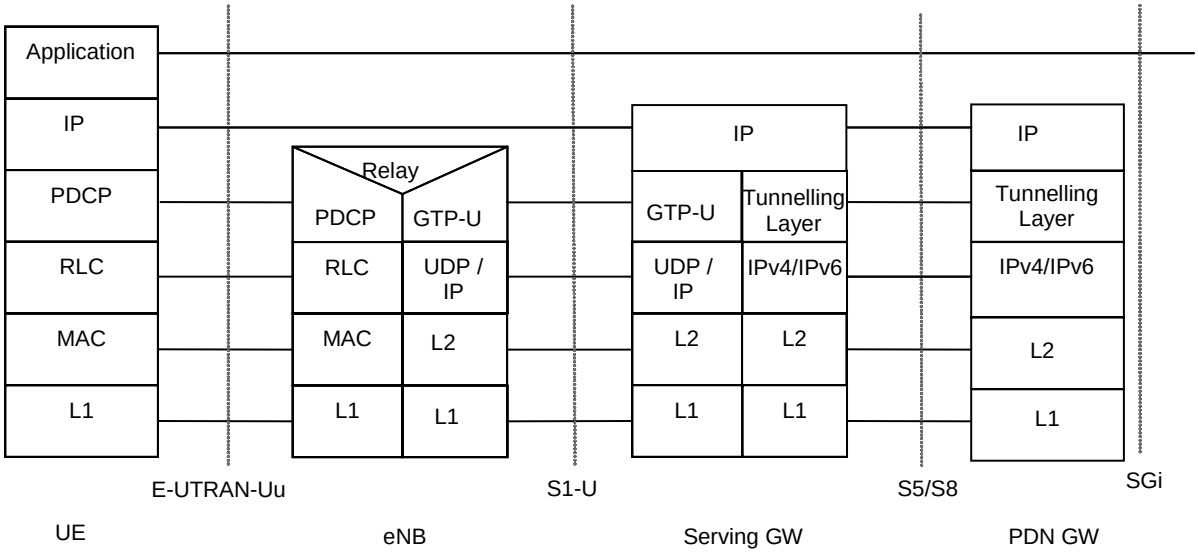
Legend:

- The control part of PMIPv6 specification, RFC 5213 [8]) protocol is used for signalling messages between Serving GW and PDN GW (S5 or S8).

Figure 5.1.3.1-1: Control Plane for PMIP-based S5 and PMIP-based S8 Interfaces

5.1.4 User Plane

5.1.4.1 UE – PDN GW User Plane with E-UTRAN

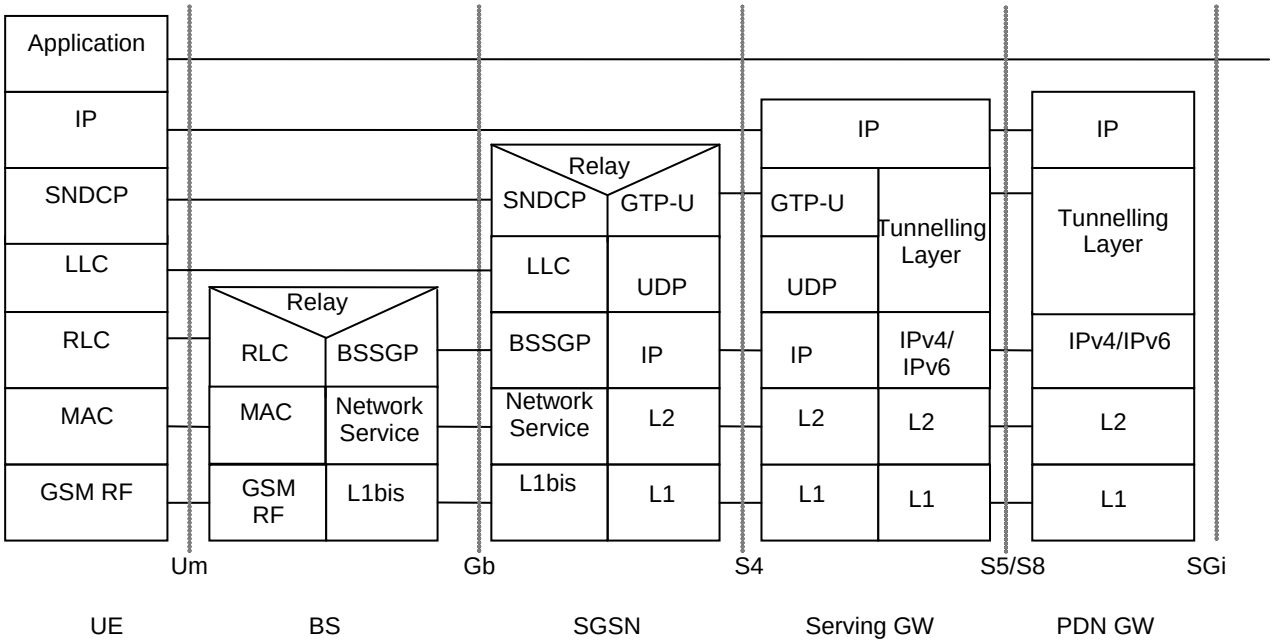


Legend:

- On the S5/S8 interface, the tunnelling layer implements GRE encapsulation applicable for PMIPv6.
- MME controls the user plane tunnel establishment and establishes User Plane Bearers between eNodeB and Serving GW.
- EUTRAN-Uu: The radio protocols of E-UTRAN between the UE and the eNodeB are specified in TS 36.300 [6].
- I**P:** This refers to network layer protocols. On the Serving Gateway this includes termination of the UE-Serving Gateway link-local protocols (e.g. IPv6 Router Solicitation/Advertisement) and forwarding of user plane IP packets between the UE-SGW point-to-point logical link and the S5/S8 tunnel for the UE.

Figure 5.1.4.1-1: User Plane for E-UTRAN

5.1.4.2 UE – PDN GW User Plane with 2G access via the S4 Interface

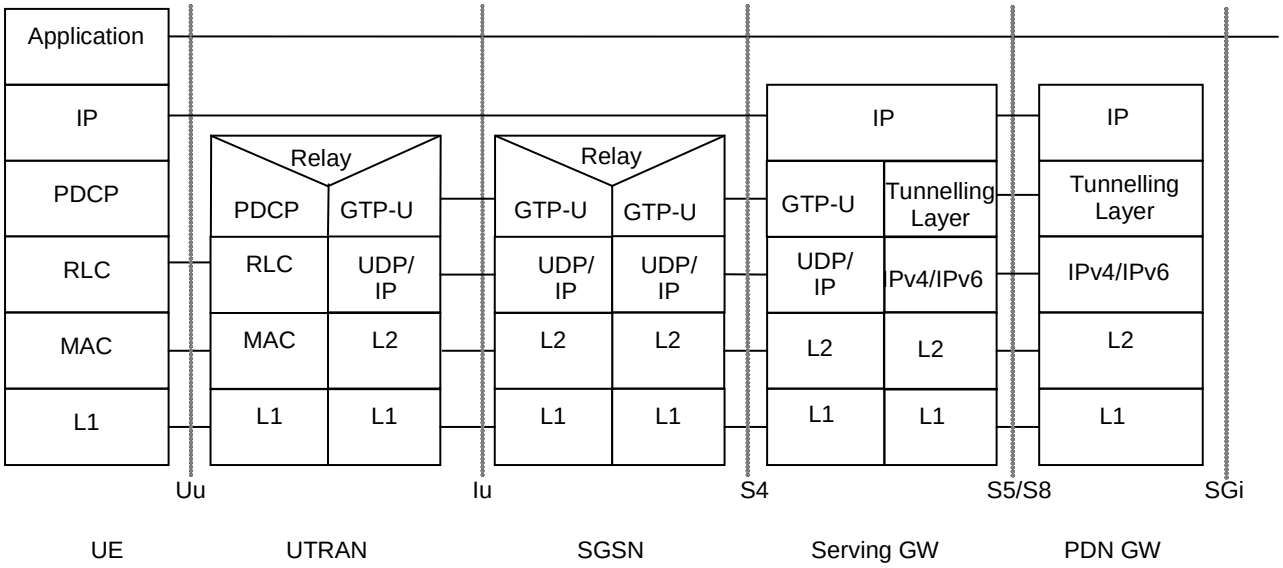


Legend:

- On the S5/S8 interface, the tunnelling layer implements GRE encapsulation applicable for PMIPv6.
- Protocols on the Um and the Gb interfaces are described in the TS 23.060 [21].
- **IP:** This refers to network layer protocols. On the Serving Gateway this includes termination of the UE-Serving Gateway link-local protocols (e.g. Router Solicitation/Advertisement) and forwarding of user plane IP packets between the UE-SGW point-to-point logical link and the S5/S8 tunnel for the UE.

Figure 5.1.4.2-1: User Plane for A/Gb mode

5.1.4.3 UE – PDN GW User Plane with 3G Access via the S4 Interface

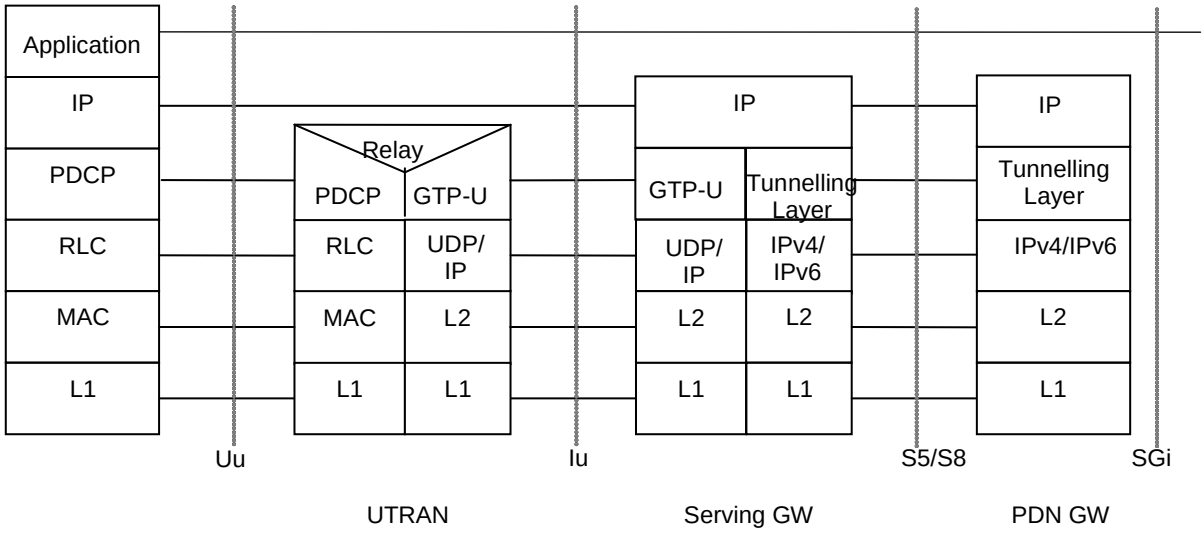


Legend:

- On the S5/S8 interface, the tunnelling layer implements GRE encapsulation applicable for PMIPv6.
- Protocols on the Uu and the Iu interfaces are described in the TS 23.060 [21].
- **IP:** This refers to network layer protocols. On the Serving Gateway this includes termination of the UE-Serving Gateway link-local protocols (e.g. IPv6 Router Solicitation/Advertisement) and forwarding of user plane IP packets between the UE-SGW point-to-point logical link and the S5/S8 tunnel for the UE.

Figure 5.1.4.3-1: User Plane for Iu mode

5.1.4.4 UE – PDN-GW User Plane with 3G Access via the S12 Interface



Legend:

- On the S5/S8 interface, the tunnelling layer implements GRE encapsulation applicable for PMIPv6.
- Protocols on the Uu interface are described in the TS 23.060 [21].
- SGSN controls the user plane tunnel establishment and may establish a Direct Tunnel between UTRAN and Serving GW.
- **IP:** This refers to network layer protocols. On the Serving Gateway this includes termination of the UE-Serving Gateway link-local protocols (e.g. IPv6 Router Solicitation/Advertisement) and forwarding of user plane IP packets between the UE-SGW point-to-point logical link and the S5/S8 tunnel for the UE.

Figure 5.1.4.4-1: User Plane for UTRAN mode and Direct Tunnel on S12

5.2 Initial E-UTRAN Attach with PMIP-based S5 or S8

This clause is related to the case when the UE powers-on in the LTE network with PMIP-based S5 or S8 interface and includes the case of roamers from a GTP network into a PMIPv6 network when PMIP-based S5 is used to connect the Serving GW and the PDN GW of the visited PLMN. Proxy Mobile IP version 6 is used on S5 or S8 interface. It is assumed that the MAG is collocated with the Serving GW for the PMIPv6 procedure between the Serving GW and the PDN GW.

When only GTP-based S5 or S8 connections are established for roamers from a GTP network into a PMIPv6 network the procedure as described in TS 23.401 [4] applies.

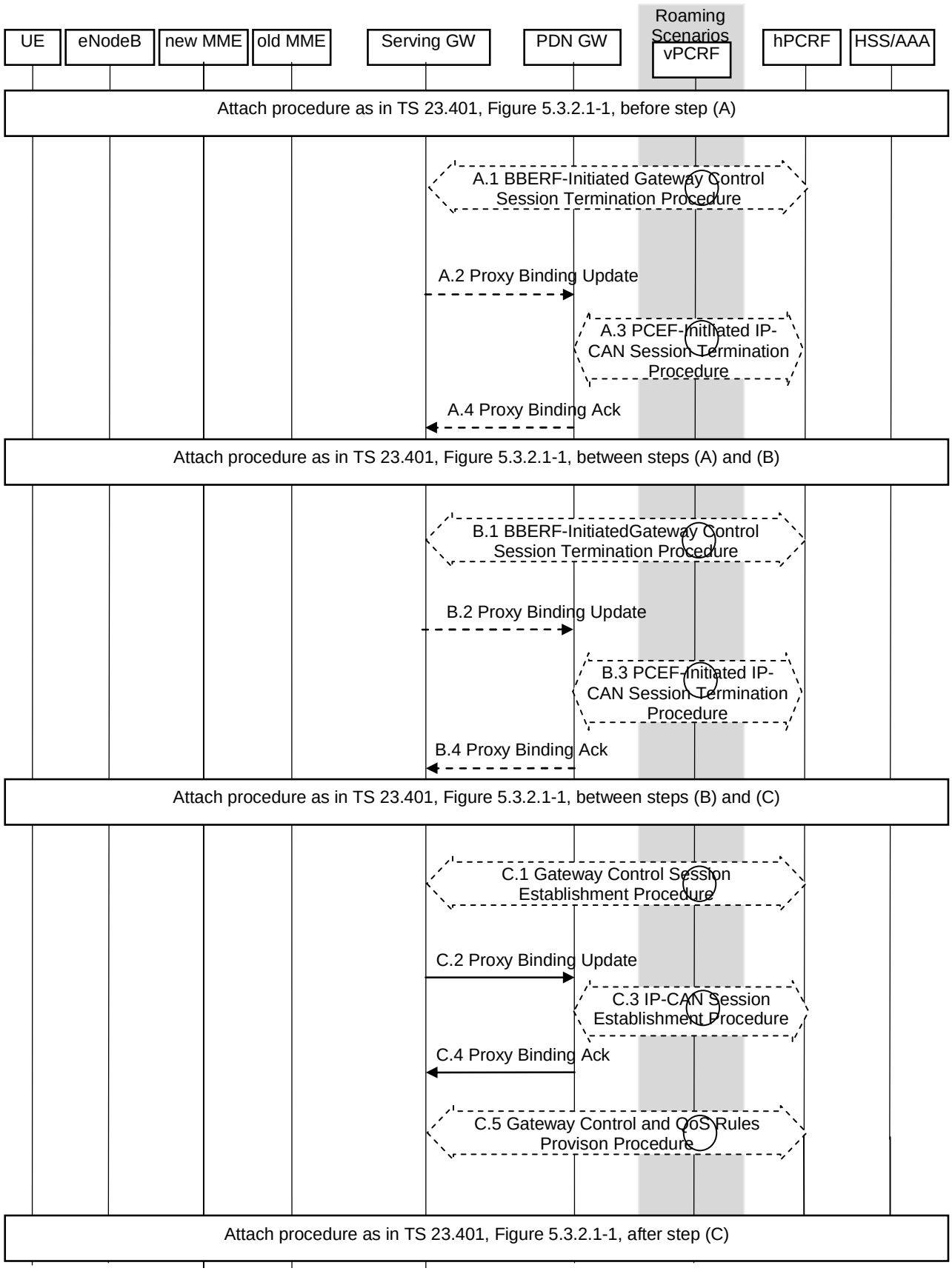


Figure 5.2-1: Initial E-UTRAN attach with PMIP-based S5 or S8

This procedure applies to the Non-Roaming (Figure 4.2.1-1), Roaming (Figure 4.2.1-2) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the Serving GW and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF.

This procedure is also used to establish the first PDN connection over E-UTRAN with PMIP based S5 or S8 when the UE already has active PDN connections only over a non-3GPP access network and wishes to establish simultaneous PDN connections to different APNs over multiple accesses.

The optional interaction steps between the gateways and the PCRF in the procedures in figure 5.2-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

A.1) The Serving GW initiates the Gateway Control Session Termination Procedure with the PCRF, as specified in TS 23.203 [19]. The S-GW provides information to enable the PCRF to uniquely identify the IP-CAN session. This results in the removal of the Gateway Control session in S-GW.

A.2) The Serving GW sends a Proxy Binding Update (MN NAI, lifetime=0) message to the PDN GW. The MN NAI identifies the UE. The lifetime field indicates that the message is used to de-register the UE at the PDN-GW.

A.3) The PDN GW initiates the IP CAN session Termination Procedure with the PDN GW as specified in TS 23.203 [19]. The PDN GW provides information to enable the PCRF to uniquely identify the IP-CAN session. This results in the removal of IP-CAN session related information in the PCRF and in the PDN-GW.

A.4) The PDN GW responds to the Serving GW with the result of the deregistration with Proxy Binding Update Acknowledgement message.

Steps between A.4 and B.1 and steps between B.4 and C.1 are described in TS 23.401 [4], clause 5.3.2.1.

Steps B.1 to B.4 are the same as Steps A.1 through A.4.

C.1) The Serving GW initiates the Gateway Control Session Establishment Procedure with the PCRF, as specified in TS 23.203 [19]. The S-GW provides the information to the PCRF to correctly associate it with the IP-CAN session to be established in step C.3 and also to convey subscription related parameters to the PCRF that have been received between steps (B) and (C) from the MME, including the APN-AMBR and Default Bearer QoS. The Serving GW provides in addition the UE Location Information IE and user CSG information, if available. The Serving GW also indicates its support for the extended TFT filter format.

In the case of Emergency Attach, if the IMSI provided by the MME to the S-GW in step before C.1 is marked as unauthenticated, the SGW provides this IMSI marked as unauthenticated to the PCRF in the GW Control Session Establishment. This IMSI marked as unauthenticated is provided by the PCRF to the PDN GW in step C.3. In this case, the IMEI is used as the UE Identity in the message to the PCRF.

C.2) The Serving GW sends a Proxy Binding Update (MN NAI, Lifetime, Access Technology Type, Handover Indicator, APN, GRE key for downlink traffic, UE Address Info Additional Parameters, Charging Characteristics) to the PDN GW in order to establish the new registration. The MN NAI identifies the UE for whom the message is being sent. The Lifetime field must be set to a nonzero value in the case of a registration. Access Technology Type is set to indicate 3GPP access to EPS. Handover Indication option is set to indicate attachment over a new interface as no Handover indication is received from the MME. The APN may be necessary to differentiate the intended PDN from the other PDNs supported by the same PDN GW. The Serving GW includes the EPS bearer identity of the default bearer received from the MME if multiple PDN connections to the same APN are supported. The optional Additional Parameters may contain information, for example, protocol configuration options. The UE Address Info IE is used to request an IPv6 prefix, IPv4 address, or both IPv4 address and IPv6 prefix. Based on PDN Type parameter received in the Create Session Request, Serving GW includes request for IPv4 Home Address (PDN Type set to IPv4), or IPv6 Home Network Prefix (PDN type set to IPv6) or both IPv4 home address and IPv6 HNP (PDN type set to IPv4v6) in the PBU as specified in PMIPv6 specification, RFC 5213 [8]). In the case of a subscribed IPv4 address and/or IPv6 prefix provided by the MME in the PDN Address Allocation IE, the UE Address Info IE is set to the subscribed IPv4 address and/or IPv6 prefix.

In case of Emergency Attach, if IMSI is not provided by MME to SGW or the IMSI provided is marked as unauthenticated, the S-GW creates MN NAI based on IMEI as specified in TS 23.003 [16].

NOTE 1: Any time after Step C.1 is initiated, Step C.2 can be initiated by MAG.

C.3) The PDN GW initiates the IP CAN Session Establishment Procedure with the PCRF, as specified in TS 23.203 [19]. The PDN GW provides information to the PCRF used to identify the session and associate Gateway Control Sessions established in step C.1 correctly. The PDN GW also provide the PCRF with the UE IPv4 address and/or IPv6 prefix newly assigned as a result of step C.2, which might lead the PCRF to update the

QoS rules to include this IPv4 address and/or IPv6 prefix. The PCRF creates IP-CAN session related information and responds to the PDN GW with PCC rules UE Location Information IE, user CSG information, if received from the Serving GW, and event triggers.

In case of Emergency Attach, if MN NAI based on IMEI is received in the PBU message in step C.2, the PDN GW uses the IMEI as a UE Identity in the message to the PCRF.

C.4) The PDN GW responds with a PMIPv6 Binding Acknowledgement (MN NAI, Lifetime, UE Address Info, GRE key for uplink traffic, Charging ID, Additional Parameters) message to the Serving GW. The MN NAI is identical to the MN NAI sent in the Proxy Binding Update. The Lifetime indicates the duration the binding will remain valid. The PDN GW takes into account the request from Serving GW and the policies of operator when the PDN GW allocates the UE Address Info. The UE address info returns the newly assigned IPv4 address and/or IPv6 prefix assigned to the UE, if one was requested in the PMIPv6 Proxy Binding Update message. IP address allocation by the PDN-GW is as stated in clause 4.7.1. "IP Address Allocation with PMIP-based S5/S8". If the PDN GW sends the DHCPv4 Address Allocation Procedure Indication in the Proxy Binding Acknowledgement message, the UE IPv4 address assigned by the PDN GW is not provided as part of the default bearer activation procedures to the UE. In this case, the Serving GW does not forward the IPv4 address assigned by the PDN GW to the MME, but sets the PDN Address to 0.0.0.0 in the message to the MME. If a valid IPv4 address and/or IPv6 prefix received in the Proxy Binding Update message, the PDN GW validates the addresses and returns it the UE Address Info IE of the Proxy Binding Acknowledge message. If the corresponding Proxy Binding Update contains the EPS bearer identity, the PDN GW shall acknowledge if multiple PDN connections to the given APN are supported. The Charging ID is assigned for the PDN connection for charging correlation purposes. The optional Additional Parameter information element may contain other information, including for example Protocol Configuration Options.

NOTE 2: In case the QoS rules have changed, the PCRF updates the QoS rules at the S-GW by initiating the GW Control Session Modification Procedure, as specified in TS 23.203 [19].

NOTE 3: QoS rules may lead to establishment of new dedicated bearers along with the default bearer.

C.5) The PCRF initiates the Gateway Control and QoS Rules Provision Procedure specified in TS 23.203 [19] by sending a message with the QoS rules and Event Trigger information to the S-GW. The PCRF also indicates whether the extended TFT filter format is to be supported for the PDN connection.

NOTE 4 The Serving GW learns from the PBA whether the PDN GW supports multiple PDN connections to the same APN or not.

After steps C.1-C.5 the procedure continues as it is defined in clause 5.3.2 in TS 23.401 [4] with the exception that the steps in block D are not performed.

5.3 Detach for PMIP-based S5/S8

The procedure in this clause provides the PMIPv6-based S5/S8 variants to all E-UTRAN Detach Procedures, including UE, MME or HSS initiated detach procedure (TS 23.401 [4] clause 5.3.8).

In case of detach, all the bearers at the Serving GW are terminated. Further, the IP CAN session for the UE in the PDN GW is also terminated.

If the UE is connected to both E-UTRAN and a non-3GPP access before the UE triggers detach on E-UTRAN, and the UE wants to preserve all or a subset of the active PDN connections routed over E-UTRAN system, a UE initiated PDN disconnection procedure shall be performed for each of the PDN connections that are not required to be preserved. The UE then shall initiate the applicable handover procedure to transfer to the access system through which the UE remains attached to the Evolved Packet Core each of the PDN connections to be preserved.

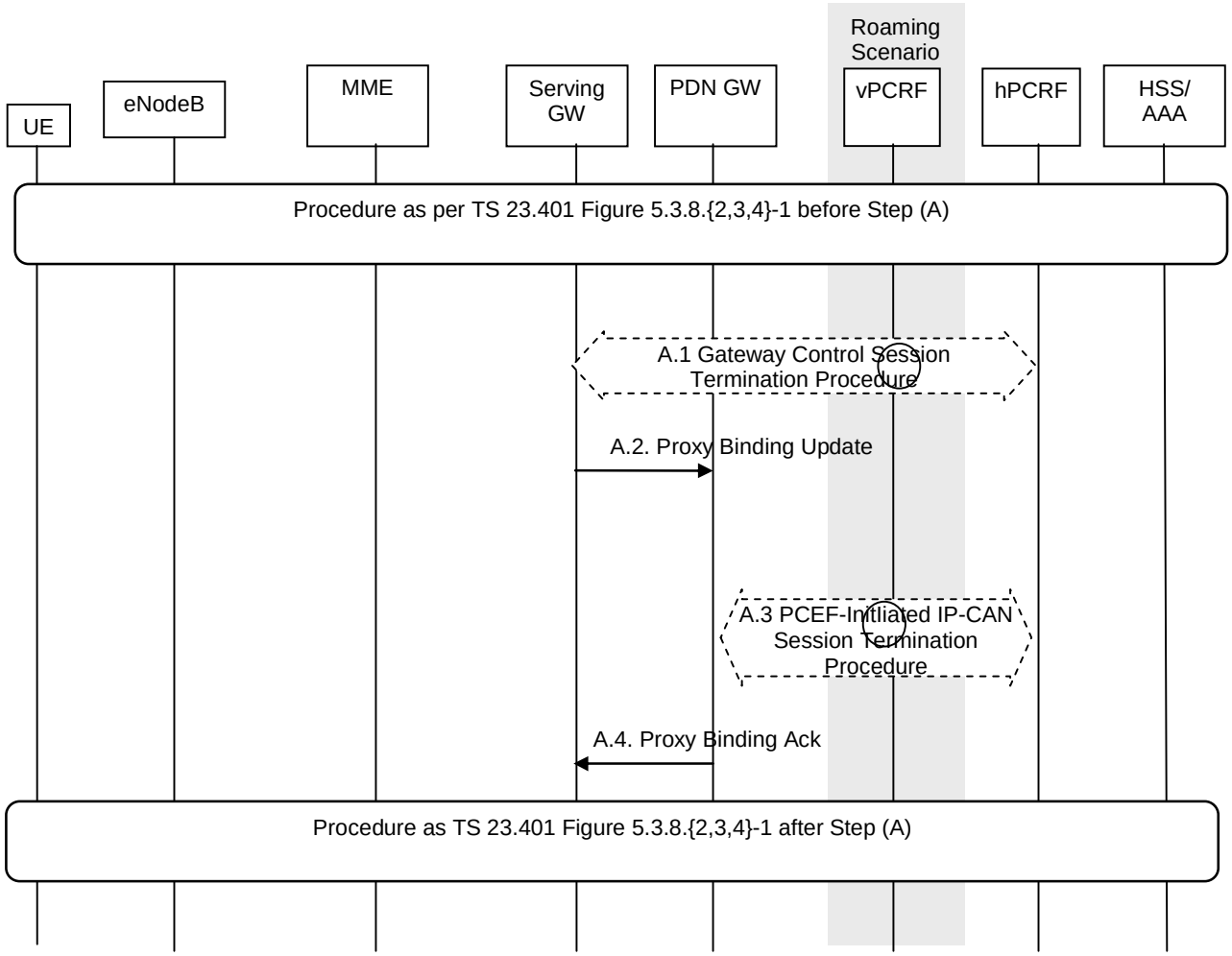


Figure 5.3-1: E-UTRAN Detach Procedure for PMIP-based S5/S8

NOTE: When multiple PDN connections are active a part of this procedure including steps A.1 to A.4 are repeated for each PDN connection of the UE.

The optional interaction steps between the gateways and the PCRF in Figure 5.3-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

This procedure applies to the Non-Roaming (Figure 4.2.1-1), Roaming (Figure 4.2.1-2) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the Serving GW and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF.

In the non-roaming case, the vPCRF is not involved at all.

A.1) The Serving GW initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [19]. The S-GW provides information to enable the PCRF to unambiguously identify the IP-CAN session corresponding to the Gateway Control Session and indicates User Location Information and/or UE Time Zone Information to the PCRF as an Event Report if the corresponding event trigger is set. This results in the removal of the Gateway Control session in S-GW.

A.2) The Serving GW sends a Proxy Binding Update (MN NAI, APN, lifetime=0) message to the PDN GW to release the PDN connection of the UE at the PDN-GW. If only one PDN connection per APN is supported then the MN NAI and the APN identify the PDN connection of the UE. If multiple PDN connections per APN are supported then the MN NAI, the APN and the EPS bearer identity of the default bearer identify the PDN connection of the UE. The lifetime field indicates that the message is used to release the PDN connection of the UE at the PDN-GW.

A.3) The PDN GW initiates the PCEF-Initiated IP-CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [19]. The PDN GW provides information to enable the PCRF to uniquely identify the

IP-CAN session. This results in the removal of IP-CAN session related information in the PCRF and in the PDN GW.

A.4) The PDN GW responds to the Serving GW with the result of the PDN connection release with Proxy Binding Update Acknowledgement

5.4 Dedicated Bearer Procedures for E-UTRAN Access with PMIP-based S5/S8

5.4.1 General

The procedure given in Figure 5.4.1-1 applies to all dedicated resource allocation operations for E-UTRAN which are triggered by PCRF, with the only exception of MME-initiated Dedicated Bearer Deactivation procedure which is covered in clause 5.4.5.3 The procedures initiated by the S-GW in the E-UTRAN differ for each case.

The procedure described in Figure 5.4.1-1 shows only the steps, due to PMIP based S5/S8, that are different from the GTP variant of the procedure given in TS 23.401 [4].

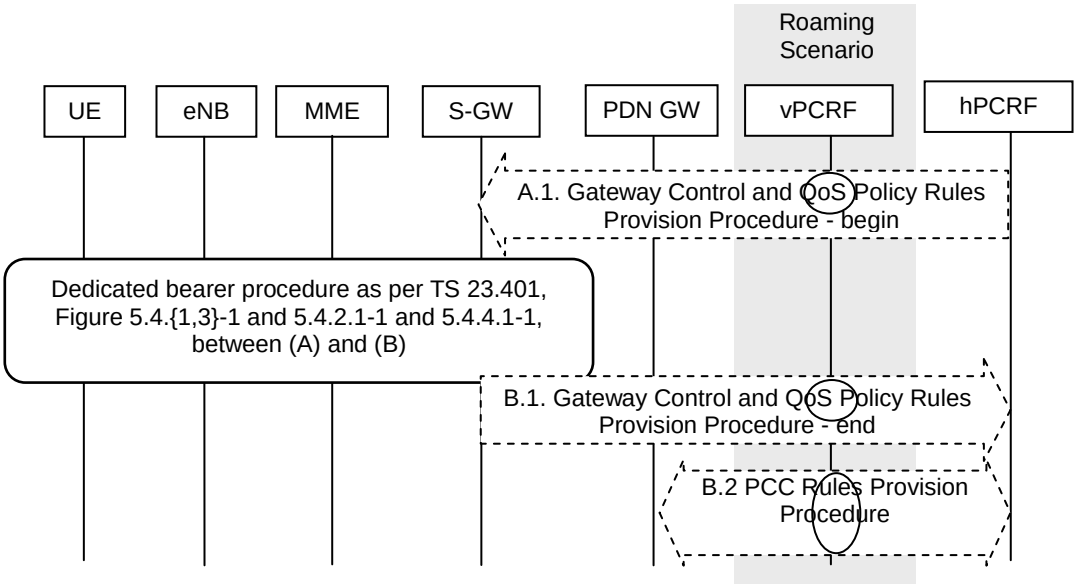


Figure 5.4.1-1: Dedicated Resource Allocation Procedure, UE in Active Mode

This procedure applies to the Non-Roaming (Figure 4.2.1-1), Roaming (Figure 4.2.1-2) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the Serving GW and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF.

If dynamic policy provision is not deployed, the steps shown in the figure are not taken. Instead, a configured static policy may be applied.

A.1) The PCRF initiates the Gateway Control and QoS Rules Provision Procedure specified in TS 23.203 [19] by sending a message with the QoS rules and Event Trigger information to the S-GW.

Steps between A.1 and B.1 are described in TS 23.401 [4], clauses 5.4.{1, 2.1, 3, 4.1}.

NOTE 1: For a PMIP-based S5/S8, before procedure steps (step 3 of TS 23.401 [4], clause 5.4.1), the PCRF sends a PCC decision provision (QoS policy) message to the S-GW and not to the P-GW as done for GTP-based S5/S8. The S-GW uses this QoS policy to determine that traffic flow(s) shall be aggregated to or removed from an active bearer. The S-GW generates the TFT and updates the EPS Bearer QoS to match the aggregated set of traffic flows. It is possible that the S-GW bearer binding function will result in the modification, creation or removal of bearers at this point. For modification, the S-GW sends an Update Bearer Request (PTI, EPS Bearer Identity, EPS Bearer QoS, TFT) message to the MME. For creation of a dedicated bearer, the S-GW sends a Create Bearer message and for removal, the S-GW sends a Delete Bearer Request.

B.1) The Serving GW indicates to the PCRF whether the requested QoS Policy Rules Provision could be enforced or not thus completing the GW Control and QoS Rules Provision procedure started in step A.1. The Serving GW indicates User Location Information and/or UE Time Zone Information to the PCRF as an Event Report if the corresponding event trigger is set.

B.2) The PCRF initiates the PCC Rules Provision Procedure as specified in TS 23.203 [19]. The PCRF provides updated PCC rules to the PCEF for enforcement by means of an PCC Rules Provision procedure specified in TS 23.203 [19].

NOTE 2: Step B.2 may occur before step A.1 or performed in parallel with steps A.1-B.1 if acknowledgement of resource allocation is not required to update PCC rules in PCEF. For details please refer to TS 23.203 [19].

Interactions between PCRF initiated dedicated bearer procedure and handover are described in clauses 5.7.1 and 5.7.2.

5.4.2 Dedicated Bearer Activation

When the QoS Policy rules provided by the PCRF to the Serving Gateway in Step A.1 of Figure 5.4.1-1 above result in the Serving Gateway to decide to activate a dedicated bearer, this procedure is applied.

The procedure depicted in Figure 5.4.1-1 applies for this case. On receiving message A.1, the Serving GW decides that a new bearer needs to be activated, the Serving GW uses this QoS policy to assign the EPS Bearer QoS, i.e., it assigns the values to the bearer level QoS parameters (excluding AMBR); see TS 23.401 [4] clause 4.7.3. The Serving GW follows the procedure shown in TS 23.401 [4], clause 5.4.1 by sending a Create Bearer Request message (EPS Bearer QoS, TFT, S1 TEID) to the MME.

The message descriptions for A.1, B.1 and B.2 in clause 5.4.1 apply to this case as well. The steps between A.1 and B.1 are described in TS 23.401 [4], clause 5.4.1.

5.4.3 Bearer Modification with Bearer QoS Update

5.4.3.1 PCC Initiated Bearer Modification with Bearer QoS Update

When the QoS Policy rules provided by the PCRF to the Serving Gateway in step A.1 of Figure 5.4.1-1 above results in the Serving Gateway to decide to modify the QoS of an already existing bearer, this procedure is applied. QoS modification may result in a bearer modification in the E-UTRAN access.

The procedure depicted in Figure 5.4.1-1 applies to this case as well. On receiving message A.1, the Serving GW uses this QoS policy to determine that traffic flow(s) shall be aggregated to or removed from an active bearer. The Serving GW generates the TFT and updates the EPS Bearer QoS to match the aggregated set of traffic flows. The Serving GW then follows the procedure shown in TS 23.401 [4], clause 5.4.2 by sending the Update Bearer Request (EPS Bearer QoS, TFT) message to the MME.

The message descriptions for A.1, B.1 and B.2 in clause 5.4.1 apply to this procedure as well. The steps between A.1 and B.1 are described in TS 23.401 [4], clause 5.4.2.1.

5.4.3.2 HSS-Initiated Subscribed QoS Modification

The HSS Initiated Subscribed QoS Modification for a PMIP-based S5/S8 is depicted in Figure 5.4.3.2-1.

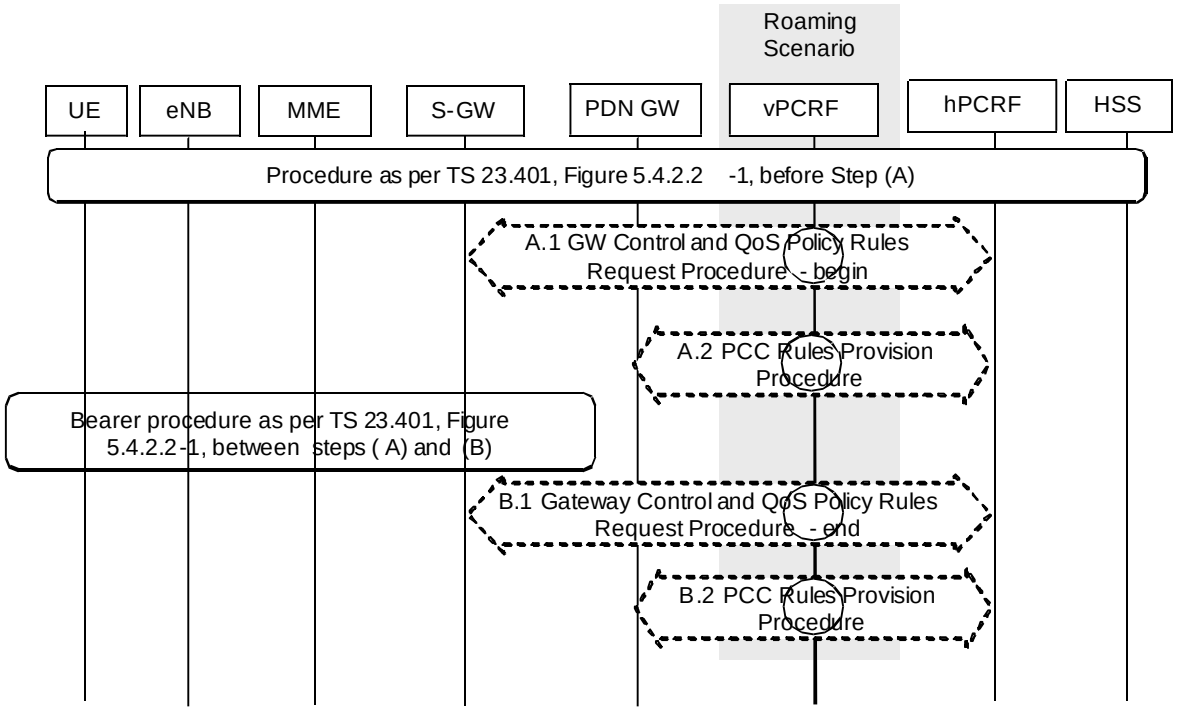


Figure 5.4.3.2-1: HSS-initiated Subscribed QoS Modification

A.1. The Serving GW initiates the Gateway Control and QoS Policy Rules Request Procedure with the PCRF as specified in TS 23.203 [19]. The S-GW provides the updated default EPS Bearer QoS for the default bearer to the PCRF and the PCRF responds with updated QoS rules. The PCRF makes a PCC decision as a result of the Gateway Control and QoS policy request and provides the updated QoS Rules to the Serving GW.

A.2. The PCRF initiates the PCC Rules Provision Procedure with the PDN GW as specified in TS 23.203 [19] to updates the rules in the PDN GW.

After Step A.1, the Serving GW follows the procedure shown in TS 23.401 [4], clause 5.4.2.1 by sending the Update Bearer Request message to the MME. The procedure is completed when the Serving GW receives a Update Bearer Response from the MME in Step 10 of TS 23.401 [4] clause 5.4.2.1.

B.1. The Serving GW indicates to the PCRF whether the requested QoS Policy Rules Provision could be enforced or not and thus completing the GW Control and QoS Rules Provision procedure started in step A.1.

B.2. The PCRF executes the Policy and Charging Rules Provision Procedure as specified in TS 23.203 [19] to update the PCC rules in the PDN GW.

NOTE: Step B.2 may be performed in parallel with steps A.1-B.1 if acknowledgement of resource allocation is not required at the PCRF to update PCC rules in PCEF. For details please refer to TS 23.203 [19].

5.4.4 Dedicated Bearer Modification without Bearer QoS Update

When the QoS Policy rules provided by the PCRF to the Serving Gateway in step A.1 of figure 5.4.1-1 above results in the Serving Gateway to decide to only update the set of TFTs corresponding to an already existing dedicated bearer, this procedure is applied.

NOTE: If neither the contents of the TFT nor the APN-AMBR are modified, this procedure does not apply.

The procedure depicted in Figure 5.4.1-1 applies to this case as well. On receiving message A.1, the Serving GW uses this QoS policy to determine that traffic flow(s) shall be aggregated to or removed from an active dedicated bearer. The Serving GW generates the TFT and determines that no update of the EPS Bearer QoS is needed. The Serving GW then follows the procedure shown in TS 23.401 [4], clause 5.4.3 by sending the Update Bearer Request (TFT) message to the MME.

The message descriptions for A.1, B.1 and B.2 in clause 5.4.1 apply to this procedure as well. The steps between A.1 and B.1 are described in TS 23.401 [4], clause 5.4.3.

5.4.5 Dedicated Bearer Deactivation

5.4.5.1 PCC-initiated Dedicated Bearer Deactivation

When the QoS Policy rules provided by the PCRF to the Serving Gateway in step A.1 of figure 5.4.1-1 above results in the Serving Gateway to decide to deactivate an existing dedicated bearer, this procedure is applied.

The procedure depicted in Figure 5.4.1-1 applies to this case as well. On receiving message A.1, the Serving GW uses this QoS policy to determine that a dedicated bearer needs to be deactivated, the Serving GW follows the procedure shown in TS 23.401 [4], clause 5.4.4 by sending the Delete Bearer Request message to the MME. If the S-GW determines that the default bearer needs to be deactivated, the S-GW follows the procedure specified in clause 5.6.2.1.

The message descriptions for A.1, B.1 and B.2 in clause 5.4.1 apply to this procedure as well. The steps between A.1 and B.1 are described in TS 23.401 [4], clause 5.4.4.1.

5.4.5.2 Void

5.4.5.3 MME-initiated Dedicated Bearer Deactivation

This clause contains the procedure steps that vary between the GTP and PMIP variant of S5 and S8 for the procedure defined in TS 23.401 [4], clause 5.4.4.2 for -MME initiated dedicated bearer deactivation.

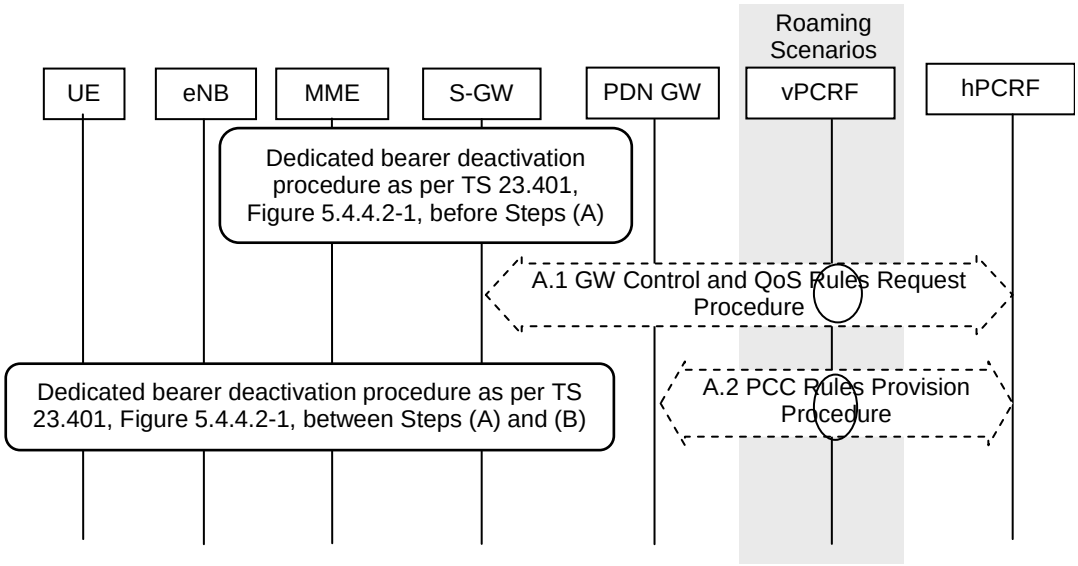


Figure 5.4.5.3-1: MME-initiated Dedicated Bearer Deactivation

This procedure applies to the Non-Roaming (Figure 4.2.1-1), Roaming (Figure 4.2.1-2) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the Serving GW and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF.

The optional interaction steps between the gateways and the PCRF in the procedures in Figure 5.4.5.3-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

Before Step A.1, the procedure shown in TS 23.401 [4], clause 5.4.4.2 is followed and the Serving GW receives a Delete Bearer Command message from the MME.

A.1) The Serving GW decides to deactivate the bearers and initiates the Gateway Control and QoS Policy Rules Request Procedure with the PCRF as specified in TS 23.203 [19]. The Serving GW informs the PCRF about the deleted QoS Rules and indicates User Location Information and/or UE Time Zone Information to the PCRF as an Event Report if the corresponding event trigger is set.

A.2) The PCRF initiates the PCC Rules Provision Procedure with the PDN GW as specified in TS 23.203 [19] to updates the rules in the PDN GW. The PCC rules provide the PDN GW with information required to enforce the remaining dedicated resource allocation policy, after removing PCC rules corresponding to the QoS rules deactivated by step A.1.

After step A.1, the Serving GW follows the procedure shown in TS 23.401 [4], clause 5.4.4.2 by sending the Delete Bearer Request message to the MME. The Serving GW does not need to wait for step A.1 to complete to proceed with the deactivation of bearers with the MME. The procedure is completed when the Serving GW receives a Delete Bearer Response from the MME in Step 8 of TS 23.401 [4], clause 5.4.4.2.

5.5 UE-initiated Resource Request and Release

This clause is related to the case when UE-initiated resource request and release is supported, and it is utilized for the PMIP-based S5/S8 traffic flow aggregates.

In the non-roaming case, vPCRF will not be involved.

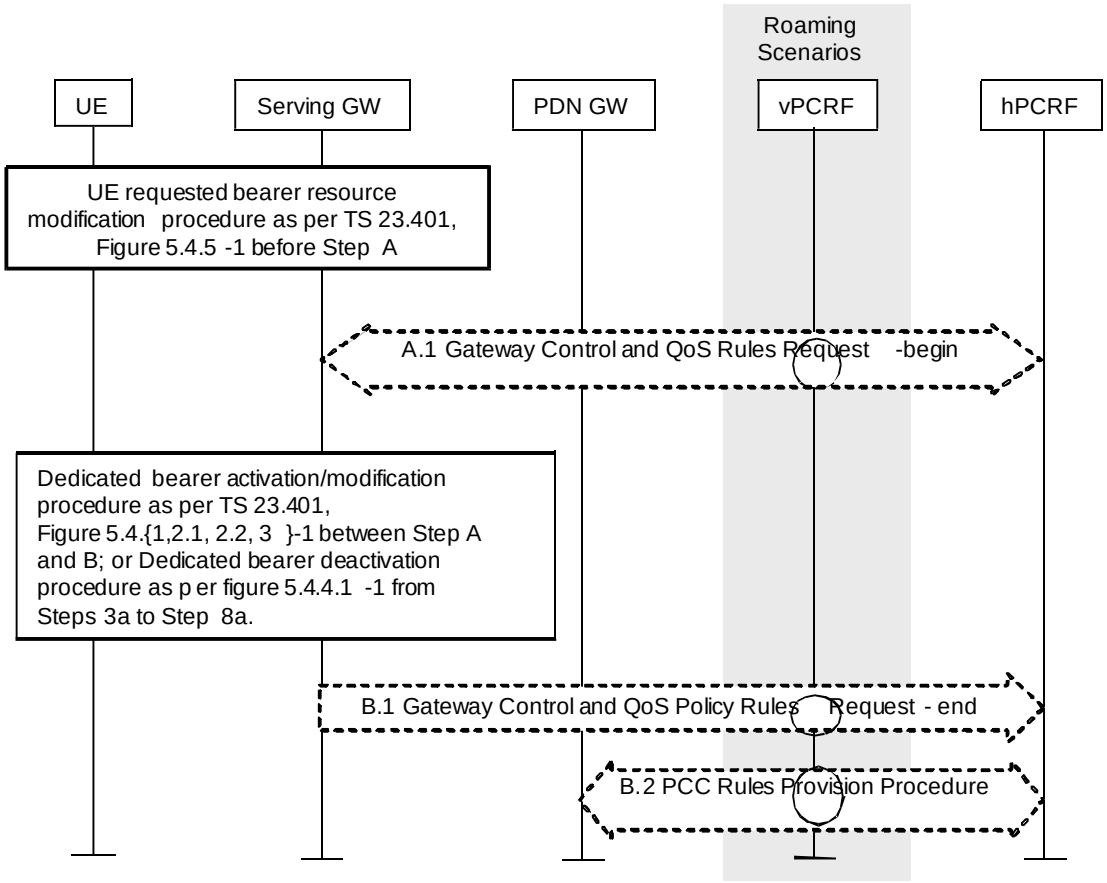


Figure 5.5-1: UE-initiated resource request/release with PMIP-based S5/S8

This procedure applies to the Non-Roaming (Figure 4.2.1-1), Roaming (Figure 4.2.1-2) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the Serving GW and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF.

The optional interaction steps between the gateways and the PCRF in the procedures in Figure 5.5-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

A.1. The Serving GW initiates the Gateway Control and QoS Policy Rules Request Procedure as specified in TS 23.203 [19]. The Serving GW provides the content of the Traffic Aggregate Description (TAD) and the requested QoS change to the PCRF as an Event Report. The PCRF makes a PCC decision as a result of the Gateway Control and QoS policy request and provides the updated QoS Rules to the Serving GW. The PCRF declaration of support for the extended TFT filter format is a precondition for the Serving GW accepting and forwarding TAD filters that use the extended TFT filter format to the PCRF.

Steps between A.1 and B.1 are described in TS 23.401 [4], clauses 5.4.1, 5.4.2 and 5.4.3 for resource allocation/modification or clause 5.4.4.1 for resource deactivation. Based on the QoS policy rules, the Serving GW decides whether to initiate a dedicated resource allocation activation or dedicated resource allocation modification (with or without QoS update).The Serving GW uses this QoS policy to assign the EPS Bearer QoS, i.e. it assigns the values to the bearer level QoS parameters (excluding AMBR); see clause 4.7.3 of TS 23.401 [4] and sends the appropriate message to the MME.

B.1. The Serving GW indicates to the PCRF whether the requested QoS Policy Rules Provision could be enforced or not and indicates User Location Information and/or UE Time Zone Information to the PCRF as an Event Report if the corresponding event trigger is set. This completes the GW Control and QoS Rules Provision procedure started in step A.1.

B.2. The PCRF initiates the Policy and Charging Rules Provision Procedure as specified in TS 23.203 [19] to update the PCC rules in the PDN GW.

NOTE: Step B.2 may be performed in parallel with Steps A.1-B1 if acknowledgement of resource allocation is not required at the PCRF to update PCC rules in PCEF. For details please refer to TS 23.203 [19].

5.6 Multiple PDN Support with PMIP-based S5/S8

5.6.1 UE requested PDN connectivity

The UE requested PDN connectivity procedure for E-UTRAN is depicted in figure 5.6.1-1. The procedure allows the UE to request for connectivity to an additional PDN over E-UTRAN, including allocation of a default bearer, when the UE already has active PDN connections over E-UTRAN. This procedure is also used to request for connectivity to an additional PDN over E-UTRAN when the UE is simultaneously connected to E-UTRAN and a non-3GPP access, and the UE already has active PDN connections over both the accesses. In this procedure, the UE is assumed to be in active mode. Proxy Mobile IP is used on S5 or S8 interface. It is assumed that the MAG is collocated with the Serving GW for the PMIPv6 procedure between the Serving GW and the PDN GW.

When only GTP-based S5 or S8 connections are established for roamers from a PMIP network into a GTP network the procedure as described in clause 5.10.2 of TS 23.401 [4] applies.

When PMIP-based S5/S8 is used the EPS bearer identities of the default bearers are used to differentiate the PDN connections for a given APN, i.e. the MN-ID, the APN and the EPS bearer identity of the default EPS bearer identify the PDN connection. The Serving Gateway shall include the EPS bearer identity of the default EPS bearer if multiple PDN connections per APN are supported in the Proxy Binding Update messages. If the EPS bearer identity is included in a Proxy Binding Update, the PDN GW shall explicitly indicate the support of multiple PDN connections to a given APN. The MME is configured if the Serving GWs in its PLMN support multiple PDN connections to the same APN over PMIP based S5/S8. If the Serving GW does not support multiple PDN connections to the same APN and the UE requests a PDN connection for an APN for which the UE already has an active PDN connection, the MME shall reject the PDN connectivity request. If the PDN GW does not support multiple PDN connections for a given APN, and the Serving GW supports multiple PDN connections to the same APN and the UE requests a PDN connection for an APN for which the UE already has an active PDN connection, the Serving GW shall reject the PDN connectivity request.

The procedure is also used for the re-establishment of existing PDN connectivity after the UE performed the handover from non-3GPP accesses for the first PDN connection by the Attach procedure. The UE triggers the re-establishment of existing PDN connectivity after the handover by providing a Request Type indicating "Handover" as specified in TS 23.401 [4].

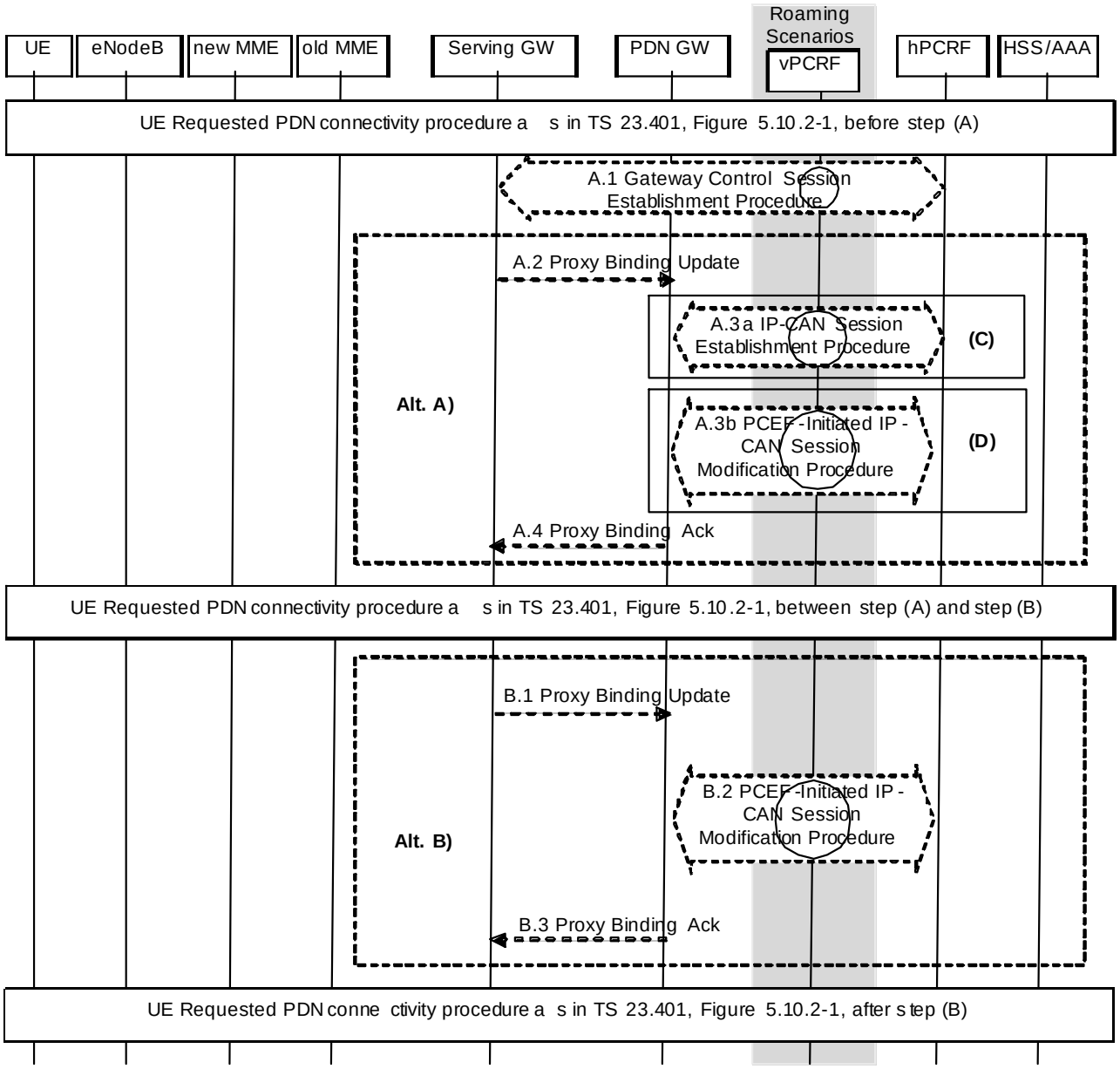


Figure 5.6.1-1: UE requested PDN connectivity with PMIP-based S5 or S8

This procedure applies to the Non-Roaming (Figure 4.2.1-1), Roaming (Figure 4.2.1-2) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the Serving GW and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF.

The optional interaction steps between the gateways and the PCRF in the procedures in figure 5.6.1-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

For UE request additional PDN connectivity to PDNs when connected to 3GPP access network with PMIP-based S5 or S8, the IP address is not available after step A1, steps in (Alt A) are performed after step A.1, excluding steps in (Alt B). The step in (C) is performed only when the UE establishes additional PDN connectivity with a PDN it is not already connected to, excluding step (D).

For re-establishment of existing PDN connectivity after the UE performed the handover from non-3GPP accesses, the steps shown in (Alt A) and (Alt B) are mutually exclusive in this procedure, i.e. either steps A.2-A.4 are executed or steps B.1-B.3. In order to execute the alternative (Alt B), the IP address of the UE needs to be available after step A.1. The IP Address(es) of the UE is received in step A.1, if dynamic policy provisioning is deployed. If multiple PDN connections to same APN are supported by the Serving GW, (Alt A) shall be used in this procedure.

In case the IP address(es) of the UE is available after step A.1, (Alt B) provides lower jitter for dual radio handovers. In case the IP address(es) of the UE is not available after step A.1, (Alt A) shall be used.

For re-establishment of existing PDN connectivity after the UE performed the handover from non-3GPP accesses, the following also applies:

- In step A.2/B.1 the Serving GW sets the Handover Indicator to indicate handoff between two different interfaces of the UE.
- The step in (D) and step B.2 are performed only when the UE re-establishes PDN connectivity after a handover. The steps in (D) correspond to the PCEF-Initiated IP-CAN Session Modification procedure specified in TS 23.203 [19].
- In step A.4/B.3, the UE Address Info shall contain the IP address the UE obtained during PDN connectivity establishment for this PDN over the non-3GPP access. The PDN GW also includes the Charging ID for the PDN connection in the Proxy binding acknowledgement. For the case of additional PDN connectivity with a PDN, the PDN-GW generates a Charging Id for the PDN connection. For the case of re-establishment of existing PDN connectivity after the UE performed a handover from non-3GPP access, the PDN GW reuses the Charging Id previously assigned to the PDN connection if the source access is a PMIP-based access or to the Default Bearer if the source access is GTP-based.

The steps A.1-A.4 correspond to steps C.1-C.4 in Figure 5.2-1.

The steps B.1-B.3 correspond to steps A.2, A.3b, A.4 in Figure 5.6.1-1.

5.6.2 PDN Disconnection

5.6.2.1 UE, MME or S-GW initiated PDN Disconnection

When GTP-based S5 or S8 is used the procedure described in clause 5.10.3 of TS 23.401 [4] applies for the UE or MME initiated PDN disconnection. The PMIP variant of this procedure is specified below. In addition, if the default bearer belonging to a PDN connection is to be deactivated by the S-GW, e.g. due to un-successful modification of QoS of default bearer that was triggered by PCRF interaction, the S-GW deactivates all bearers belonging to the PDN connection using the following procedure.

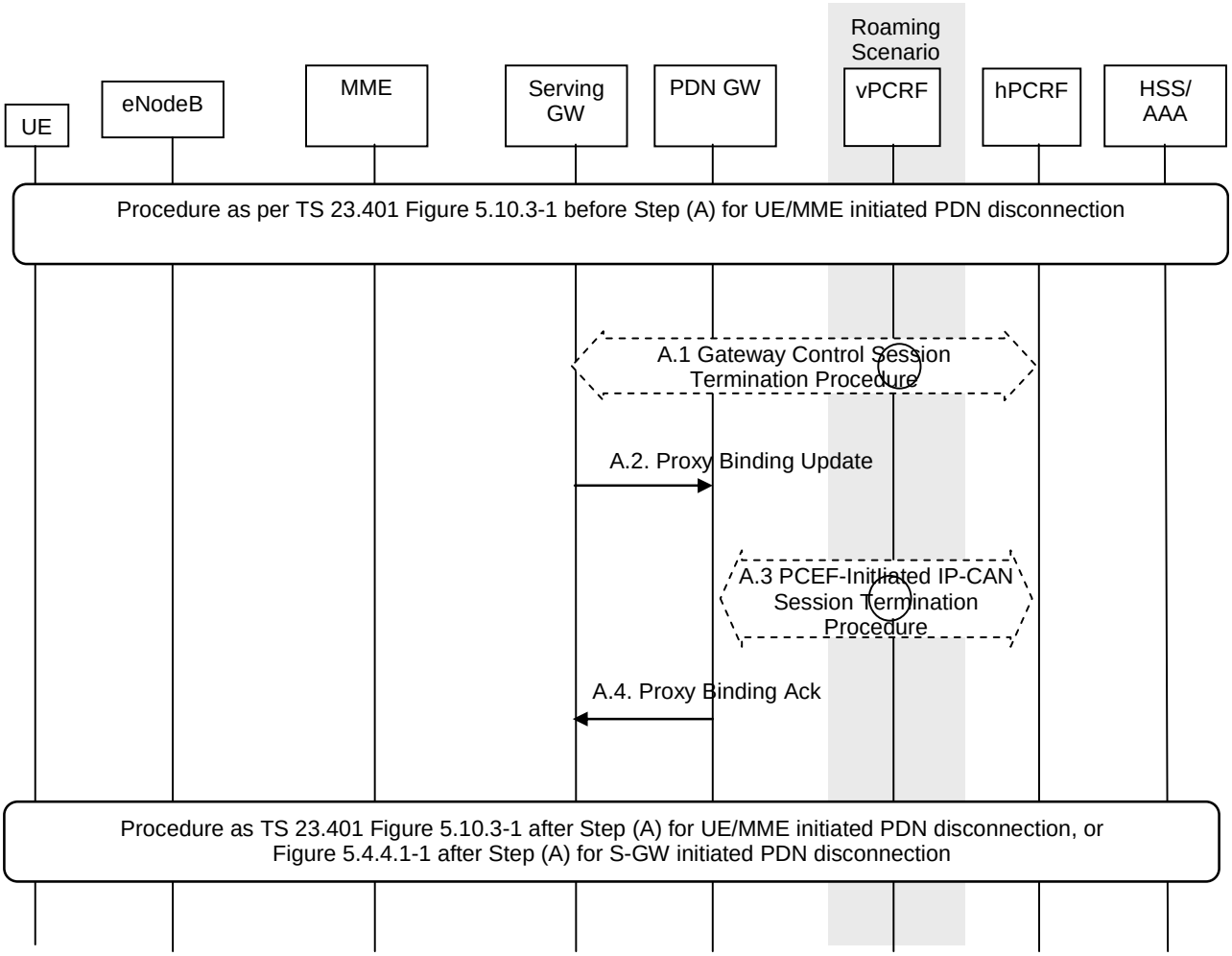


Figure 5.6.2-1: UE, MME or S-GW initiated PDN disconnection Procedure for PMIP-based S5/S8

Steps A.1 to A.4 are described in clause 5.3. For the case of S-GW initiated PDN disconnection, which corresponds to PDN GW initiated bearer deactivation procedure of clause 5.4.4.1 of TS 23.401 [4], the procedure starts from step A.1 and there are no steps corresponding to box (B) of figure 5.4.4.1-1 of TS 23.401 [4].

5.6.2.2 PDN-GW-initiated PDN Disconnection

The default bearer and all the dedicated resource allocations associated with the PDN address are released in this procedure.

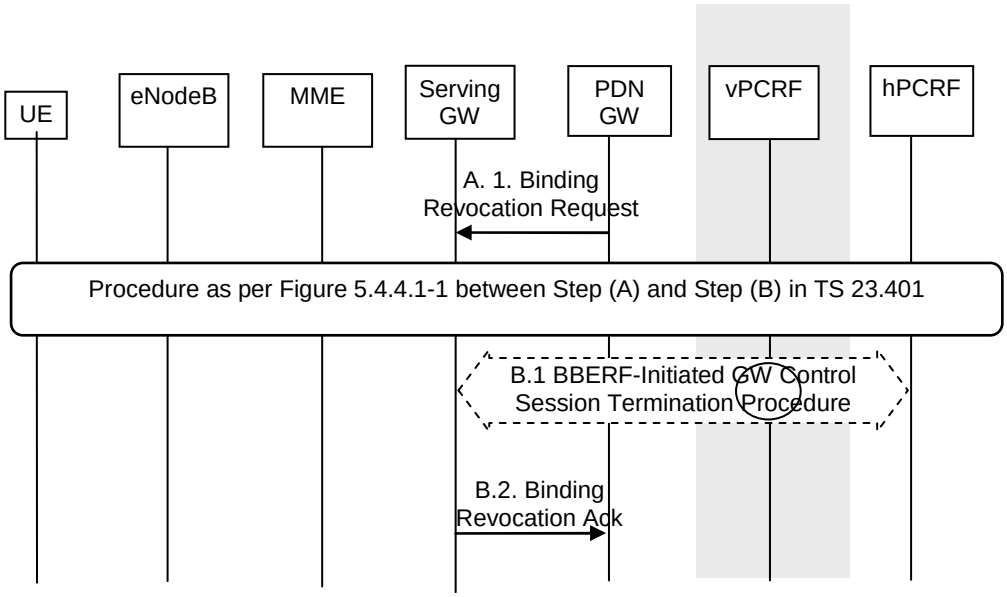


Figure 5.6.2.2-1: PDN GW initiated PDN Disconnection Procedure for PMIP-based S5/S8

This procedure applies to the Non-Roaming (Figure 4.2.1-1), Roaming (Figure 4.2.1-2) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the Serving GW and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF.

The optional interaction steps between the gateways and the PCRF in the procedures in figure 5.6.2.2-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

A.1. The PDN GW sends a Binding Revocation Indication (PDN address) message to the Serving GW.

Steps between A and B are described in clause 5.4.4.1 of TS 23.401 [4], using the indication that all bearers belonging to the given PDN address shall be released.

B.1. The Serving GW initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [19]. The S-GW provides the information to enable the PCRF to uniquely identify the IP-CAN session and indicates User Location Information and/or UE Time Zone Information to the PCRF as an Event Report if the corresponding event trigger is set. This results in the removal of the Gateway Control session in S-GW.

B.2. The Serving GW returns a Binding Revocation Acknowledgement message to the PDN GW.

NOTE: Step B.2 may occur before steps B.1 since the Serving GW need not wait for terminating the GW Control Session with the PCRF before acknowledging the Binding Revocation.

5.7 Handover and Tracking area Update Procedures for PMIP-based S5/S8 Interface

5.7.0 Intra-LTE TAU and Inter-eNodeB Handover without Serving GW Relocation

This clause contains the procedure steps that vary between the GTP and PMIP variant of S5 and S8 for the TAU with MME without Serving GW change procedure defined in TS 23.401 [4], clause 5.3.3.2 as well as Inter-eNodeB Handover without Servig GW change procedures as described in TS 23.401 [4], clauses 5.5.1.1.2 and 5.5.1.2.2.

The procedure is shown in Figure 5.7.2-1. The parameters to be provided to the PGW, as described in TS 23.401 [4], are sent by the Serving GW via the PCRF to the PGW.

5.7.1 Intra-LTE TAU and Inter-eNodeB Handover with Serving GW Relocation

This clause contains the procedure steps that vary between the GTP and PMIP variant of S5 and S8 for the TAU with MME and Serving GW change procedure defined in TS 23.401 [4], clause 5.3.3.1 as well as Inter-eNodeB Handover with CN Node Relocation described in TS 23.401 [4], clause 5.5.1.2.

In case of a Serving GW relocation, the target Serving GW must establish a Gateway Control Session with the PCRF to perform policy controlled functions such as Bearer-Binding. The source Serving GW relinquishes its Gateway Control Session with the PCRF in step B.

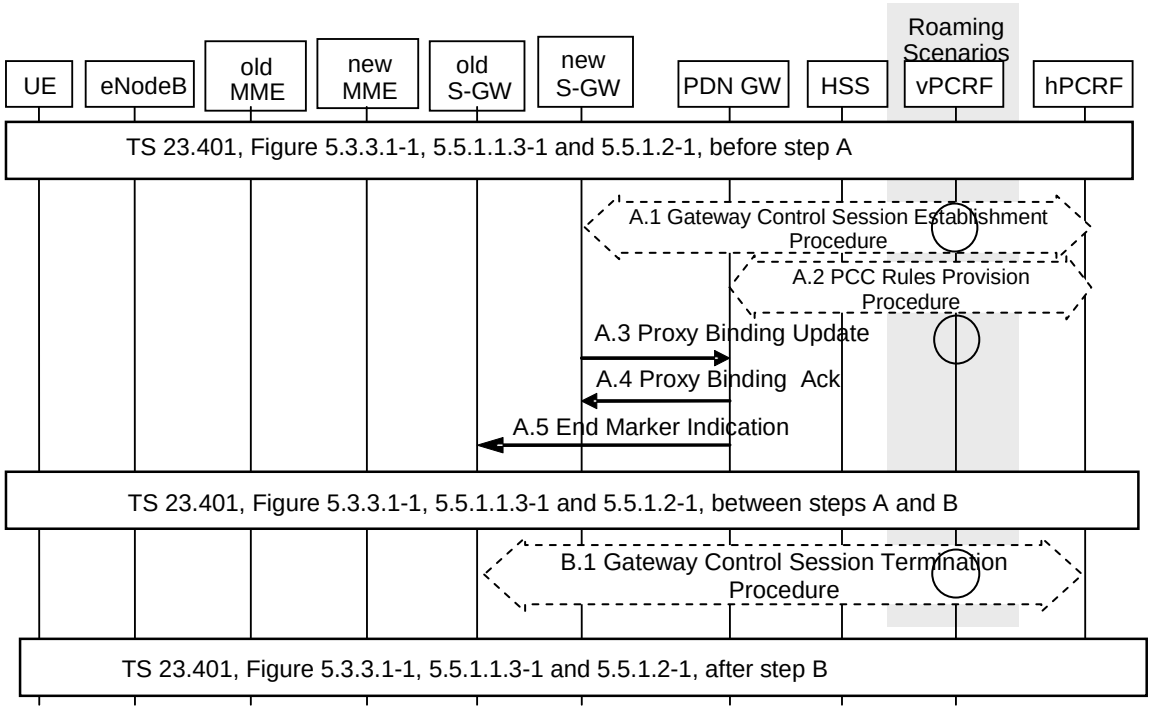


Figure 5.7.1-1: Intra-LTE and Inter-eNodeB Handover with Serving GW Relocation

This procedure concerns both the non-roaming (S5) as in Figure 4.2.1-1 and roaming case (S8) as in Figure 4.2.1-2. In the roaming case, the vPCRF in the VPLMN forwards messages between the Serving GW and the hPCRF in the HPLMN. In the case of Local Breakout as in Figure 4.2.3-4, the vPCRF also forwards messages sent between the PDN GW and the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

The optional interaction steps between the gateways and the PCRF in the procedures in Figure 5.7.1-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

A.1) The Target Serving GW initiates the Gateway Control Session Establishment Procedure with the PCRF as specified in TS 23.203 [19]. As part of the procedure the Serving GW informs the PCRF of the RAT type, UE Location Information IE and the user CSG information, if available. The PCRF sends information to the Serving GW enabling bearer binding and other behaviour. The Target Serving GW checks whether the QoS rules provided by the PCRF aligns with the TFT and Bearer Level QoS of the EPS bearer contexts. If there is a mismatch, the Target Serving GW initiates appropriate EPS bearer procedures.

NOTE 1: The Target Serving GW preserves the Bearer Binding that have already been established by the Source Serving GW. To enable this the EPS Bearer ID, TFT is transferred before Step A as follows: across S10 in Forward Relocation Request and across S11 in Create Session Request. The Event Triggers indicate to the Serving GW under what conditions to report events to the PCRF.

NOTE 2: The PCRF provides to the Target Serving GW the QoS rules which were active at the Source Serving GW before the handover. Any change of the QoS rules is performed via an additional QoS Rule Provision Procedure after the handover.

A.2) The PCRF may update the PCC rules at the PDN GW by initiating the PCC Rules Provision Procedure as specified in TS 23.203 [19]. The PCRF also notifies the PDN GW of the UE Location Information IE and user CSG information (if this has been received from the Serving GW preceding step A.1).

A.3) The new Serving GW performs a PMIPv6 Proxy Binding Update (MN NAI, Lifetime, Access Technology Type option, APN, GRE key for downlink traffic, *Additional Parameters*) message in order to re-establish the user plane as a result of the Serving GW relocation. The MN NAI identifies the UE for whom the message is being sent. Within Access Technology Type option an indication for RAT (E-UTRAN) type is set; an indication for handover between MAGs for the same interface is also set. If multiple PDN connections for the given APN are supported by the Serving GW then the APN and the EPS bearer identity of the default bearer disambiguates which PDN connection this message refers to, otherwise the APN itself identifies the PDN connection of the UE. The additional parameters may include protocol configuration options and other information.

A.4) The PDN GW acknowledges the Binding Update by sending a Proxy Binding Ack (MN NAI, Lifetime, UE Address Info, GRE key for uplink traffic, Charging ID, *Additional Parameters*) message to the Serving GW. If the EPS bearer identity is included in the Proxy Binding Update, the PDN GW shall acknowledge if multiple PDN connections to the given APN are supported. A PMIP tunnel is established at this point between the PDN GW and the Serving GW. The UE Address Info includes one or more IP addresses. The Additional Parameters may contain protocol configuration options and other information. The Charging Id provided is the Charging Id previously assigned to the PDN connection.

A.5) If the Serving GW is relocated, the PDN GW shall send End Marker Indication message to the source SGW immediately after switching the path. If the source Serving GW has downlink user plane established, the source Serving GW shall send one or more "end marker" packets to the source eNodeB immediately after receiving this indication in order to assist the reordering function in the target eNodeB. Otherwise the souce Serving GW shall ignore the message and shall not send Downlink Data Notification.

Editor's note: The protocol detail of "End Marker Indication" is FFS and is to be studied in CT WG4.

NOTE 3: The Serving GW learns from the PBA whether the PDN GW supports multiple PDN connections to the same APN or not.

Steps between A.4 and B.1 are described in TS 23.401 [4], clauses 5.3.3.1 and 5.5.1.

B.1) The old Serving GW initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [19]. The Serving GW ceases to perform Bearer Binding and associated policy controlled functions.

Procedures on the MME for X2 and S1 handover are described in clause 5.5 of TS 23.401 [4]. If the MME receives a rejection to an S1 interface procedure (e.g. EPS bearer(s) request) from the eNodeB with an indication that an X2/S1 handover is in progress and if during the handover procedure the MME detects that the Serving GW or/and the MME needs be relocated, the MME rejects any EPS bearer(s) request received since handover procedure started and includes an indication that the request has been temporarily rejected due to handover procedure in progress.

For PMIP based S5/S8, if dynamic PCC is deployed and with Serving GW relocation, when the Source Serving GW receives an indication from the MME that the PCRF initiated dedicated bearer procedure was temporarily rejected due to handover, the Source Serving GW starts a locally configured guard timer. The Source Serving GW shall re-attempt, up to a pre-configured number of times, at expiry of the guard timer or abort the procedure if it determines that Serving GW is relocated based on receiving the Delete Session request message from the MME.

5.7.2 TAU/RAU or Handover between GERAN A/Gb Mode or UTRAN Iu Mode and E-UTRAN

In case of inter-RAT TAU/RAU or handovers, the Serving GW may or may not be relocated. The PMIP based S5/S8 variants procedure steps for inter-RAT TAU/RAU or handover without Serving GW relocation are shown in Figure 5.7.2-1 and those corresponding to a change of Serving GW are shown in Figure 5.7.2-2.

The procedures in this clause correspond to the following Figures in TS 23.401 [4]:

- Figure 5.3.3.2-1 [UTRAN Iu mode to E-UTRAN] Tracking Area Update.
- Figure 5.3.3.3-1E-UTRAN to UTRAN/GERAN RA Update.
- Figure 5.3.3.6-1 E-UTRAN to GERAN A/Gb mode Routeing Area Update.

- Figure 5.5.2.1.3-1: E-UTRAN to UTRAN Iu mode Inter RAT HO, execution phase.
- Figure 5.5.2.2.3-1: UTRAN Iu mode to E-UTRAN Inter RAT HO, execution phase.
- Figure 5.5.2.3.3-1: E-UTRAN to GERAN A/Gb mode Inter RAT HO, execution phase.
- Figure 5.5.2.4.3-1: GERAN A/Gb mode to E-UTRAN Inter RAT HO, execution phase.

In TS 23.401 [4], the clauses corresponding to Figure 5.7.2-1 and Figure 5.7.2-2 cover both the case of Serving GW relocation and no Serving GW relocation. In case of no Serving GW relocation, Steps (A) in the above figures are between the un-changed Serving GW and the PCRF and the Steps (B) in those figures do not apply, as shown in Figure 5.7.2-1. In case of Serving GW relocation, Steps (A) in the above figure are between the target Serving GW and the PCRF and the Steps (B) is between the source Serving GW and the PCRF, as shown in Figure 5.7.2-2.

In case of no Serving GW relocation, the S-GW signals the change of RAT to the PCRF. In addition, if the Serving GW has received the User Location Information IE or the user CSG information from the MME, this information is also sent to the PCRF. If PCC rules provided to the PDN-GW have changed, the PCRF updates these rules at the PDN-GW. The PCRF sends the RAT Type change or User Location Information and user CSG information, if received from the Serving- GW, to the PDN GW.

The user plane already exists between the Serving GW and the PDN GW and remains unchanged. In case of RAU or handover to 2G/3G, user plane routing is assumed to proceed over the S4 interface towards the S2/S3 SGSN. When an inter-RAT TAU occurs, the enhanced packet core may signal this event to the PDN GW, for example to inform the PDN GW of a RAT type change. In the case of a PMIP-based S5 and S8, a Modify Bearer Request is not sent from the Serving GW to the PDN GW. Instead, the PCRF in the HPLMN reports the change of event. The PCRF signals any change in the policy resulting from the event to the PDN GW, provisioning updated policy and charging rules.

In case dynamic PCC is not deployed, a change of RAT type will not be signalled to the PDN GW using PMIP based S5/S8 interfaces, if no change of Serving GW has occurred.

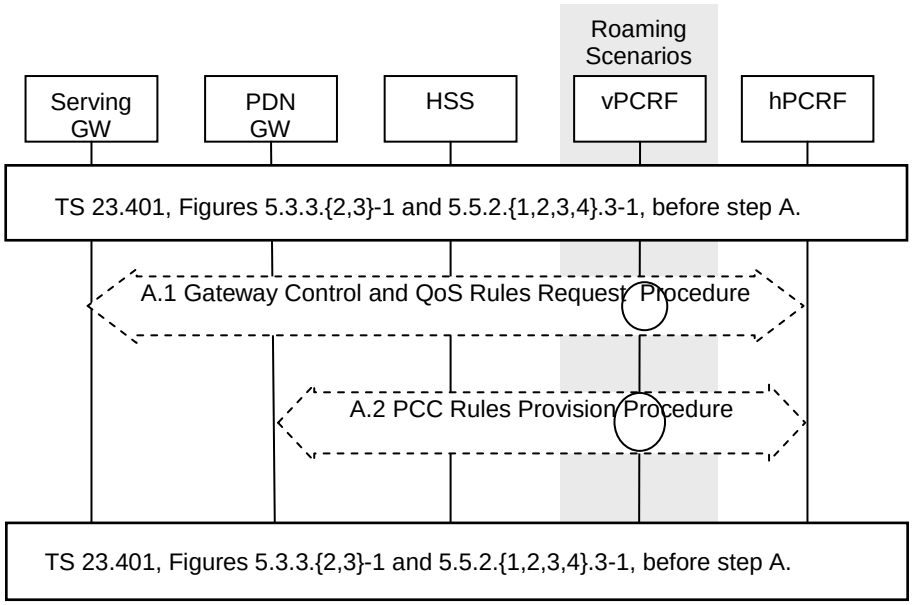


Figure 5.7.2-1: Inter-RAT TAU/RAU or Handover without Serving GW relocation

This procedure applies to the Non-Roaming (Figure 4.2.1-1), Roaming (Figure 4.2.1-2) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the Serving GW and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF.

The optional interaction steps between the gateways and the PCRF in the procedures in Figure 5.7.2-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

A.1) The Serving GW informs the PCRF about the change of RAT type and UE Location Information IE and user CSG information (if this has been received from the MME preceding step A) by initiating the Gateway Control and QoS Policy Rules Request Procedure as specified in TS 23.203 [19].

A.2) The PCRF updates the PCC rules at the PDN GW by initiating the PCC Rules Provision Procedure as specified in TS 23.203 [19] if the PCC rules have changed based on the RAT type reported by the Serving GW in step A.1. Further, the hPCRF notifies the PDN GW of the change in RAT and the UE Location Information IE and user CSG information (if this has been received from the Serving GW preceding step A.1).

Step A.2 may be initiated before A.1 completes.

If dynamic PCC is deployed and during the handover with MME relocation without serving GW relocation, when the Serving GW receives an indication from the MME that the PCRF initiated dedicated bearer procedure was temporarily rejected due to handover, the Serving GW starts a locally configured guard timer. The Serving GW shall re-attempt, up to a pre-configured number of times, when it either detects that the handover is completed or failed using message reception or at expiry of the guard timer.

The following procedure describes inter-RAT TAU/RAU or Handover in the case of Serving Gateway relocation for PMIP-based S5/S8.

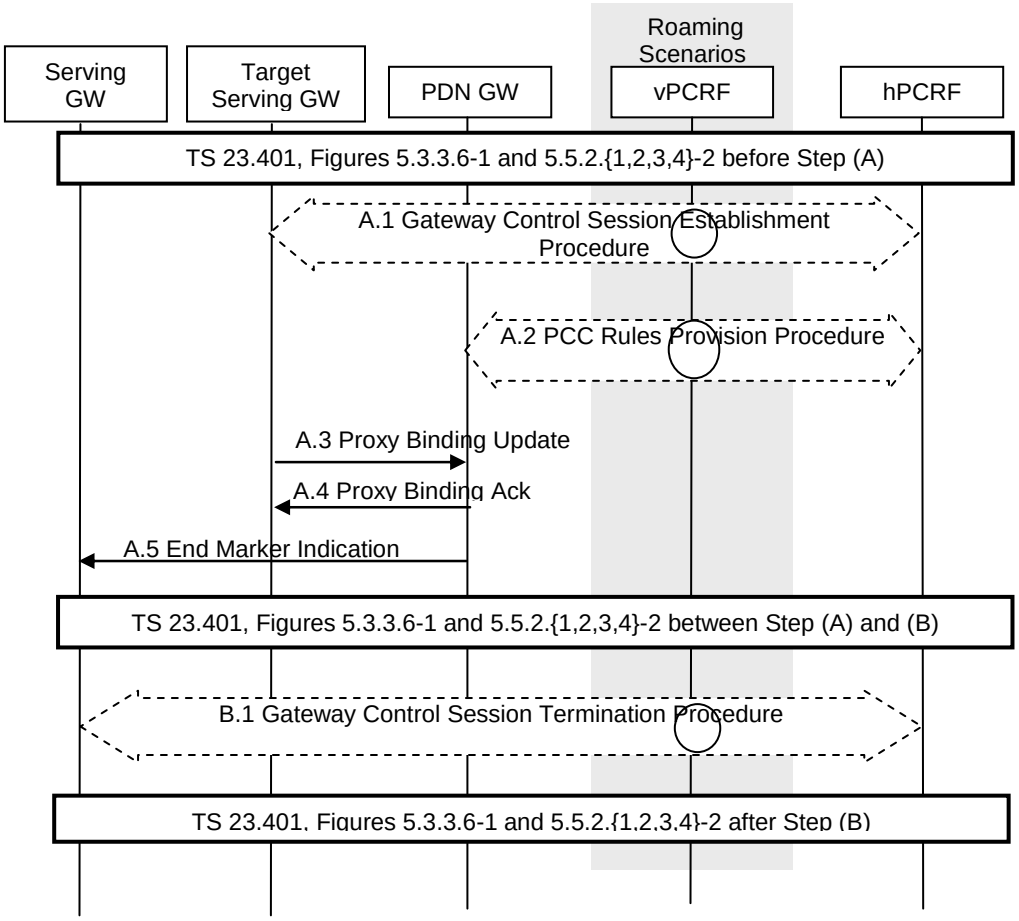


Figure 5.7.2-2: Inter-RAT TAU/RAU or Handover with Serving GW Relocation

This procedure concerns both the non-roaming (S5) as in Figure 4.2.1-1 and roaming case (S8) as in Figure 4.2.1-2. In the roaming case, the vPCRF in the VPLMN forwards messages between the Serving GW and the hPCRF in the HPLMN. In the case of Local Breakout as in Figure 4.2.3-4, the vPCRF forwards messages sent between the PDN GW and the hPCRF as well. In the non-roaming case, the vPCRF is not involved at all.

If dynamic policy provisioning is not deployed, the optional steps in the procedure are not applied.

A.1) The Target Serving Gateway initiates a Gateway Control Session Establishment Procedure with the PCRF, as specified in TS 23.203 [19] and informs the PCRF of the new RAT type, UE Location Information IE and user CSG information (if this has been received from the MME preceding step A). The Target Serving GW checks whether the QoS rules provided by the PCRF aligns with the TFT and Bearer Level QoS of the EPS bearer contexts. If there is a mismatch, the Target Serving GW initiates appropriate EPS bearer procedures.

NOTE 1: The PCRF provides to the Target Serving GW the QoS rules which were active at the Source Serving GW before the handover. Any change of the QoS rules is performed via an additional QoS Rule Provision Procedure after the handover.

A.2) The PCRF sends an updated policy to the PDN GW by initiating the Policy and Charging Rules Provision Procedure as specified in TS 23.203 [19]. This contains any effected PCC rules and Event Triggers resulting from the preceding step that may require enforcement or event reporting to be performed by the PDN GW. The UE Location Information IE and user CSG information are also sent to the PDN GW from the PCRF (if this has been received from the Serving GW preceding step A.1).

A.3) The Target Serving GW sends a Proxy Binding Update (MN NAI, Lifetime, Access Technology Type, APN, GRE key for downlink traffic, *Additional Parameters*) message in order to re-establish the user plane as a result of the Serving GW relocation. The MN NAI identifies the UE for whom the message is being sent. Access Technology Type is set to indicate 3GPP access to EPS; an indication for handover between MAGs for the same interface is also set. If multiple PDN connections for the given APN are supported by the Serving GW then the APN and the EPS bearer identity of the default bearer disambiguates which PDN connection this message refers to, otherwise the APN itself identifies the PDN connection of the UE. The additional parameters may include protocol configuration options and other information.

A.4) The PDN GW acknowledges the Binding Update by sending a Proxy Binding Ack (MN NAI, Lifetime, UE Address Info, GRE key for uplink traffic, Charging ID, *Additional Parameters*) message to the Target Serving GW. If the EPS bearer identity is included in the Proxy Binding Update the PDN GW shall acknowledge if multiple PDN connections to the given APN are supported. A PMIP tunnel is established at this point between the PDN GW and the Target Serving GW. The UE Address Info includes one or more IP addresses. The Additional Parameters may contain protocol configuration options and other information. The Charging Id provided is the Charging Id previously assigned to the PDN connection.

NOTE 2: The Serving GW learns from the PBA whether the PDN GW supports multiple PDN connections to the same APN or not.

A.5) If the Serving GW is relocated, the PDN GW shall send End Marker Indication message to the source SGW immediately after switching the path. If the source Serving GW has downlink user plane established, the source Serving GW shall send one or more "end marker" packets to the source eNodeB or source S4 SGSN immediately after receiving this indication. Otherwise, the source Serving GW shall ignore the message and shall not send Downlink Data Notification.

Editor's note: The protocol detail of "End Marker Indication" is FFS and is to be studied in CT WG4.

Steps between A.4 and B.1 are described in the clauses of TS 23.401 [4], containing the figures referenced in Figure 5.7.2-1 above.

B.1) The old Serving GW initiates the Gateway Control Session Termination Procedure with the PCRF, as specified in TS 23.203 [19]. The S-GW provides information to enable the PCRF to uniquely identify the IP-CAN session. This results in the removal of the Gateway Control session in S-GW.

5.8 ME Identity Check Procedures for PMIP-based S5/S8

ME identity check by the MME in case of PMIP-based S5/S8 is performed as defined for GTP-based S5/S8, see clause 5.3.2.1 (E-UTRAN Initial Attach procedure) of TS 23.401 [4].

No ME identity check support is specified on the S5/S8 reference point.

5.9 UE-triggered Service Request for PMIP-based S5/S8

This clause contains the procedure steps that vary between the GTP and PMIP variant of S5 and S8 for the UE-triggered Service Request procedure defined in TS 23.401 [4], clause 5.3.4.1, for the case where the RAT Type reported in the Service Request has changed compared to the last reported RAT Type.

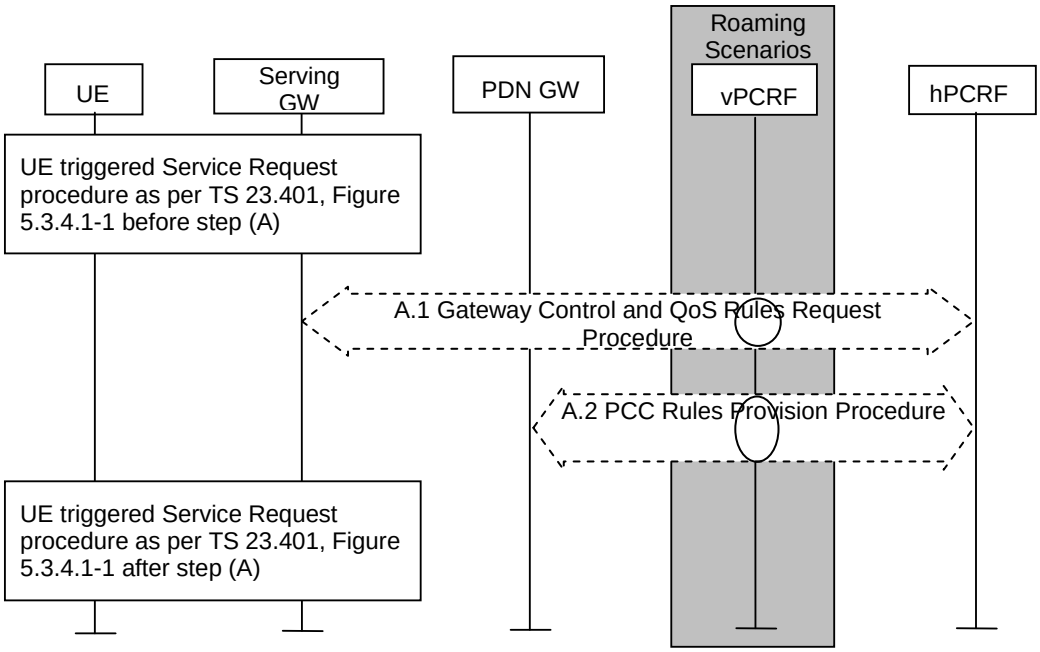


Figure 5.9-1: UE-triggered Service Request for PMIP-based S5/S8

This procedure concerns both the non-roaming (S5) and roaming case (S8). In the roaming case, the vPCRF in the VPLMN forwards messages between the Serving GW and the hPCRF in the HPLMN. In the case of Local Breakout, the vPCRF forwards messages sent between the PDN GW and the hPCRF as well. In the non-roaming case, the vPCRF is not involved at all.

The optional interaction steps between the gateways and the PCRF in the procedures in Figure 5.9-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

A.1) The Serving GW informs the PCRF about the change of RAT type, UE Location Information IE and user CSG information (if this has been received from the MME preceding step A) by initiating the Gateway Control and QoS Policy Rules Request Procedure as specified in TS 23.203 [19].

A.2) The PCRF updates the PCC rules at the PDN GW by initiating the PCC Rules Provision Procedure as specified in TS 23.203 [19] if the PCC rules have changed based on the RAT type reported by the Serving GW in step A.1. The UE Location Information IE and user CSG information are also sent to the PDN GW from the PCRF (if this has been received from the Serving GW preceding step A.1).

Further, the hPCRF notifies the PDN GW of the change in RAT.

Step A.2 may be initiated before step A.1 completes: Once the hPCRF receives the event report from the Serving GW as part of step A.1, the hPCRF may complete step A.1 and initiate step A.2 in any order.

5.10 PMIP-based S5/S8 procedures for GERAN/UTRAN over S4

5.10.1 General

This clause presents the PMIP-based S5/S8 procedures equivalent to the GTP-based procedures presented in TS 23.060 [21] for interworking. The differences required for interpretation of the PMIP-based S5/S8 procedures in other clauses of this specification are clarified below.

If PCC is not deployed, only default bearers may be provided for UE connection to a PDN. This is described fully in the PMIP-based S5/S8 procedures referred to in clause 5.10. Secondary PDP context requests are not supported in this case.

Bearer-specific parameters sent along S4 are not forwarded to the PDN GW or PCRF in many cases. Bearers terminate in the Serving GW when PMIP-based S5/S8 has been deployed. Though EPS bearer identifier information is not relevant to the PCRF or PCEF in these cases, some bearer-oriented parameters must be forwarded to the PCRF for

authorization and so that the PCRF will generate the correct corresponding PCC rules to send to the PDN GW for enforcement.

5.10.2 GPRS procedures that update the PDN GW

Several procedures employing GTP-based S5/S8 includes a "Modify Bearer" exchange, initiated by the Serving GW, responded to by the PDN GW. The equivalent interaction for a PMIP-based S5/S8 is shown in figure 5.7.2-1.

The following procedures in TS 23.060 [21] will make use of the procedure shown in this specification, clause 5.7.2 to signal RAT change as determined by the SGSN. Aside from the new RAT type, no additional parameter must be sent as an event report by the Serving GW to the PDN GW by means of the PCRF (as described in TS 23.203 [19]).

The procedure in clause 5.7.2 refers directly to procedures in TS 23.401 [4], while the procedures described here in support of S4 refer to clauses in TS 23.060 [21]. The following clarifications to the procedure in clause 5.7.2 must be considered to interpret clause 5.7.2:

- **6.9.2.2.1a: Serving RNS Relocation Procedure, Combined Hard Handover and SRNS Relocation Procedure, and Combined Cell/URA Update and SRNS Relocation Procedure using S4**

  Steps A.1 and A.2 of the procedure in clause 5.7.2 occur instead of the steps shown in the box (B1) in TS 23.060 [21], clause 6.9.2.2.1a, figure 39b. The APN AMBR, RAT Type and other parameters defined in clause 6.9.2.2.1a step B and C are transmitted according to clause 5.7.2, as additional IEs transmitted between the S-GW, PCRF and P-GW. IEs are returned to the S-GW (insofar as step A.2 implies a Gateway Control and QoS Rules Provision procedure as described in TS 23.203 [19]).

  This procedure applies also to 6.9.2.2.3 Combined Cell / URA Updates and SRNS Relocation Procedure.

- **6.9.2.2.5A Enhanced Serving RNS Relocation Procedure Using S4**

  Steps A.1 and A.2 of the procedure in clause 5.7.2 occur instead of the steps shown in the box (step B and C) in figure 44b1 and steps B and C in figure 44b2 in TS 23.060 [21], clause 6.9.2.2.5A.

- **6.12.1A: UE Initiated Service Request Procedure Using S4**

  Steps A.1 and A.2 of the procedure in clause 5.7.2 occur instead of the steps shown in the box (B1) in TS 23.060 [21], clause 6.12.1A, figure 50A.

- **6.13.1.1.2: Iu mode to A/Gb mode Intra-SGSN Change using S4**

  Steps A.1 and A.2 of the procedure in clause 5.7.2 occur instead of the steps shown in the box (A1) in TS 23.060 [21], clause 6.13.1.1.2, figure 52-2.

- **6.13.1.2.2: A/Gb mode to Iu mode Intra-SGSN Change using S4**

  Steps A.1 and A.2 of the procedure in clause 5.7.2 occur instead of the steps shown in the box (A1) in TS 23.060 [21], clause 6.13.1.2.2, figure 53-2.

- **6.13.2.1.2: Iu mode to A/Gb mode Inter-SGSN Change using S4**

  Steps A.1 and A.2 of the procedure in clause 5.7.2 occur instead of the steps shown in the box (B1) in TS 23.060 [21], clause 6.13.2.1.2, figure 54-3.

- **6.13.2.2.2: A/Gb mode to Iu mode Inter-SGSN Change using S4**

  Steps A.1 and A.2 of the procedure in clause 5.7.2 occur instead of the steps shown in the box (B1) in TS 23.060 [21], clause 6.13.2.2.2, figure 55-3.

- **8.1.4A Paging response for GPRS Downlink Transfer with no established User plane on S4**

  Steps A.1 and A.2 of the procedure in clause 5.7.2 occur instead of the steps shown in the box (C) in TS 23.060 [21], clause 8.1.4, figure 56b.

5.10.3 UE allocated resources

The UE (or the SGSN on behalf of the UE) requests resources in several procedures in TS 23.060 [21]. The procedure described in clause 5.5 of this specification provides the PMIP-based S5/S8 describes UE-initiated resource request, modification and release. This procedure, with the additional clarification given below, will support the following procedures shown in TS 23.060 [21].

In each case, the SGSN provides a Bearer identifier (the LBI) over S4. The bearer binding performed by the Serving GW is in this case constrained to either reject or modify (increase or decrease the resource assigned to) the indicated bearer. The Serving GW shall not provide a different bearer as a result of the PDP Context Activation or Modification procedures.

- **9.2.2.1A: A PDP Context Activation using S4**

  Steps A.1 to A.4 of the procedure in clause 5.6.1 occur instead of the steps shown in the box (A1) in TS 23.060 [21], clause 9.2.2.1A, figure 64a. Step A.1 and A.3a include the RAT Type, Default Bearer QoS and APN-AMBR IEs, and other IEs defined in TS 23.060 [21] clause 9.2.2.1A, step B.

  Step A.3b in clause 5.6.1 of this specification (insofar as it implies a Gateway Control and QoS Rules Provision procedure as described in TS 23.203 [19]) returns the IEs to the S-GW, including EPS Bearer QoS and other IEs defined in TS 23.060 [21] clause 9.2.2.1A, step C.

NOTE: As described in TS 23.060 [21], an S4-based SGSN applies the BCM 'MS/NW' whenever the S4 is selected for a certain MS. The Serving GW is not aware of the BCM.

  If the UE requests a PDP context (effectively an additional PDN connection) for an APN for which the UE already has an active PDN connection, the SGSN shall reject the PDN connectivity request unless it is configured that the Serving GW supports multiple PDN connections to the same APN.

- **9.2.2.1.1A, Figure 66a: Secondary PDP Context Activation Procedure, PDP Creation Part using S4**

  Step A.1 of the procedure in clause 5.5 corresponds to the steps described in the box (A1) and (A2) in TS 23.060 [21], clause 9.2.2.1.1A, figure 66a.

  In step A.1, additional IEs are required by the PCRF and PDN GW in order properly assign QoS rules and prepare the dedicated bearer. The TFT and EPS Bearer QoS (excluding ARP) IEs are received from the SGSN by the S-GW over S4. These parameters are then forward to the PCRF as described in clause 5.5.

- **9.2.3.3A: MS-Initiated EPS Bearer Modification Procedure using S4, Request Part**

  The procedure step in TS 23.060 [21], clause 9.2.3.3A, figure 72c, step B corresponds with step A.1 of figure 5.5-1 (of this specification).

  The Serving GW provides the same information to the PCRF as the PDN GW provides according to step B in TS 23.060 [21], clause 9.2.3.3A; this clause defines the IEs included in step A.1 of clause 5.5.

- **9.2.3.3B: MS-Initiated EPS Bearer Modification Procedure using S4, Execution Part**

  The procedure step in TS 23.060 [21], clause 9.2.3.3B, figure 72d, step A corresponds with step A.1 of figure 5.5-1 (of this specification). The following information elements may be sent, depending on the scenario, see TS 23.060 [21], clause 9.2.3.3B:

- **9.2.3.3C MS-Initiated EPS Bearer Modification Procedure using S4, Response Part**

  The procedure step in TS 23.060 [21], clause 9.2.3.3A, figure 72c, step C corresponds with step figure 5.5-1 (of this specification), steps B.1 and B.2, with one difference - before step B.1, step A of the procedure in TS 23.060 [21], clause 9.2.3.3C occurs. The Serving GW indicates to the PCRF the result of the resource allocation. This may result in additional interaction with the PDN GW (see TS 23.203 [19]).

5.10.4 Network allocated resources

Network entities may request resources by means of off-path signalling to support PMIP-based S5/S8. This is defined in clause 5.4.1. All IEs present in messages sent in the replaced 'boxes' in procedures in the following list are sent instead using messages described in this specification. The following procedures in TS 23.060 [21] employ this procedure:

- **9.2.2.3A: Network Requested PDP Context Activation Procedure using S4**

  Step A.1 of the procedure in clause 5.4.1 occurs instead of the steps shown in the box (A1) in TS 23.060 [21], clause 9.2.2.3A, Figure 69c. Steps B.1 and B.2 of the procedure in clause 5.4.1 correspond to the box (B1).

- **9.2.3.1A: SGSN-Initiated EPS Bearer Modification Procedure, Request Part**

  Step A.1 of clause 5.5 occurs instead of the steps inside box (A1) in TS 23.060 [21], clause 9.2.3.1A, figure 70c. Figure 5.5-1 refers to TS 23.401 [4] yet the procedure applies to the SGSN-Initiated EPS Bearer Modification Procedure using S4 as well.

- **9.2.3.1B: SGSN-Initiated EPS Bearer Modification Procedure, Response Part**

  Steps B.1 and B.2 of clause 5.5 occurs instead of the steps inside box (B1) in TS 23.060 [21], clause 9.2.3.1B, figure 70d. Figure 5.5-1 refers to TS 23.401 [4] yet the procedure applies to the SGSN-Initiated EPS Bearer Modification Procedure using S4 as well.

- **9.2.3.2A: PDN GW-Initiated EPS Bearer Modification Procedure**

  Step A.1 of the procedure in clause 5.4.1 occurs instead of the steps shown in the box (A1) in TS 23.060 [21], clause 9.2.3.2A, Figure 71c.

  Steps B.1 and B.2 of the procedure in clause 5.4.1 correspond to the box (A2). Step B.1 indicates whether the resource allocation was successful. This may result in additional interaction with the PDN GW (refer to TS 23.203 [19]).

5.10.5 UE released resources

The UE may release dedicated resources by means of off-path signalling to support PMIP-based S5/S8 deployments, as shown in clause 5.5.

- **9.2.4.1A.1: MS-and SGSN Initiated PDN connection Deactivation Procedure using S4**

  Steps A.1 to A.4 of the procedure in clause 5.6.2.1 "UE, MME or S GW initiated PDN Disconnection" occur instead of steps shown in the box (A1) in TS 23.060 [21], clause 9.2.4.1A.1, figure 74a.

- **9.2.4.1A.2: MS- and SGSN Initiated Bearer Deactivation using S4**

  Steps A.1, B.1 and B.2 of the procedure in clause 5.5 "UE-initiated Resource Request and Release" procedure occur instead of the steps shown in the box (A1) in TS 23.060 [21], clause 9.2.4.1A.2, figure 74b.

5.10.6 PDN GW released resources

The PDN GW may release resources by means of off-path signalling to support PMIP-based S5/S8 deployments as shown in clause 5.4.1. The following procedures in TS 23.060 [21] employ this procedure:

- **9.2.4.3A: PDN GW-Initiated PDP Context Deactivation Procedure using S4**

  Step A.1 in clause 5.4.1 corresponds to the steps shown in box (A1) of TS 23.060 [21], clause 9.2.4.3A, figure 77a.

- **9.2.4.3B: PDN GW-Initiated PDP Context Deactivation Procedure using S4**

  Steps B.1 and B.2 in clause 5.4.1 correspond to the steps in the box (B1) in TS 23.060 [21], clause 9.2.4.3B, figure 77b.

5.10.7 Attach

The GPRS Attach Procedure is supported by the following PMIP-based S5/S8 procedures:

Clause 5.3 is employed instead of box (A) in TS 23.060 [21], clause 6.5.3A, figure 22A. clause 5.3 is also used instead of box (B) in TS 23.060 [21], clause 6.5.3B, figure 22B.

5.10.8 Detach interaction using S4

The MS-, SGSN- and HLR-initiated GPRS detach procedures are supported by the following equivalent PMIP-based S5/S8 procedure:

Clause 5.3 is employed instead of the gray box (A1) in TS 23.060 [21], clause 6.6.3, Figure 25A.

5.10.9 Interaction with CGI/SAI reporting using S4

In the Interaction with CGI / SAI reporting using S4 Procedure as depicted in Figure 15.1.3-3 of TS 23.060 [21], if CGI or SAI changes are considered relevant to charging, a change notification is sent to the PDN GW. There is no response to this report. This corresponds to a Location change (CGI/SAI) event report provided to the PCRF by means of a Gateway Control and QoS Rules Request, as defined in TS 23.203 [19]. This procedure ensures that the event is reported to the PDN GW as well.

5.10.10 RAU Procedure Support

RAU procedures in TS 23.060 [21] send messages from the S4 SGSN to the S-GW and thence to P-GW using GTPv2. For PMIP-based S5/S8, these exchanges occur via PCC.

TS 23.203 [19], figure 7.7.3-1 "Gateway Control and QoS Rules Request", depicts the procedure. The BBERF(S-GW) sends a Gateway Control and QoS Rules Request message to the PCRF including the APN-AMBR. The PCRF sends a PCC Rules Provision message to the PDN GW including the APN-AMBR. The PDN GW responds with an Acknowledge Policy and Charging Rules Provisioning message with the APN-AMBR to the PCRF. The PCRF responds to the BBERF(S-GW) with a Gateway Control and QoS Rules Reply message with the APN-AMBR parameter. The response from the PCRF to the BBERF to the initial Gateway Control and QoS Rules Request message must wait (synchronously) for the completion of the PCC Rules Provision exchange between the PCRF and PCEF.

- **6.9.1.2.2a: Inter SGSN Routeing Area Update and Combined Inter SGSN RA / LA Update using S4**

  Instead of the steps shown in the box (B1) in TS 23.060 [21], clause 6.9.1.2.2a, figure 33b, the procedure described above is employed.

- **6.9.2.1a: Routeing Area Update Procedure using S4**

  Instead of the steps shown in the box (B1) in TS 23.060 [21], clause 6.9.2.1a, figure 36b, the procedure described above is employed.

5.11 PDN GW initiated IPv4 address Delete Procedure

This procedure is initiated by the PDN GW when the UE releases the IPv4 address using DHCPv4 procedure or the lease for the IP address has expired. The procedure is used to delete the IPv4 address from the PDN connection context.

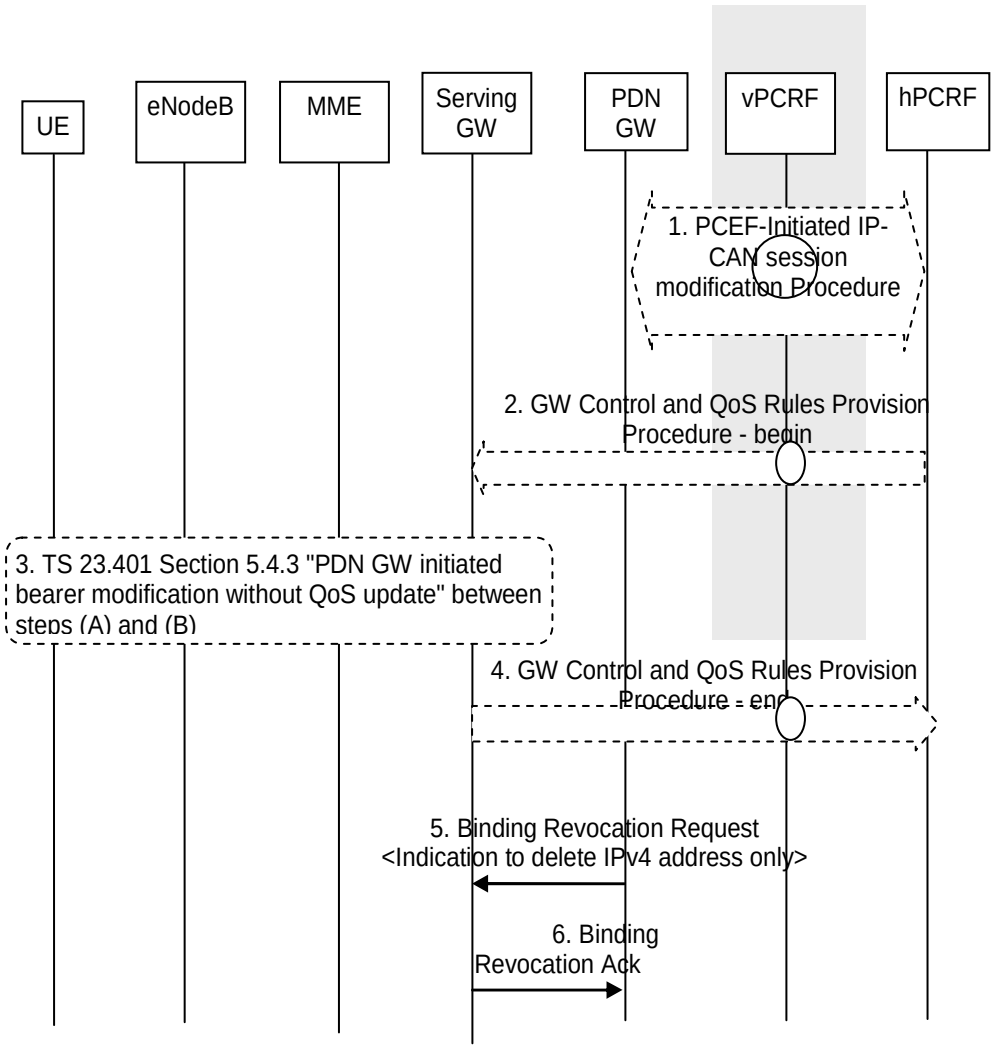


Figure 5.11-1: PDN GW initiated IPv4 address Delete Procedure

This procedure applies to the Non-Roaming (Figure 4.2.1-1), Roaming (Figure 4.2.1-2) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the Serving GW and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF.

The optional interaction steps between the gateways and the PCRF in the procedures in figure 5.11-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

1. The PCEF initiates the Gateway Control Session Modification Procedure with the PCRF as specified in TS 23.203 [19]. The PDN GW provides the information to enable the PCRF to uniquely identify the IP CAN session.

2. In case QoS rules have to be modified, e.g. change of SDF filters, the PCRF initiates a GW Control and QoS rules provision procedure as described in TS 23.203 [19] to inform the S-GW of the updated QoS rules.

3. The S-GW initiates the "PDN GW initiated bearer modification without QoS update" as described in TS 23.401 [4], clause 5.4.3, between steps (A) and (B).

4. The S-GW informs the PCRF of the success of the QoS rules enforcement, thus ending the GW Control and QoS rules provision procedure described in TS 23.203 [19].

5. The PDN GW sends a Binding Revocation Indication (PDN address) message to the Serving GW to revoke the IPv4 address.

6. The Serving GW returns a Binding Revocation Acknowledgement message to the PDN GW.

5.12 Location Change Reporting Procedure for PMIP-based S5/S8

This clause contains the procedure steps that vary between the GTP and PMIP variant of S5 and S8 for the Location Change Reporting procedure provided in clause 5.9.2 of TS 23.401 [4]. If the Serving GW has received the User Location Information IE and/or user CSG information from MME, this event is reported to the PCRF by means of a Gateway Control and QoS Rules Request, as defined in TS 23.203 [19]. This procedure ensures that the event is reported to the PDN GW as well.

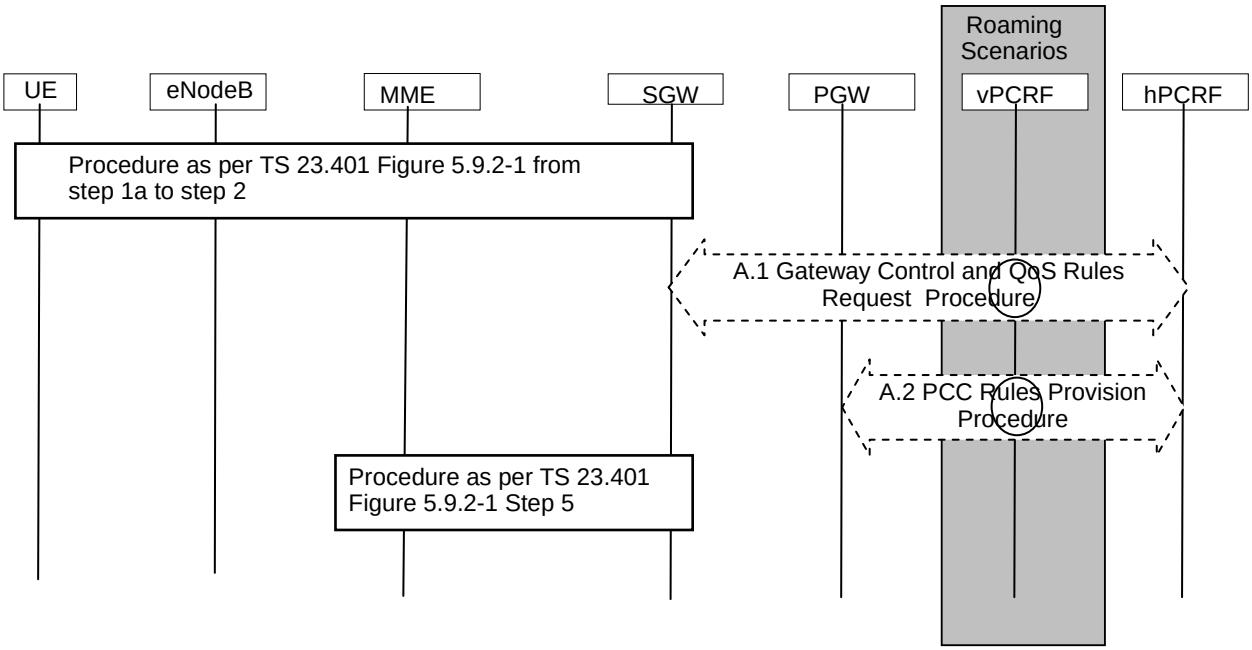


Figure 5.12-1: Notification of the ECGI/TAI information changes

This procedure concerns both the non-roaming (S5) as in Figure 4.2.1-1 and roaming case (S8) as in Figure 4.2.1-2. In the roaming case, the vPCRF in the VPLMN forwards messages between the Serving GW and the hPCRF in the HPLMN. In the case of Local Breakout as in Figure 4.2.3-4, the vPCRF forwards messages sent between the PDN GW and the hPCRF as well. In the non-roaming case, the vPCRF is not involved at all.

The optional interaction steps between the gateways and the PCRF in the procedures in Figure 5.12-1 only occur if dynamic policy provisioning is deployed and the MME has been requested to report the User Location Information IE and/or user CSG information changes to the PGW for the UE.

A.1) The Serving GW informs the PCRF about the change User Location Information IE and/or user CSG information by initiating the Gateway Control and QoS Policy Rules Request Procedure as specified in TS 23.203 [19].

A.2) The hPCRF notifies the PDN GW of the UE Location Information IE and/or user CSG information by initiating the PCC Rules Provision Procedure as specified in TS 23.203 [19]

Step A.2 may be initiated before step A.1 completes.

5.13 Support for Machine Type Communications (MTC)

5.13.1 General

Support for Machine Type Communications (MTC) is described in TS 23.401 [4]. The common procedures and functionalities are only captured in TS 23.401 [4].

5.13.2 PDN GW control of overload

The PDN GW may provide mechanisms for avoiding and handling overload situations. These include the rejection of PDN connection requests from UEs.

When PMIP is used for S5/S8 interface, PDN GW may reject the PDN connection request (i.e. Proxy Binding Update) with indication that the APN is congested. In addition the PDN GW may indicate a "PDN-GW back-off time" for a specific APN to the MME in the reject message.

Other PDN GW functionalities and the behaviour of Serving GW/MME/SGSN upon receiving the reject messages are described in TS 23.401 [4].

5.13.3 Usage of low access priority indicator

For PDN connection establishment requests, the SGSN/MME includes the low access priority indicator in the request message to the Serving GW/PDN Gateway. The Serving GW shall forward the indicator to PDN GW in Proxy Binding Update message.

Other functions related to indicators are described in TS 23.401 [4].

6 Functional Description and Procedures for Trusted Non-3GPP IP Accesses

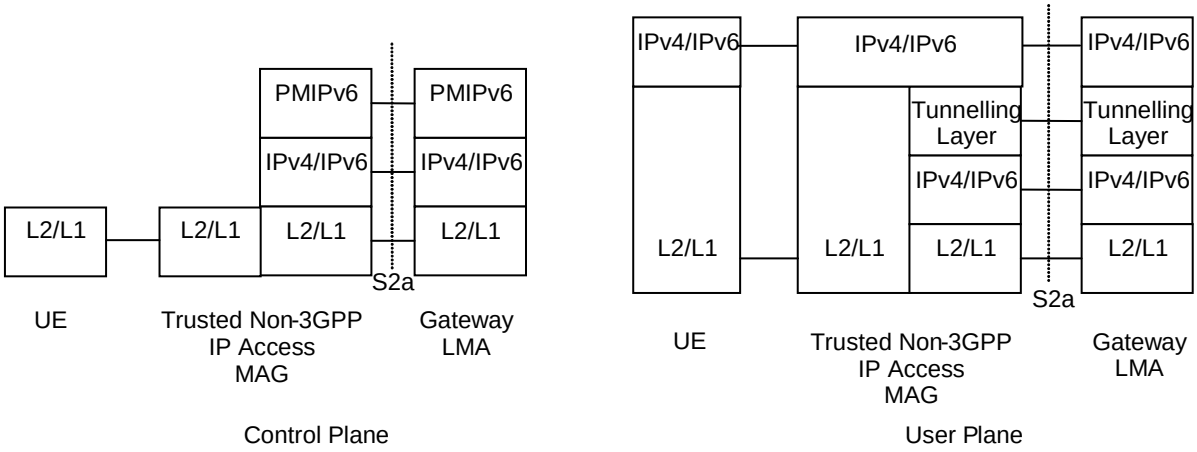
6.1 Control and User Plane Protocol Stacks

6.1.1 Protocol Stacks for S2a

The following protocols shall be supported on S2a:

- PMIPv6.
- MIPv4 FA mode.
- GTP based protocol for Trusted WLAN as specified in clause 16.

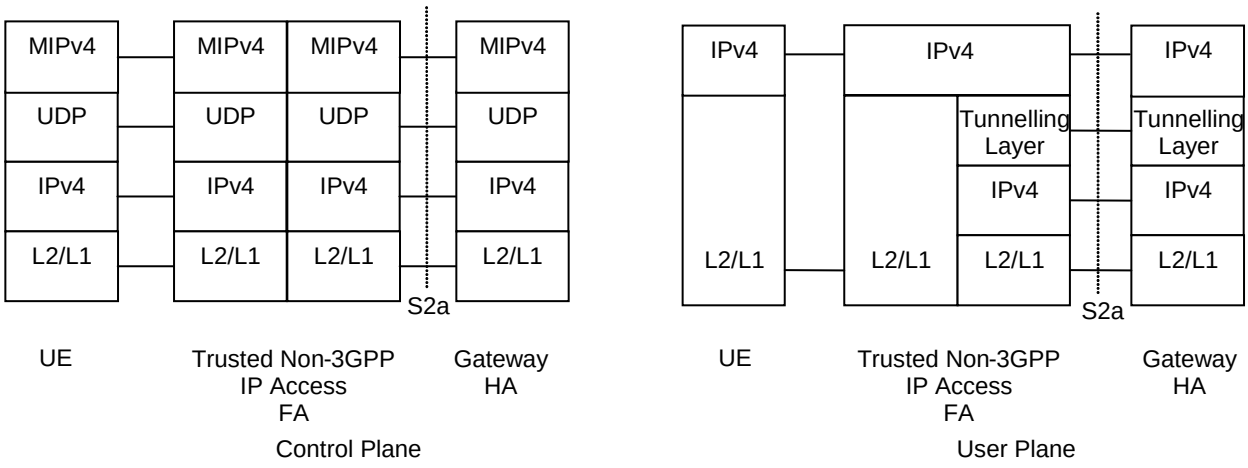
The figures below illustrate the control planes for Mobility Management (MM) and the user planes for each protocol option.



Legend:

- According to terms defined in PMIPv6 specification, RFC 5213 [8], the functional entities terminating both the control and user planes are denoted MAG in the non-3GPP IP access and LMA in the Gateway. LMA includes also the function of a Home Agent.
- The MM control plane stack is PMIPv6 specification, RFC 5213 [8,] over IPv6/IPv4.
- The user plane carries remote IPv4/v6 packets over either an IPv4 or an IPv6 transport network.
- The tunnelling layer implements GRE encapsulation applicable for PMIPv6.
- **IPv4/IPv6:** This refers to network layer protocols. On the Trusted Non-3GPP IP Access MAG this includes termination of the UE-MAG link-local protocols (e.g. IPv6 Router Solicitation/Advertisement) and forwarding of user plane IP packets between the UE-MAG point-to-point logical link and the S2a tunnel for the UE.

Figure 6.1.1-1: Protocols for MM control and user planes of S2a for the PMIPv6 option



Legend:

- According to terms defined in MIPv4 RFC 5944 [12], the functional entities terminating both the control and user planes are denoted MN (Mobile Node) in the UE, FA (Foreign Agent) in the non-3GPP IP access, and HA (Home Agent) in the Gateway.
- The MM control plane stack is MIPv4 RFC 5944 [12] over UDP over IPv4.
- The user plane carries remote IPv4 packets over an IPv4 transport network.
- The tunnelling layer implements IP encapsulation applicable for MIPv4 as defined in RFC 5944 [12]. In some cases the tunnelling layer may be transparent.
- **IPv4:** This refers to network layer protocols. On the Trusted Non-3GPP IP Access FA user plane this includes termination of the UE-FA link-local protocols (e.g. ARP messages) and forwarding of user plane IP packets between the UE-FA point-to-point logical link and the S2a tunnel for the UE.

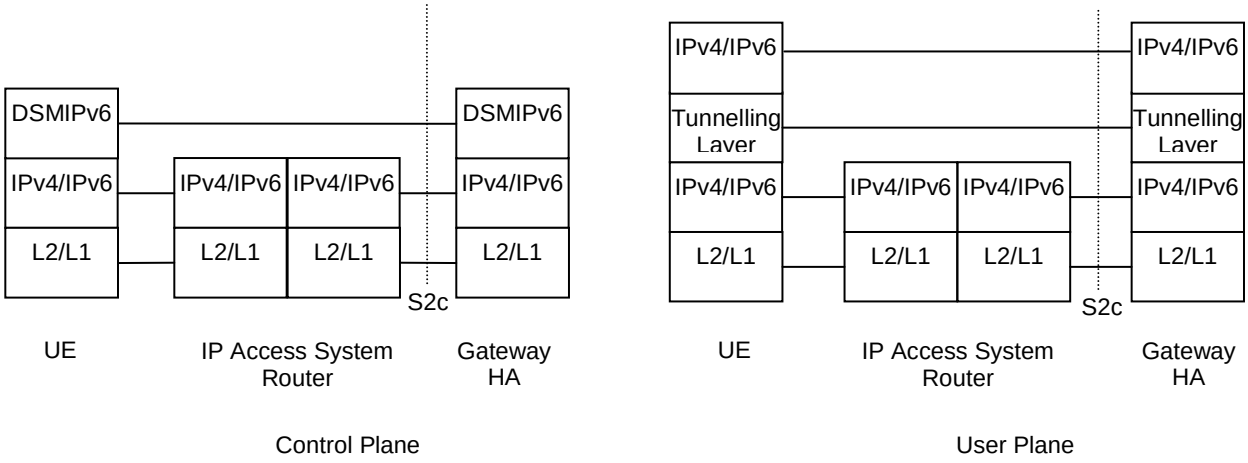
Figure 6.1.1-2: Protocols for MM control and user planes of S2a for the MIPv4 FA mode option

6.1.2 Protocol Stacks for S2c over Trusted Non-3GPP IP Accesses

The following protocol shall be supported on S2c over Trusted Non-3GPP IP Accesses:

- DSMIPv6, with IPsec and IKEv2 used to secure mobility signalling, as specified in RFC 4877 [22]

The figure below illustrates the control plane for Mobility Management (MM) and the user plane.



Legend:

- According to terms defined in DSMIPv6 [10], the functional entities terminating both the control and user planes are denoted MN (Mobile Node) in the UE, and HA (Home Agent) in the Gateway.
- The MM control plane stack is DSMIPv6 [10] over IPv6/IPv4.
- The user plane carries remote IPv4/v6 packets over either an IPv4 or an IPv6 transport network.
- The tunnelling layer implements IP encapsulation applicable for MIPv6 as defined in DSMIPv6 [10]. In some cases the tunnelling layer may be transparent.

Figure 6.1.2-1: Protocols for MM control and user planes of S2c for the DSMIPv6 option

6.2 Initial Attach on S2a

6.2.1 Initial Attach Procedure with PMIPv6 on S2a and Anchoring in PDN GW

PMIPv6 specification, RFC 5213 [8], is used to setup a PMIPv6 tunnel between the trusted non-3GPP IP access and the PDN GW. In both roaming and non-roaming cases, S2a is present. It is assumed that MAG exists in the trusted non-3GPP IP access.

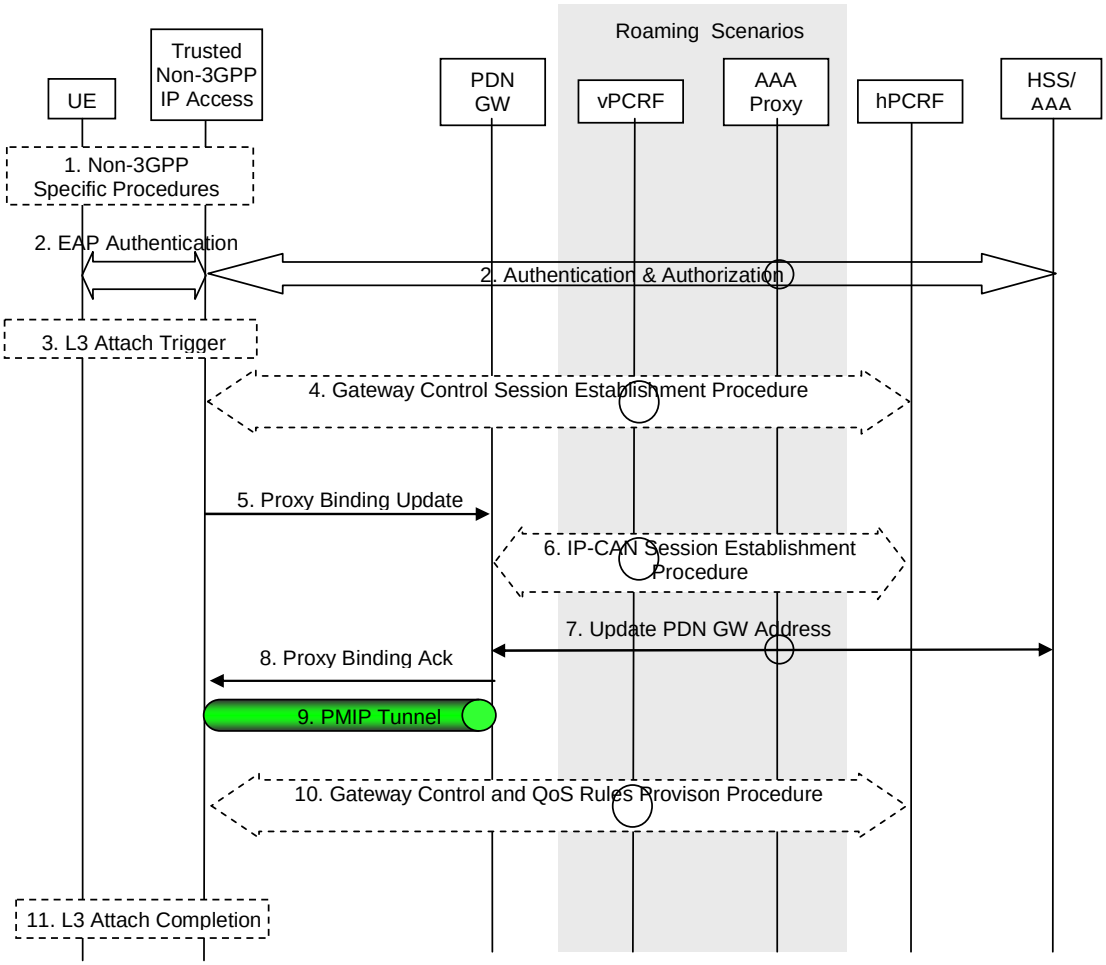


Figure 6.2.1-1: Initial attachment with Network-based MM mechanism over S2a for roaming, LBO and non-roaming scenarios

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured in the gateway.

This procedure applies to the Non-Roaming (Figure 4.2.2-1), Roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the non-3GPP access and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF. In the Roaming and LBO cases, the 3GPP AAA Proxy serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN. In the non-roaming case, the vPCRF is not involved at all.

This procedure is also used to establish the first PDN connection over a trusted non-3GPP access with S2a when the UE already has active PDN connections only over a 3GPP access and wishes to establish simultaneous PDN connections to different APNs over multiple accesses.

1) The initial Non-3GPP access specific L2 procedures are performed. These procedures are Non-3GPP access specific and are outside the scope of 3GPP.

2) The EAP authentication procedure is initiated and performed involving the UE, Trusted Non-3GPP IP Access and the 3GPP AAA Server. In the roaming case, there may be several AAA proxies involved. Subscription data is provided to the Trusted non-3GPP IP Access by the HSS/AAA in this step. The list of all the authorized APNs along with additional PDN GW selection information is returned to the access gateway as part of the reply from the 3GPP AAA Server to the trusted non-3GPP access as described in clause 4.5.1. The 3GPP AAA Server also returns to the trusted non-3GPP access the MN NAI to be used to identify the UE in Proxy Binding Update and Gateway Control Session Establishment messages (steps 4 and 10). If supported by Non-3GPP access network, the Attach Type is indicated to the Non-3GPP access network by the UE. The mechanism for supporting attach type is access technology specific and out of scope for 3GPP standardization. Attach Type indicates "Handover" when the UE already has active PDN connection(s) due to mobility from 3GPP access to non-3GPP access.

NOTE 1: The MN NAI returned from the 3GPP AAA Server to the trusted non-3GPP access is a permanent IMSI based MN NAI.

3) After successful authentication and authorization, the non-3GPP access specific L3 attach procedure is triggered. The UE may send requested APN to the Non-3GPP IP access in this step.

   If the UE sends a requested APN in this step, the Trusted non-3GPP Access verifies that it is allowed by subscription. If the UE does not send a requested APN the Trusted non-3GPP Access uses the default APN.

   The PDN Gateway selection takes place at this point as described in clause 4.5.1. This may entail an additional interaction with the Domain Name Server function in order to obtain the PDN GW address. If the PDN subscription profile returned by the 3GPP AAA Server in step 2 contains a PDN GW identity for the selected APN and the Attach Type does not indicate "Handover", the Non-3GPP access GW may request a new PDN GW as described in clause 4.5.1, e.g. to allocate a PDN GW that allows for more efficient routeing.

   The UE may request the type of address (IPv4 address or IPv6 prefix or both) during this step.

   If supported by the non-3GPP access, the UE may send Protocol Configuration Options in this step using access specific mechanisms. The Protocol Configuration Options provided by the UE may include the user credentials for PDN access authorization. In that case, in order to handle situations where the UE may have subscriptions to multiple PDNs, the UE should also send a requested APN to the non-3GPP IP access.

4) The Trusted non-3GPP access initiates the Gateway Control Session Establishment Procedure with the PCRF, as specified in TS 23.203 [19]. The Trusted non-3GPP access provides the information to the PCRF to correctly associate it with the IP-CAN session to be established in step 6 and also to convey subscription related parameters to the PCRF, including the APN-AMBR (if forwarded by the trusted non-3GPP IP access) and Default Bearer QoS.

5) The MAG function of Trusted Non-3GPP IP Access sends a Proxy Binding Update (MN-NAI, Lifetime, Access Technology Type, Handover Indicator, APN, GRE key for downlink traffic, Charging Characteristics, *Additional Parameters*) message to PDN GW. The MN NAI identifies the UE. The Lifetime field must be set to a nonzero value. Access Technology Type is set to a value matching the characteristics of the non-3GPP access. The MAG creates and includes a PDN connection identity if the MAG supports multiple PDN connections to a single APN. Handover Indicator is set to indicate attachment over a new interface as the UE has provided Attach Type indicating "Initial" attach. The Additional Parameters include the Protocol Configuration Options provided by the UE in step 3 and may also include other information. The MAG requests the IP address types (IPv4 address and/or IPv6 Home Network Prefix) based on requested IP address types and subscription profile in the same way as the PDN type is selected during the E-UTRAN Initial Attach in TS 23.401 [4]. If the PDN requires an additional authentication and authorization with an external AAA Server, the PDN GW performs such an additional authentication and authorization at the reception of the Proxy Binding Update.

NOTE 2: Any time after initiation of Step 4, Step 5 can be initiated by MAG.

6) The PDN GW initiates the IP-CAN Session Establishment Procedure with the PCRF, as specified in TS 23.203 [19]. The PDN GW provides information to the PCRF used to identify the session and associate Gateway Control Sessions established in step 4 correctly. The PCRF creates IP-CAN session related information and responds to the PDN GW with PCC rules and event triggers. If available, the PCRF may modify the APN-AMBR and provides the APN-AMBR and Default Bearer QoS to the PDN GW in the response message.

7) The selected PDN GW informs the 3GPP AAA Server of its PDN GW identity and the APN corresponding to the UE's PDN Connection. The message includes information that identifies the PLMN in which the PDN GW is located. This information is registered in the HSS as described in clause 12. The PDN GW shall only use the APN-AMBR and Default Bearer QoS received from the 3GPP AAA server in this step if these parameters have not been received in step 6.

8) The PDN GW processes the proxy binding update and creates a binding cache entry for the UE. The PDN GW allocates IP address(es) for the UE. The PDN GW then sends a Proxy Binding Acknowledgement (MN NAI, Lifetime, *UE Address Info, GRE key for uplink traffic, charging ID, Additional Parameters*) message to the MAG function in Trusted Non-3GPP IP Access, including the IP address(es) allocated for the UE. The UE Address Info includes one or more IP addresses. The Lifetime indicates the duration of the binding. If the corresponding Proxy Binding Update contains the PDN connection identity, the PDN GW shall acknowledge if multiple PDN connections to the given APN are supported. The Charging ID is assigned for the PDN connection for charging correlation purposes. The Additional Parameters may include Protocol Configuration Options and other information.

NOTE 3: If UE requests for both IPv4 and IPv6 addresses, both are allocated. If the PDN GW operator dictates the use of IPv4 addressing only or IPv6 addressing only for this APN, the PDN GW shall allocate only IPv4 address or only IPv6 prefix to the UE. If the UE requests for only IPv4 or IPv6 address only one address is allocated accordingly.

NOTE 4: The MAG learns from the PBA whether the PDN GW supports multiple PDN connections to the same APN or not.

9) The PMIPv6 tunnel is set up between the Trusted Non-3GPP IP Access and the PDN GW.

10) The PCRF may update the QoS rules in the trusted non-3GPP access by initiating the GW Control Session Modification Procedure, as specified in TS 23.203 [19].

11) L3 attach procedure is completed via non-3GPP access specific trigger. IP connectivity between the UE and the PDN GW is set for uplink and downlink directions. At this step the IP address information is provided to the UE. Unless already known from step 3, the Non-3GPP IP access should indicate the connected PDN identity (APN) to the UE. If supported by the non-3GPP access, the Protocol Configuration Options provided by the PDN GW in step 8 are returned to the UE in this step using access specific mechanisms.

6.2.2 Void

6.2.3 Initial Attach procedure with MIPv4 FACoA on S2a and Anchoring in PDN-GW

MIPv4 [12] is used to setup a MIP tunnel between the Trusted non-3GPP IP Access and the PDN GW. It is assumed that a Foreign Agent (FA) is located in the Trusted non-3GPP IP Access.

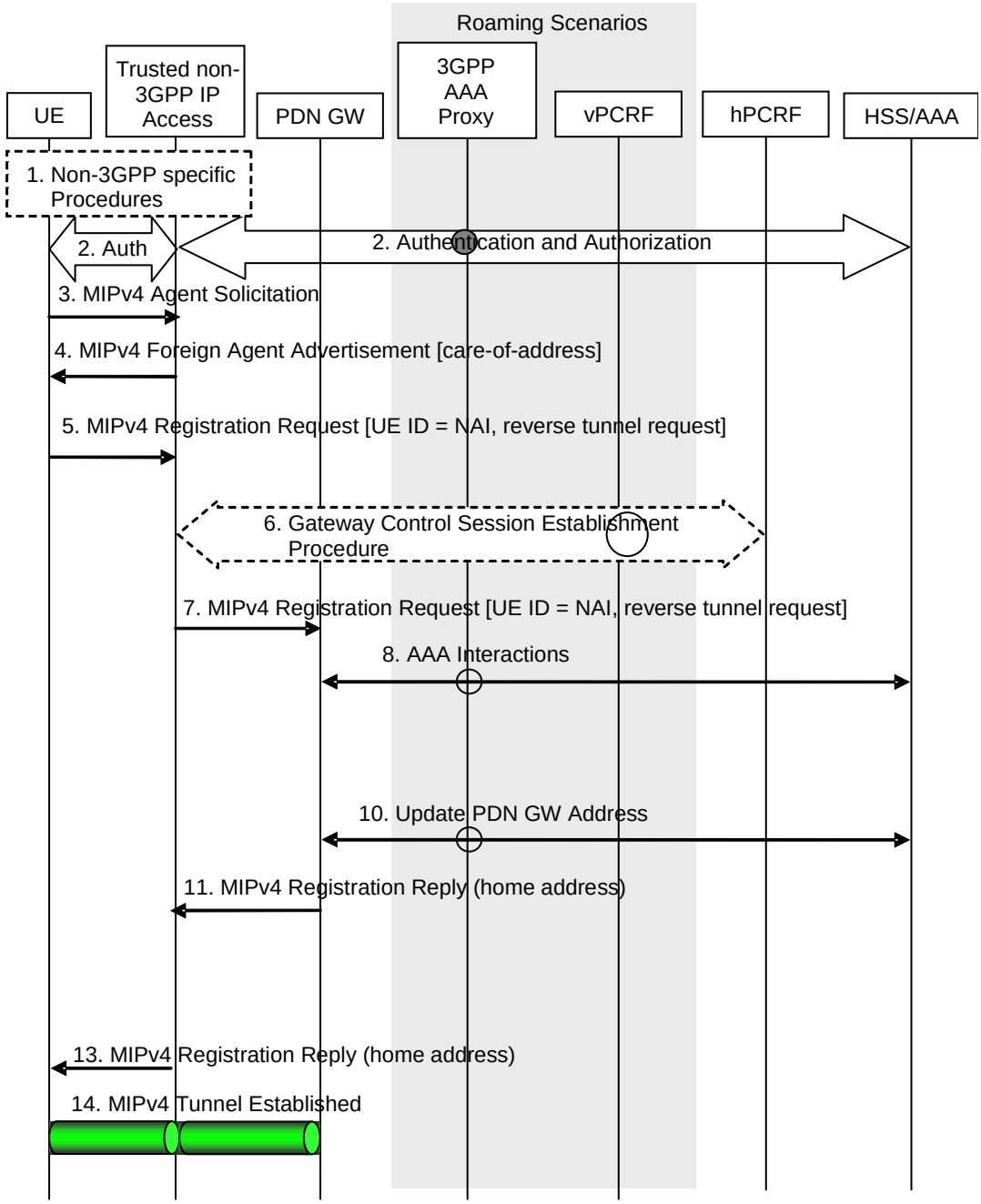


Figure 6.2.3-1: Initial attachment when MIPv4 FACoA mode MM mechanism is used over S2a

When the Attach procedure occurs in the Non-Roaming case (Figure 4.2.2-1), the vPCRF is not involved. The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

This procedure applies to the Non-Roaming (Figure 4.2.2-1), Roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the non-3GPP access and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF. In the Roaming and LBO cases, the 3GPP AAA Proxy serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN. In the non-roaming case, the vPCRF is not involved at all.

This procedure is also used to establish the first PDN connection over a trusted non-3GPP access with MIPv4 FACoA on S2a when the UE already has active PDN connections only over a 3GPP access and wishes to establish simultaneous PDN connections to different APNs over multiple accesses.

The event that triggers Authentication and Authorization in step 2 between the Trusted Non-3GPP IP Access and the 3GPP AAA Server, depends on the specific access technology.

1) The initial Non-3GPP access specific L2 procedure and Non-3GPP access specific authentication procedures may be performed. These procedures are outside the scope of 3GPP.

2) The EAP-based authentication procedure for trusted non-3GPP access networks between UE and the 3GPP EPC shall be performed as defined by TS 33.402 [45]. The PDN Gateway information is returned as part of the reply from the 3GPP AAA Server to the FA in the trusted non-3GPP access as described in clause 4.5.1. The Attach Type is indicated to the Non-3GPP access network by the UE as described in the step 2 of clause 6.2.1.

3) The UE may send an Agent Solicitation (AS) RFC 5944 [12] message. Specification of this message is out of the scope of 3GPP.

4) The FA in the Trusted Non-3GPP IP Access sends a Foreign Agent Advertisement (FAA) [12] message to the UE. The FAA message includes the Care-of Address (CoA) of the Foreign Agent function in the FA. Specification of this message is out of the scope of 3GPP.

5) The UE sends a Registration Request (RRQ) (MN-NAI, lifetime, APN) message to the FA as specified in RFC 5944 [12]. The MN NAI identifies the UE. Reverse Tunnelling shall be requested. This ensures that all traffic will go through the PDN GW. The RRQ message shall include the NAI-Extension RFC 2794 [34]. The UE may not indicate a specific Home Agent address in the RRQ message, in which case the PDN Gateway/Home Agent is selected by the FA as per step 2. The UE then receives the IP address of the PDN Gateway in step 13 as part of the Registration Reply (RRP) message. The UE should then include the PDN Gateway address in the Home Agent address field of subsequent RRQ messages. Subscription data is provided to the Trusted non-3GPP IP Access by the HSS/AAA in this step. The UE may request connectivity to a specific PDN by using an APN as specified in RFC 5446 [39]. If the UE provides an APN the FA verifies that it is allowed by subscription. If the UE does not provide an APN the FA establishes connectivity with the default PDN. The PDN Gateway selection takes place at this point as described in clause 4.5.1. This may entail an additional name resolution step.

6) The Trusted non-3GPP access initiates the Gateway Control Session Establishment Procedure with the PCRF, as specified in TS 23.203 [19]. The Trusted non-3GPP access provides the information to the PCRF to correctly associate it with the IP-CAN session to be established in Step 9 and also to convey subscription related parameters to the PCRF, including the APN-AMBR (if forwarded by the trusted non-3GPP IP access) and Default Bearer QoS.

7) The FA processes the message according to RFC 5944 [12] and forwards a corresponding RRQ (MN-NAI, APN) message to the PDN GW.

8) The selected PDN GW obtains Authentication and Authorization information from the 3GPP AAA/HSS.

9) The PDN GW allocates an IP address for the UE. The PDN GW initiates the IP-CAN Session Establishment Procedure with the PCRF, as specified in TS 23.203 [19]. The PDN GW provides information to the PCRF used to identify the session and associate Gateway Control Sessions established in step 6 correctly. The PCRF creates IP-CAN session related information and responds to the PDN GW with PCC rules and event triggers.

10) The selected PDN GW informs the 3GPP AAA Server of the PDN GW identity and the APN corresponding to the UE's PDN Connection. The message includes information that identifies the PLMN in which the PDN GW is located. This information is registered in the HSS as described in clause 12.

11) The PDN GW sends a RRP (MN-NAI, Home Address, Home Agent Address, Lifetime) as defined in RFC 5944 [12] to the FA. The Home Address includes UE Home IP address, the Home Agent Address contains the IP address of Home Agent. The Lifetime indicates the duration of the binding.

12) In case the QoS rules have changed, the PCRF updates the QoS rules in the Trusted non-3GPP access by initiating the GW Control Session Modification Procedure, as specified in TS 23.203 [19].

13) The FA processes the RRP (MN-NAI, Home Address, Home Agent Address) according to RFC 5944 [12] and sends a corresponding RRP message to the UE.

14) IP connectivity from the UE to the PDN GW is now setup. A MIPv4 tunnel is established between the FA in the Trusted Non-3GPP IP Access and the PDN GW.

6.2.4 Initial Attach Procedure with PMIPv6 on S2a and Chained S2a and PMIP-based S8

This clause defines the initial attach procedure for the PMIP-based S8/S2a chaining. This procedure also applies to the initial attach for PMIP-based S8/S2b chaining.

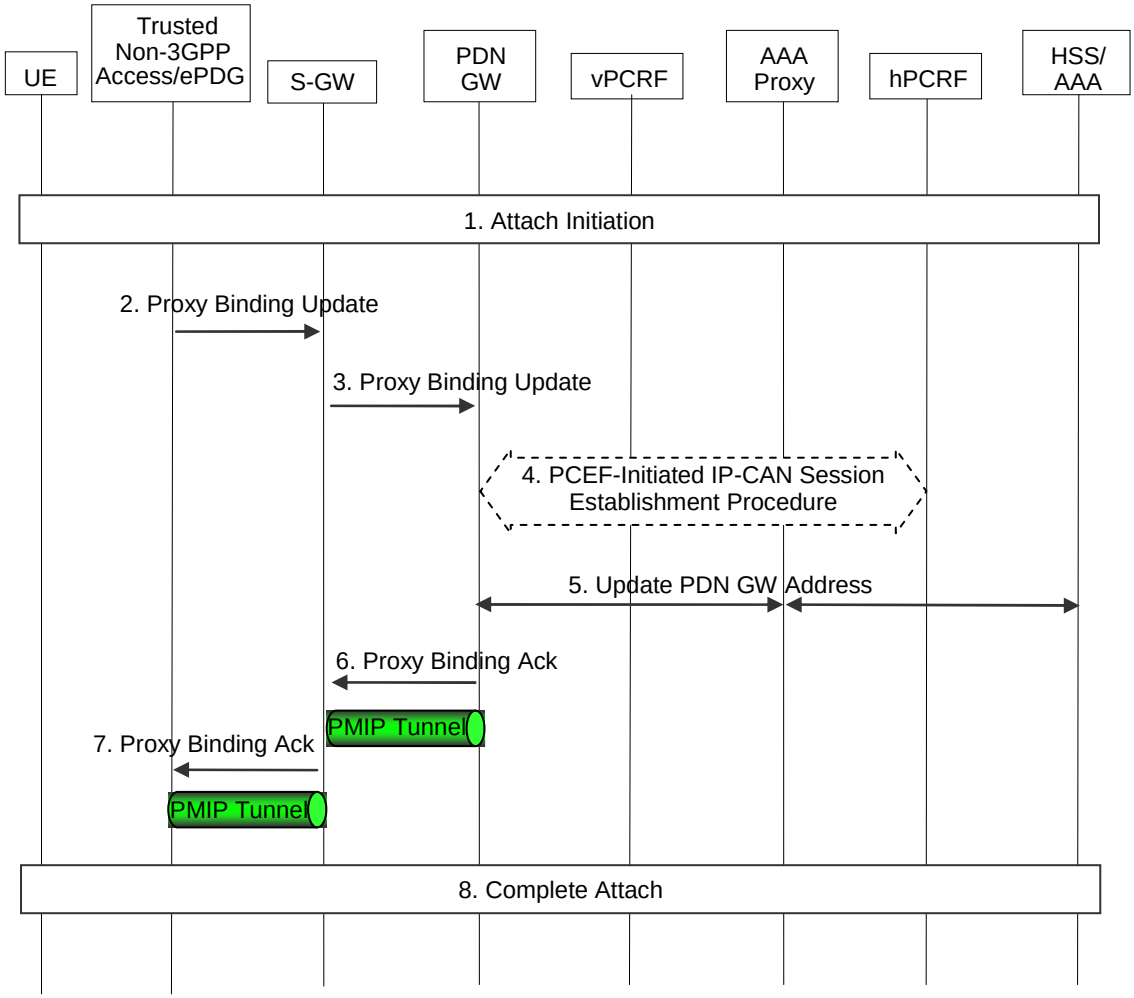


Figure 6.2.4-1: Initial attachment for chained PMIP-based S8-S2a/b roaming scenarios

1) The attach initiation on the trusted or untrusted non-3GPP access is performed as described in steps 1-4 of clause 6.2.1 (for trusted non-3GPP access) and step 1 of clause 7.2.1 (for untrusted non-3GPP access). As part of the authentication procedure, the 3GPP AAA proxy obtains the PDN GW selection information from the HSS/AAA as described in clause 4.5.1, and performs Serving GW selection as described in clause 4.5.3. 3GPP AAA proxy provides both PDN GW selection information and Serving GW identity to the MAG function of the trusted non-3GPP access or ePDG. Then the MAG function performs the PDN GW selection. If PCC is deployed, the MAG function of the Trusted Non-3GPP IP access is notified to interact with the PCRF when it is PMIP-based chained case.

2) The MAG function of Trusted Non-3GPP IP Access or ePDG sends a Proxy Binding Update (MN-NAI, Lifetime, Access Technology Type, Handover Indicator, APN, GRE key for downlink traffic, PDN GW address, Additional Parameters) message to the Serving GW in the VPLMN. The MN NAI identifies the UE. The Lifetime field must be set to a nonzero value, indicating registration. Access Technology Type is set to a value matching the characteristics of the non-3GPP access. The MAG creates and includes a PDN connection identity if the MAG supports multiple PDN connections to a single APN. Handover Indicator is set to indicate attachment over a new interface. The MAG requests the IP address types (IPv4 address and/or IPv6 Home Network Prefix) based on requested IP address types and subscription profile in the same way as the PDN type is selected during the E-UTRAN Initial Attach in TS 23.401 [4]. The Additional Parameters may include Protocol Configuration Options and other information.

3) The Serving GW sends a corresponding Proxy Binding Update (MN-NAI, Lifetime, Access Technology Type, Handover Indicator, APN, GRE key for downlink traffic, Additional Parameters) message (as in step 2) to the PDN GW. The GRE key for downlink traffic is allocated by the Serving GW. If the MAG included the PDN connection identity in the Proxy Binding Update of the previous step and the Serving GW supports multiple PDN connections to a single APN then the Serving GW forwards the PDN connection identity to the PDN GW.

NOTE 1: In this Release of the specification, the Serving GW uses the right protocol to connect with the PDN GW based on the pre-configured information on itself in case the selected Serving GW supporting both PMIP and GTP.

4) The PDN GW initiates the PCEF-initiated IP CAN Session Establishment Procedure with the hPCRF, as specified in TS 23.203 [19].

5) The selected PDN GW informs the 3GPP AAA Server of the PDN GW identity. The message includes information that identifies the PLMN in which the PDN GW is located. The 3GPP AAA Server then conveys this information to the HSS for the UE.

6) The PDN GW processes the proxy binding update and allocates IP address(es) for the UE. The PDN GW creates a binding cache entry for the PMIPv6 tunnel towards the Serving GW and sends a Proxy Binding Acknowledgement (MN NAI, Lifetime, UE Address Info, GRE key for uplink traffic, Charging ID, Additional Parameters) message to the Serving GW. The MN NAI is identical to the MN NAI sent in the Proxy Binding Update. The Lifetime indicates the duration the binding will remain valid. The UE Address Info includes one or more IP addresses. If the corresponding Proxy Binding Update contains the PDN connection identity, the PDN GW shall acknowledge if multiple PDN connections to the given APN are supported. The Charging ID is assigned for the PDN connection for charging correlation purposes. The Additional Parameters may include Protocol Configuration Options and other information.

NOTE 2: If UE requests for both IPv4 and IPv6 addresses, both are allocated. If the UE requests for only IPv4 or IPv6 address only one address is allocated accordingly.

NOTE 3: The MAG learns from the PBA whether the PDN GW supports multiple PDN connection to the same APN or not.

7) The Serving GW processes the proxy binding acknowledgement and creates a binding cache entry for the PMIPv6 tunnel towards the MAG function in the trusted non-3GPP access or ePDG. At this point, the Serving GW also establishes the internal forwarding state for the concatenation of the PMIPv6 tunnels. The Serving GW then sends a corresponding Proxy Binding Acknowledgement (MN NAI, Lifetime, UE Address Info, GRE key for uplink traffic, Charging ID, Additional Parameters) message (as in step 7) to the MAG function of Trusted Non-3GPP IP Access or ePDG. The GRE key for uplink traffic is allocated by the Serving GW. The Charging ID is assigned for the PDN connection for charging correlation purposes.

8) The attach procedure is completed as described in steps 10-11 of clause 6.2.1 (for trusted non-3GPP access) and steps 6-8 of clause 7.2.1 (for untrusted non-3GPP access).

6.3 Initial Attach Procedure with DSMIPv6 on S2c in Trusted Non-3GPP IP Access

This clause is related to the case when the UE attaches to a Trusted Non-3GPP Access network and host based mobility management mechanisms are used. Dual Stack MIPv6 [10] is used for supporting mobility over S2c interface.

The S2c initial attach can be seen to consist of several modules:

A. The UE sets up local IP connectivity in a Trusted Non-3GPP Access

B. The UE discovers the HA, and establishes a security association with it to protect DSMIPv6 signalling.

C. The UE performs a Binding Update with the PDN GW

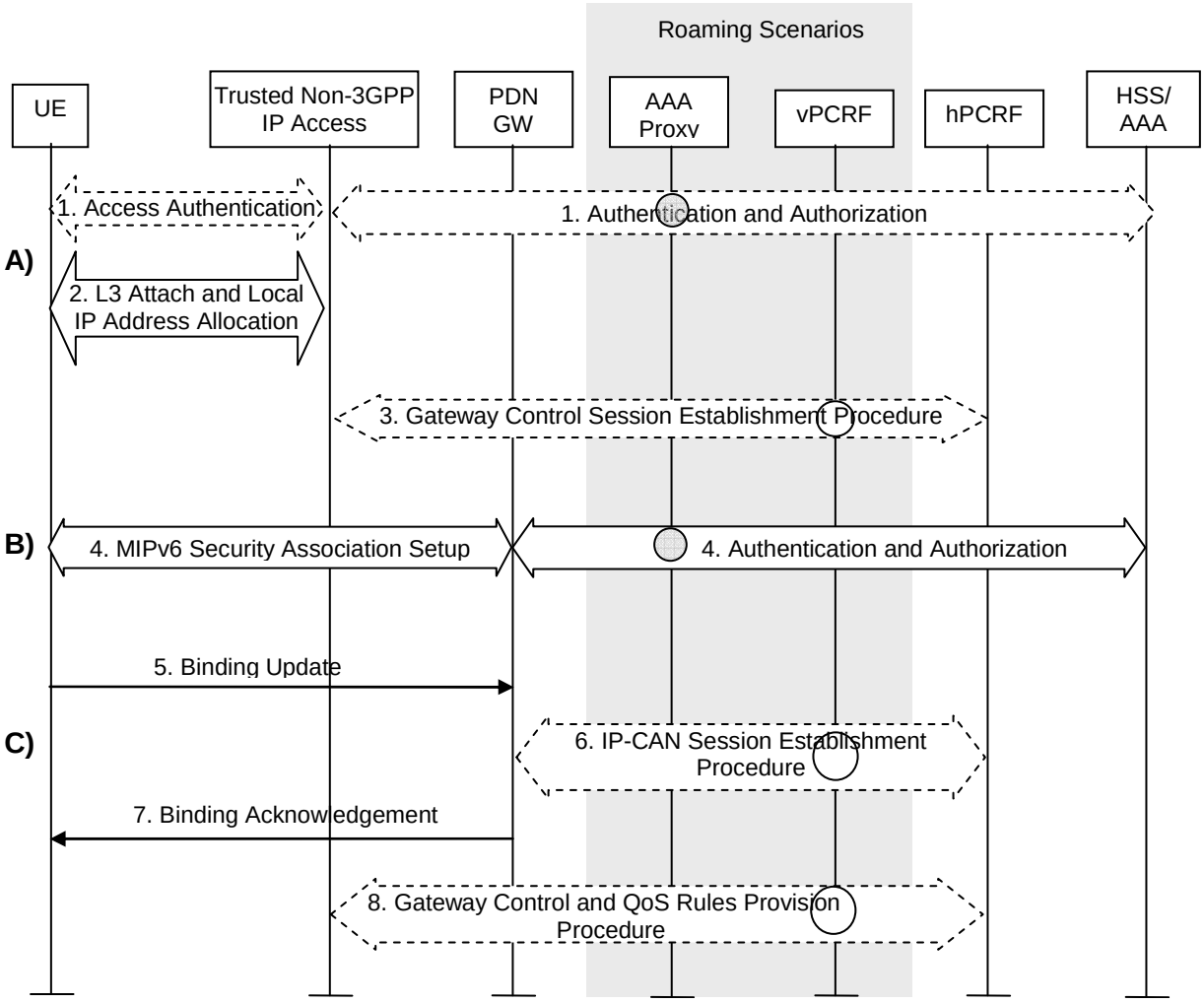


Figure 6.3-1: Initial attachment from Trusted Non-3GPP IP Access with DSMIPv6

Non-roaming (Figure 4.2.2-1), home routed roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-4) cases are supported by this procedure. The AAA proxy and vPCRF are only used in the case of home routed roaming and Local Breakout. In non-roaming scenarios, the AAA proxy and vPCRF are not involved.

This procedure is also used to establish the first PDN connection over a trusted non-3GPP access with DSMIPv6 on S2c when the UE already has active PDN connections only over a 3GPP access and wishes to establish simultaneous PDN connections to different APNs over multiple accesses.

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured in the gateway.

The UE may be authenticated and authorised to access the Trusted Non-3GPP Access network according to an access network specific procedure. These procedures are outside the scope of 3GPP, After the authentication, UE is configured with Local IP Address from the access network domain.

A) Setup of Local IP connectivity

1) Access Authentication procedure for trusted Non-3GPP access networks between UE and the 3GPP EPC shall be performed as defined by TS 33.402 [45] unless the conditions in TS 33.402 [45] are met that allow to skip this procedure. As indicated above, in the roaming case signalling may be routed via a 3GPP AAA Proxy in the VPLMN. As part of the AAA exchange for network access authentication, the AAA/HSS and/or the 3GPP AAA Proxy may return to the Trusted non-3GPP IP Access a set of home/visited operator's policies to be enforced on the usage of local IP address, or IPv6 prefix, allocated by the access system upon successful authentication. Subscription data is provided to the Trusted non-3GPP IP Access by the HSS/AAA in this step.

2) The L3 connection is established between the UE and the Trusted Non-3GPP Access system. As a result of this procedure, an IPv4 address or an IPv6 address/prefix is also assigned to the UE by the access system (i.e. a Local IP address that will be used as a Care-of Address for DSMIPv6 over the S2c reference point).

NOTE 1: It is assumed that the access system is aware that network-based mobility procedures do not need to be initiated.

NOTE 2: The access system may complete the step 2 after step 3.

3) If the access system supports PCC-based policy control, the access gateway initiates a Gateway Control Session Establishment Procedure with the PCRF as specified in TS 23.203 [19]. The message includes at least the UE IP address or IPv6 prefix allocated by the access system in step 2. The message includes also the IP-CAN type.

   Based e.g. on the UE identity and user profile, operator's policies and the IP-CAN type, the PCRF decides on the QoS policy rules and completes the session establishment towards the access gateway. The rules provided in this step are referred to the address assigned by the trusted non-3GPP access.

   In the roaming case, PCC signalling is sent via a vPCRF in the VPLMN.

NOTE 3: The UE identity information to be used by the access system to establish the session with the PCRF may be piggybacked by the AAA/HSS in step 1.

B) PDN GW/HA Discovery and HoA Configuration.

4) The UE discovers the PDN GW (Home Agent) as specified in clause 4.5.2 of TS 23.402 (this specification). A security association is established between UE and PDN GW to secure the DSMIPv6 messages between UE and PDN GW and for authentication between the UE and the PDN GW. The UE initiates the establishment of the security association using IKEv2 [9]; EAP [11] is used over IKEv2 for authentication purposes. The PDN GW communicates with the AAA infrastructure in order to complete the EAP authentication via S6b. The APN-AMBR and Default Bearer QoS is provided to the PDN GW in this step.

   If the PDN requires an additional authentication and authorization with an external AAA Server, an additional authentication is executed in this step. Details on these multiple authentications are specified in RFC 4739 [50] and in TS 33.402 [45] (Private Network Access (PNA)).

   During this step the UE may include the APN of the PDN it wants to access and it can also request the IPv6 home prefix as defined in RFC 5026 [40] in order to influence the IPv6 home network prefix assignment procedure. Even if the UE requests more than one IPv6 home prefix, the PDN GW shall assign only one IPv6 home prefix to the UE.

   During this step an IPv6 home prefix is assigned by the PDN GW to the UE as defined in RFC 5026 [40]. After the IPv6 home network prefix is assigned, UE constructs a home address from it via auto-configuration. The associated PDN identity (APN) shall be indicated to the UE via the IDr payload. In case the UE provided APN to the PDN GW earlier in this step, the PDN GW shall not change the provided APN.

   During this step, the PDN GW also informs the 3GPP AAA Server of the identity of the selected PDN GW and the APN corresponding to the UE's PDN Connection. The PDN GW also provides information that identifies the PLMN in which the PDN GW is located. This information is registered in the HSS as described in clause 12.

NOTE 4: The MN NAI and APN string are delivered from the UE to the PDN GW in step 4 in order to support PCC interactions in step 6.

C) Binding Update

5) The UE sends the DSMIPv6 Binding Update (IP Addresses (HoA, CoA), Lifetime) message to the PDN GW as specified in RFC 5555 [10]. The UE shall inform the PDN GW that IP address preservation shall be maintained for the whole home network prefix.

   The PDN GW processes the binding update. During the processing the PDN GW performs authentication and authorization of the message using the IPsec security association established in Step 4. During this step the UE can request an IPv4 home address to the PDN GW as defined in RFC 5555 [10].

6) If PCC is supported, the PDN GW initiates the IP-CAN Session Establishment Procedure with the PCRF as specified in TS 23.203 [19]. The message includes at least the HoA and the CoA. The message may also include a permanent UE identity and an APN string. The PDN GW shall provide information about the mobility protocol tunnelling header to the PCRF, the APN-AMBR and Default Bearer QoS obtained in step 4.

   The PCRF decides on the PCC rules and Event Triggers and provisions them to the PDN GW. The PDN GW installs the received PCC rules.

NOTE 5: The permanent UE identity to be used by the PDN GW to establish the session with the PCRF may be piggybacked by the AAA/HSS in step 4.

7) The PDN GW sends the DSMIPv6 Binding Ack (Lifetime, IP Addresses (HoA, CoA)) message to the UE. In this step the PDN GW may include the duration of the binding and the IPv4 home address allocated for the UE as specified in RFC 5555 [10], if previously requested by the UE and allowed by the subscription profile as it is specified in the E-UTRAN attach procedure in TS 23.401 [4]. Even in case the UE requests more than one IPv4 home address in step 5, the PDN GW shall assign only one IPv4 home address for the UE.

8) The PCRF initiates the Gateway Control and QoS Rules Provision Procedure specified in TS 23.203 [19] by sending a message with the information of mobility protocol tunnelling encapsulation header to the Trusted non 3GPP access Gateway. In case the QoS rules have changed, the updated QoS rules shall also be included in this message.

NOTE 6: Rules related to the HoA can be sent to the Trusted Non-3GPP Access based on the procedure in clause 6.6.2.

6.4 Detach and PDN Disconnection for S2a

6.4.1 UE/Trusted Non-3GPP IP Access Network Initiated Detach and UE/Trusted Non-3GPP IP Access requested PDN Disconnection Procedure with PMIPv6

6.4.1.1 Non-Roaming, Home Routed Roaming and Local Breakout Case

The procedure in this clause applies to both Detach Procedures, including UE or Trusted non-3GPP access initiated detach procedure, and UE/Trusted non-3GPP Access requested PDN disconnection procedure when supported by the Trusted non-3GPP access.

The UE can initiate the detach procedure, e.g. when the UE is power off. The Trusted Non-3GPP Access Network can initiate the detach procedure due to administrative reasons or detecting the UE's leaving by, e.g. Link-layer event specific to the access technology (refer to PMIPv6 specification, RFC 5213 [8], for more information).

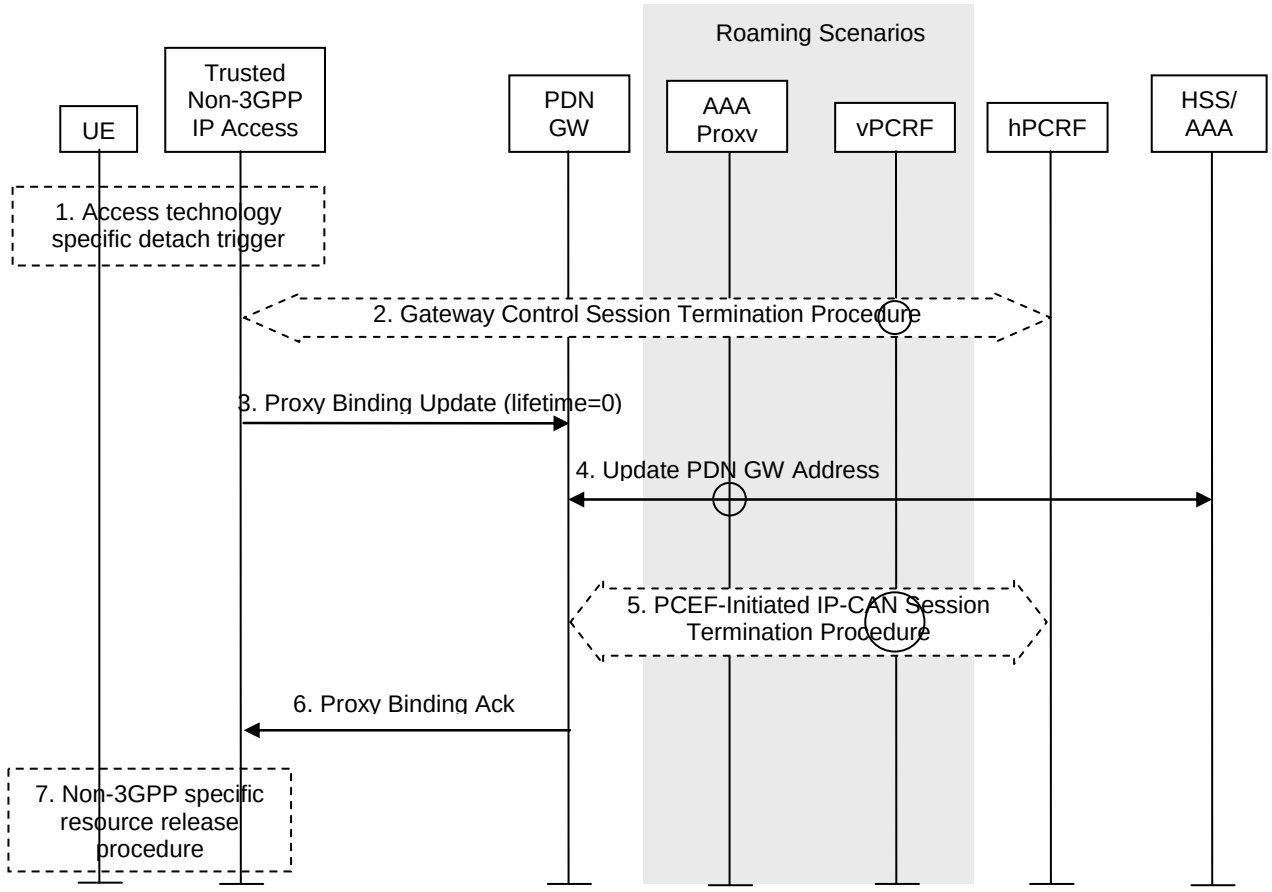


Figure 6.4.1.1-1: UE/Trusted Non-3GPP Access Network initiated detach procedure or PDN-disconnection with PMIPv6

For detach procedure and in case of connectivity with multiple PDNs, the steps 2 to 6 are repeated for each PDN the UE is connected to.

For UE-requested PDN disconnection procedure, steps 2 to 6 are performed for the PDN that the UE requested disconnection from.

This procedure applies to the Non-Roaming (Figure 4.2.2-1), Roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the non-3GPP access and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF. In the Roaming and LBO cases, the 3GPP AAA Proxy serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN. In the non-roaming case, the vPCRF is not involved at all.

If dynamic policy provisioning is not deployed, the optional steps of interaction between the gateways and PCRF do not occur. Instead, the PDN GW may employ static configured policies.

1) The UE or the Trusted Non-3GPP Access Network triggers either detach or disconnection from a specific PDN by an access technology specific procedure. In the case of PDN disconnection of a PDN connection out of multiple PDN connections, the UE shall use the access specific mechanism for differentiating the PDN connections towards the same APN (see clause 6.8.1.1) to indicate the PDN connection to be deregistered and allow the Mobile Access Gateway in the Trusted Non-3GPP IP Access to select the corresponding PDN connection identity needed in step 3 (e.g. the UE informs the Trusted Non-3GPP access of the prefix to be disconnected).

2) The Trusted Non-3GPP Access Network initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [19]. The Trusted Non-3GPP Access Network no longer applies QoS policy to traffic flows for this UE.

3) The Mobile Access Gateway (MAG) in the Trusted Non-3GPP IP Access sends a Proxy Binding Update (MN NAI, APN, lifetime=0) message to the PDN GW with lifetime value set to zero, indicating de-registration. The MN NAI identifies the UE to deregister from the PDN GW. When only one PDN connection to the given APN is

allowed the APN is needed in order to determine which PDN to deregister the UE from, as some PDN GWs may support multiple PDNs. When multiple PDN connections to the given APN are supported the APN and the PDN connection identity are needed in order to determine which PDN to deregister the UE from.

4) The PDN GW informs the 3GPP AAA Server of the PDN disconnection. If the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server notifies the HSS as described in clause 12.1.2.

5) The PDN GW deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [19].

6) The PDN GW deletes existing entries implied in the Proxy Binding Update message from its Binding Cache and sends a Proxy Binding Ack (MN NAI, APN, lifetime=0) message to the MAG.

7) Non-3GPP specific resource release procedure is executed. The resources of Trusted Non-3GPP Access Network are released. In case of disconnection from a PDN, if the PDN from which the UE is disconnected was the only PDN that the UE was connected to, detach related procedures may be performed in the Trusted non-3GPP IP access.

6.4.1.2 Chained PMIP-based S8-S2a Roaming Case

This clause defines the UE/Trusted Non-3GPP IP Access Network-initiated detach procedure UE-requested PDN disconnection procedure for PMIP-based S8-S2a chaining. This procedure also applies to UE/ePDG-initiated detach procedure for PMIP-based S8-S2b chaining.

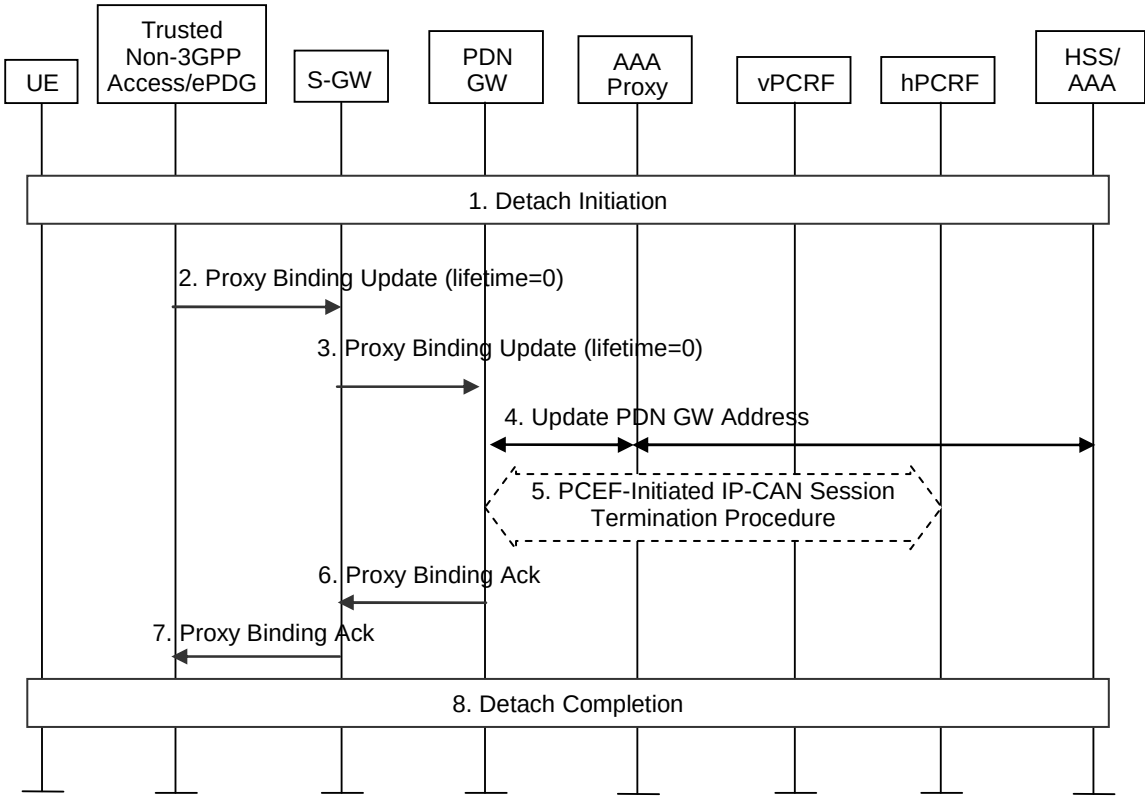


Figure 6.4.1.2-1: UE/ePDG/Trusted Non-3GPP Access Network initiated detach procedure for chained PMIP-based S8-S2a/b roaming scenarios and PDN-disconnection for chained PMIP-based S8-S2a

For detach procedure and in case of connectivity with multiple PDNs, the steps 2 to 7 are repeated for each PDN the UE is connected to.

For UE-requested PDN disconnection procedure for chained PMIP-based S8-S2a, steps 2 to 7 are performed for the PDN that the UE requested disconnection from.

1) For detach, initial steps of the detach is performed as described in steps 1-2 of clause 6.4.1.1 (for trusted non-3GPP access) and step 1 of clause 7.4.1.1 (for untrusted non-3GPP access). For UE-requested PDN disconnection in chained PMIP-based S8-S2a, steps 1-2 of clause 6.4.1.1 are performed.

2) The MAG in the Trusted Non-3GPP IP Access or ePDG sends a Proxy Binding Update (MN NAI, APN, lifetime=0) message to the Serving GW with lifetime value set to zero, indicating de-registration. The MN NAI identifies the UE to deregister from the PDN GW. When only one PDN connection to the given APN is allowed the APN is needed in order to determine which PDN to deregister the UE from, as some PDN GWs may support multiple PDNs. When multiple PDN connections to the given APN are supported the APN and PDN connection identity are needed in order to determine which PDN to deregister the UE from.

3) The Serving GW deletes all existing entries implied in the Proxy Binding Update message from its Binding Cache and releases all associated resources (e.g. GRE tunnel), and then sends a corresponding Proxy Binding Update message (as in step 2) to the PDN GW in the HPLMN.

4) The PDN GW informs the 3GPP AAA Server of the PDN disconnection. If the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server notifies the HSS as described in clause 12.1.2.

5) The PDN GW initiates the PCEF-initiated IP CAN Session Termination Procedure, as specified in TS 23.203 [19].

6) The PDN GW deletes existing entries implied in the Proxy Binding Update message from its Binding Cache and releases all associated resources, and then sends a Proxy Binding Ack (MN NAI, APN, lifetime=0) message to the Serving GW in the VPLMN.

7) The Serving GW sends a corresponding Proxy Binding Ack message (as in step 6) to the MAG function in Trusted Non-3GPP IP Access.

8) The detach procedure is completed as described in step 7 of clause 6.4.1.1 (for trusted non-3GPP access) and step 6 of clause 7.4.1.1 (for untrusted non-3GPP access). In case of disconnection from a PDN, if the PDN from which the UE is disconnected was the only PDN that the UE was connected to, detach related procedures may be performed.

6.4.2 HSS/AAA Initiated Detach Procedure with PMIPv6

6.4.2.1 Non-Roaming, Home Routed Roaming and Local Breakout Case

HSS/AAA-initiated detach procedure with PMIPv6 is illustrated in figure 6.4.2.1-1. The HSS can initiate the procedure e.g. when the user's subscription is removed. The 3GPP AAA Server can initiate the procedure, e.g. instruction from O&M, timer for re-authentication/re-authorization expired.

If the HSS/AAA-initiated detach procedure has been initiated to delete the UE from the Evolved Packet Core, the HSS/AAA server shall initiate the detach procedure for each of the access systems to which the UE is registered.

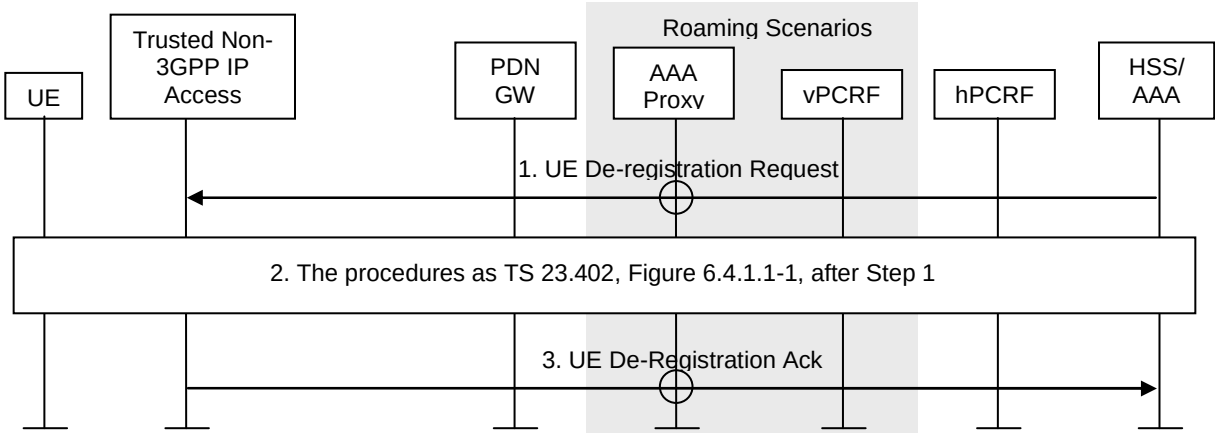


Figure 6.4.2.1-1: HSS/AAA-initiated detach procedure with PMIPv6

This procedure applies to the Non-Roaming (Figure 4.2.2-1), Roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the non-3GPP access and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF. In the Roaming and LBO cases, the 3GPP AAA Proxy serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN. In the non-roaming case, the vPCRF is not involved at all.

1) The HSS/AAA sends a Detach Indication message to the MAG in the Trusted Non-3GPP Access Network to detach a specific UE.

2) This includes the procedure after step 1 as in figure 6.4.1.1-1.

3) The MAG of the Trusted Non-3GPP Access Network sends a Detach Ack message to the 3GPP AAA Server. If the detach procedure was initiated from the 3GPP AAA Server and if the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server communicates the HSS as described in clause 12.1.2. If the detach procedure was initiated by HSS, the 3GPP AAA Server replies to the HSS as described in clause 12.1.3.

NOTE: The HSS/AAA may also send a detach indication message to the PDN GW. The PDN GW does not remove the PMIP tunnels on S2a, since the MAG in the non-3GPP access is responsible for removing the PMIP tunnels on S2a. The PDN GW acknowledges the receipt of the detach indication message to the 3GPP AAA Server.

6.4.2.2 Chained PMIP-based S8-S2a Roaming Case

This clause defines the HSS/AAA-initiated detach procedure for PMIP-based S8-S2a chaining. This procedure also applies for PMIP-based S8-S2b chaining.

If the HSS/AAA-initiated detach procedure has been initiated to delete the UE from the Evolved Packet Core, the HSS/AAA server shall initiate the detach procedure for each of the access systems to which the UE is registered.

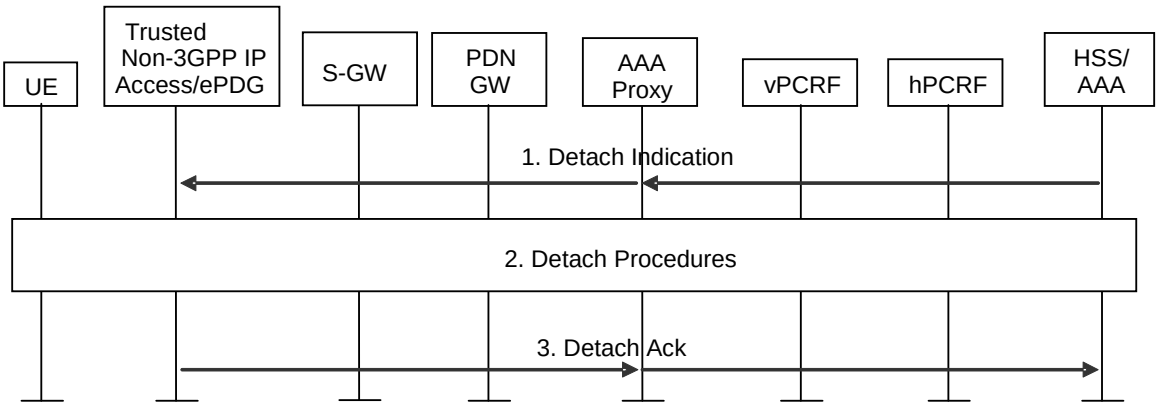


Figure 6.4.2.2-1: HSS/AAA-initiated detach procedure for chained PMIP-based S8-S2a/b roaming scenarios

1) The HSS/AAA sends a Detach Indication message to the MAG in the Trusted Non-3GPP Access Network or ePDG to detach a specific UE.

2) The detach procedure as described in steps 2-8 of clause 6.4.1.2 is performed.

3) The MAG of the Trusted Non-3GPP Access Network or ePDG sends a Detach Ack message to the 3GPP AAA Server. If the detach procedure was initiated from the 3GPP AAA Server and if the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server communicates the HSS as described in clause 12.1.2. If the detach procedure was initiated by HSS, the 3GPP AAA Server replies to the HSS as described in clause 12.1.3.

NOTE: The HSS/AAA may also send a detach indication message to the PDN GW. The PDN GW does not remove the PMIP tunnels on S2a, since the MAG in the non-3GPP access is responsible for removing the PMIP tunnels on S2a. The PDN GW acknowledges the receipt of the detach indication message to the 3GPP AAA Server.

6.4.3 UE-initiated Detach Procedure and UE-Requested PDN Disconnection Procedure with MIPv4 FACoA

The procedure in this clause applies to both UE initiated Detach Procedure and UE-requested PDN disconnection procedure with MIPv4 FACoA when supported by the Trusted non-3GPP access.

The UE can initiate this procedure, e.g. when the UE is powered off.

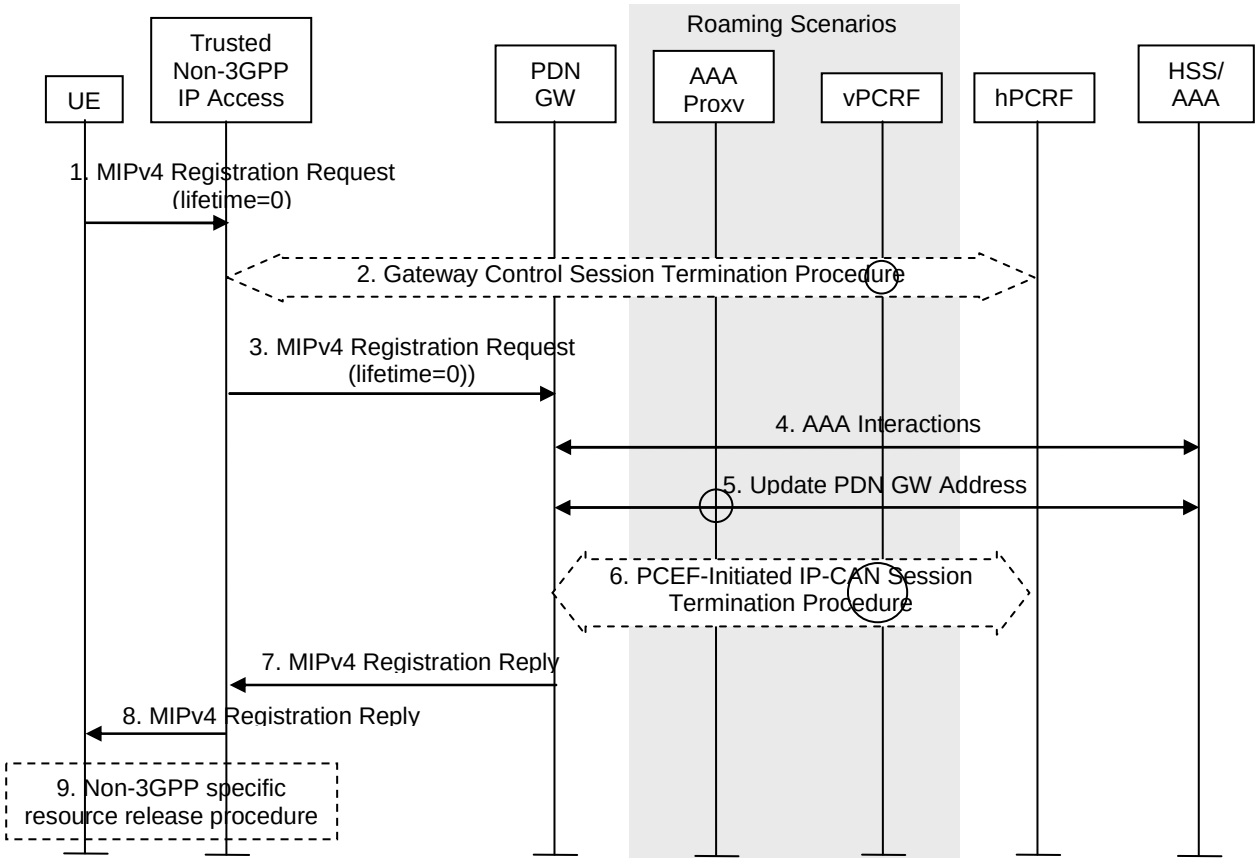


Figure 6.4.3-1: UE-initiated detach procedure with MIPv4 FACoA

NOTE: AAA proxy and vPCRF are only used in the case of home routed roaming (Figure 4.2.3-1) and local breakout (Figure 4.2.3-4).

For detach procedure and in case of connectivity with multiple PDNs, the steps 1 to 9 are repeated for each PDN the UE is connected to.

For UE-requested PDN disconnection procedure, steps 1 to 9 are performed for the PDN that the UE requested disconnection from.

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

This procedure applies to the Non-Roaming (Figure 4.2.2-1), Roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the non-3GPP access and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF. In the Roaming and LBO cases, the 3GPP AAA Proxy serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN. In the non-roaming case, the vPCRF is not involved at all.

1) The UE sends a MIPv4 Registration Request (RRQ) (MN-NAI, Home Address, Home Agent Address, Care-of Address, lifetime = 0) message to the Foreign Agent (FA) in the Trusted Non-3GPP Access Network with lifetime value set to zero, indicating de-registration. The MN-NAI identifies the UE. The Home Address includes UE Home IP addresses, the Home Agent Address contains the IP address of Home Agent. Care-of Address indicates the CoA used by the UE for the binding.

2) The Trusted Non-3GPP Access Network initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [19]. The Trusted Non-3GPP Access Network no longer applies QoS policy to traffic flows for this UE.

3) The FA relays this MIPv4 RRQ (MN-NAI, lifetime = 0) message to the PDN GW.

4) The selected PDN GW obtains Authentication and Authorization information from the AAA/HSS.

5) The PDN GW informs the 3GPP AAA Server of the PDN disconnection. If the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server notifies the HSS as described in clause 12.1.2.

6) The PDN GW deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP-CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [19].

7) The PDN GW sends a MIPv4 Registration Reply (RRP) (MN-NAI, Home Address, Home Agent Address, Lifetime=0) message to the FA.

8) Any time after step 7, the FA relays this MIPv4 RRP (MN-NAI, Home Address, Home Agent Address, Lifetime=0) message to the UE.

9) After step 7, Non-3GPP specific resource release procedure is executed.

6.4.4 Network Initiated Detach Procedure with MIPv4 FACoA

Trusted Non-3GPP Access Network initiated detach procedure with MIPv4 FACoA Mode is illustrated in Figure 6.4.4-1. The Trusted Non-3GPP Access Network can initiate this procedure due to administration reason or detecting the UE's leaving by, e.g. Link-layer event specific to the access technology (see RFC 3543 [25] for more information).

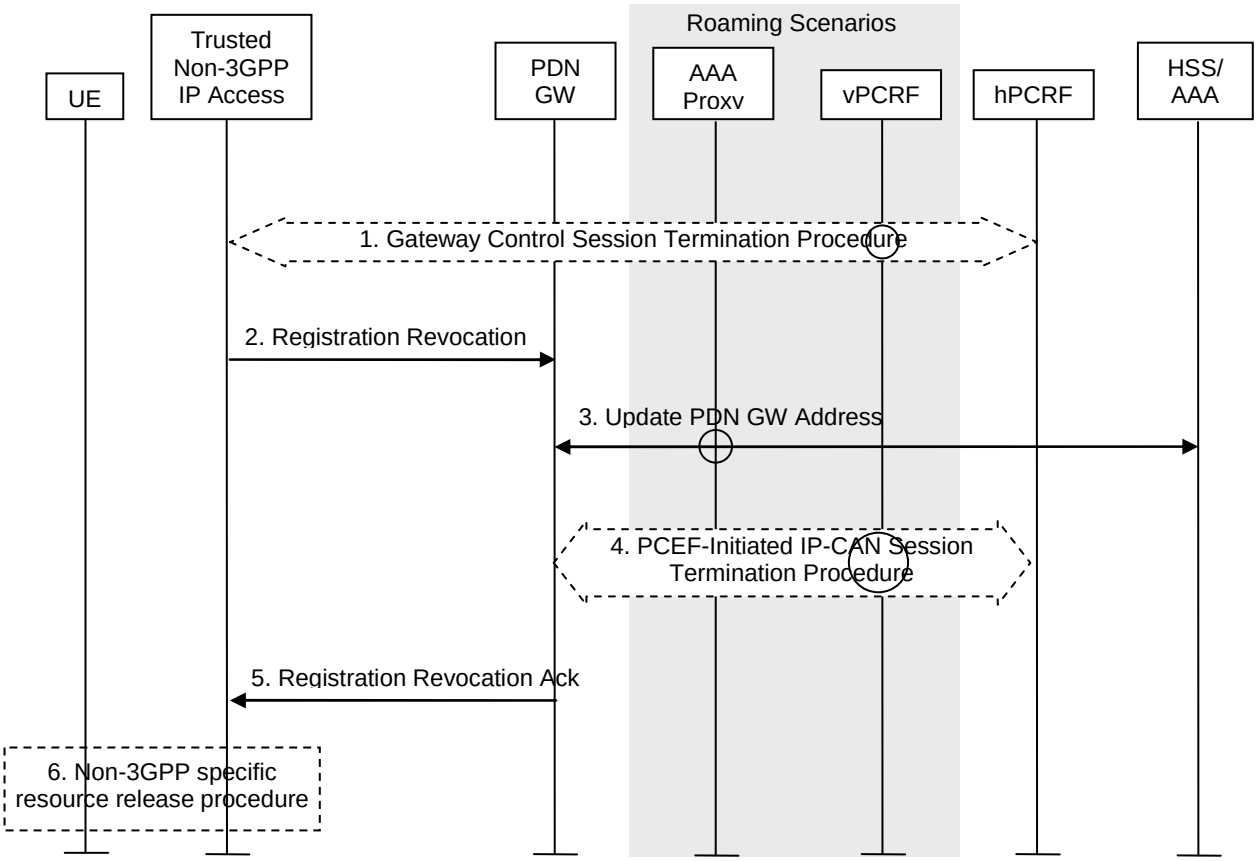


Figure 6.4.4-1: Trusted Non-3GPP Access Network initiated detach procedure with MIPv4 FACoA

NOTE: AAA proxy and vPCRF are only used in the case of home routed roaming (Figure 4.2.3-1) and local breakout (Figure 4.2.3-4).

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

This procedure applies to the Non-Roaming (Figure 4.2.2-1), Roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the non-3GPP access and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF. In the Roaming and LBO cases, the 3GPP AAA Proxy serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN. In the non-roaming case, the vPCRF is not involved at all.

1) The Trusted Non-3GPP Access Network detects the UE's leaving and initiates a Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [19]. The Trusted Non-3GPP Access Network no longer applies QoS policy to traffic flows for this UE.

2) The FA sends a Registration Revocation (Home Address, Home Agent Address, Care-of Address) message (see RFC 3543 [25]) to the PDN GW.

3) The PDN GW informs the 3GPP AAA Server of the PDN disconnection. If the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server notifies the HSS as described in clause 12.1.2.

4) The PDN GW deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP-CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [19].

5) The PDN GW sends a Registration Revocation Ack (Home Address) message (see RFC 3543 [25]) to the FA.

6) The Trusted Non-3GPP Access Network executes a specific resource release procedure.

6.4.5 HSS/AAA-initiated detach procedure with MIPv4 FACoA

HSS/AAA-initiated detach procedure with MIPv4 FACoA Mode is illustrated in Figure 6.4.5-1. The HSS can initiate the procedure e.g. when the user's subscription is removed. The 3GPP AAA Server can initiate the procedure, e.g. instruction from O&M, timer for re-authentication/re-authorization expired.

If the HSS/AAA-initiated detach procedure has been initiated to delete the UE from the Evolved Packet Core, the HSS/AAA server shall initiate the detach procedure for each of the access systems to which the UE is registered.

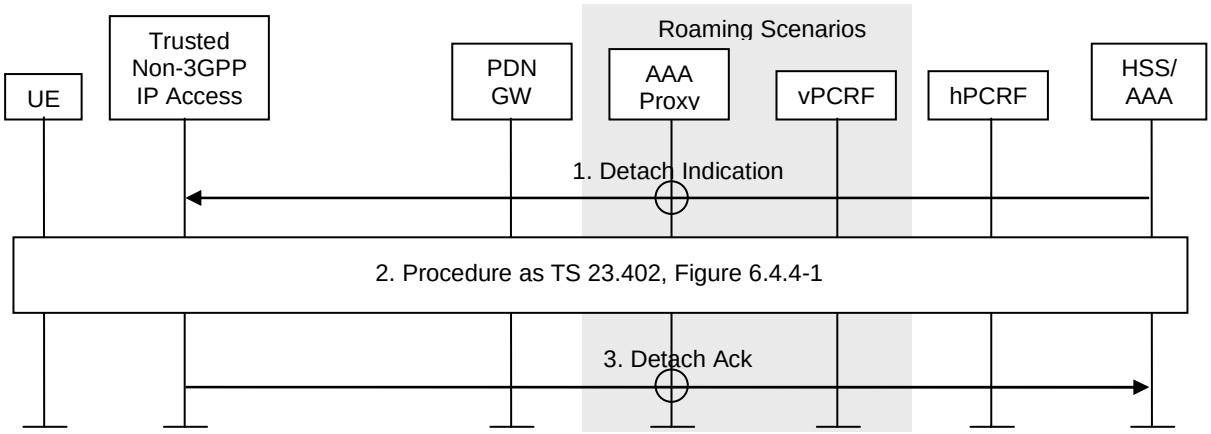


Figure 6.4.5-1: HSS/AAA-initiated detach procedure with MIPv4 FACoA

NOTE 1: AAA proxy and vPCRF are only used in the case of home routed roaming (Figure 4.2.3-1) and local breakout (Figure 4.2.3-4).

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

This procedure applies to the Non-Roaming (Figure 4.2.2-1), Roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the non-3GPP access and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the

hPCRF. In the Roaming and LBO cases, the 3GPP AAA Proxy serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN. In the non-roaming case, the vPCRF is not involved at all.

1) The HSS/AAA sends a detach indication message to the FA in the Trusted Non-3GPP Access Network to detach a specific UE.

2) This includes the procedure in figure 6.4.4-1.

3) The FA sends a Detach Ack message to the 3GPP AAA Server. If the detach procedure was initiated from the 3GPP AAA Server and if the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server communicates the HSS as described in clause 12.1.2. If the detach procedure was initiated by HSS, the 3GPP AAA Server replies to the HSS as described in clause 12.1.3.

NOTE 2: The HSS/AAA may also send a detach indication message to the PDN GW. The PGW does not remove the MIPv4 tunnels, since the MIPv4 FA in the non-3GPP access is responsible for removing the MIPv4 tunnels. The PDN GW acknowledges the receipt of the detach indication message to the 3GPP AAA Server.

6.5 Detach and PDN Disconnection for S2c in Trusted Non-3GPP IP Access

6.5.1 General

This clause is related to the cases where at least one DSMIPv6 PDN disconnection procedure is performed. In case of detach the DSMIPv6 PDN disconnection is executed for all the existing PDNs connections, while in the case of disconnecting a single PDN connection the DSMIPv6 PDN disconnection is executed only for the individual PDN connection.

The DSMIPv6 PDN disconnection procedure is on a per PDN basis and allows:

- the UE to inform the network that it requests to release a S2c based PDN connection, and

- the network to inform the UE that a S2c based PDN connection is disconnected.

The UE may be disconnected from a PDN either explicitly or implicitly:

- Explicit PDN disconnection: The network or the UE explicitly requests PDN disconnection and signal with each other.

- Implicit PDN disconnection: The network disconnects the UE from a PDN, without notifying the UE. This is typically the case when the network presumes that it is not able to communicate with the UE, e.g. due to radio conditions.

Three PDN disconnection procedures are provided when the UE accesses the EPS through S2c:

- UE-Initiated PDN disconnection Procedure;

- AAA/HSS-initiated Detach Procedure;

- PDN GW-initiated PDN disconnection Procedure.

6.5.2 UE-initiated PDN disconnection Procedure

The PDN disconnection procedure when initiated by the UE is illustrated in Figure 6.5.2-1. In case of detaching the UE from EPS, the procedure defined in this clause must be repeated for each PDN.

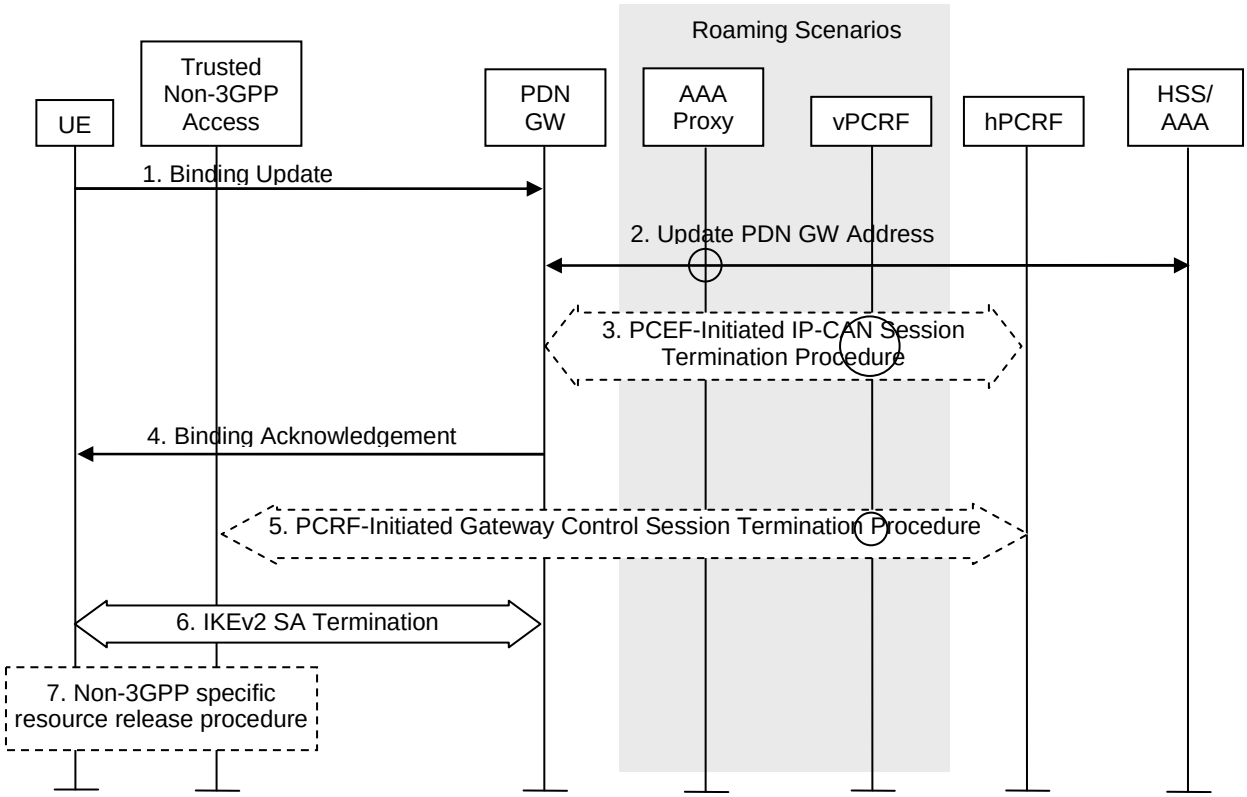


Figure 6.5.2-1: UE-initiated DSMIPv6 PDN disconnection procedure in Trusted Non-3GPP Access Network

Non-roaming (Figure 4.2.2-2), home routed roaming (Figure 4.2.3-3) and Local Breakout (Figure 4.2.3-4) cases are supported by this procedure. The AAA proxy and vPCRF are only used in the case of home routed roaming and Local Breakout. In non-roaming scenarios, the AAA proxy and vPCRF are not involved.

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

1. If the UE wants to terminate a S2c session for a given PDN, it shall send a de-registration Binding Update (HoA, Lifetime=0) as specified in RFC 5555 [10].

2. The PDN GW informs the 3GPP AAA Server of the PDN disconnection. If the PDN GW is in the VPLMN, signalling may be routed via a 3GPP AAA Proxy in the VPLMN. If the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server notifies the HSS as described in clause 12.1.2.

3. If there is an active PCC session for the UE, the PDN GW shall execute a PCEF-Initiated IP-CAN session Termination Procedure with the PCRF as specified in TS 23.203 [19].

4. The PDN GW shall send a Binding Acknowledgement as specified in RFC 5555 [10]

5. The PCRF shall remove all active QoS rules which refer to the Home Address. The PCRF executes a PCRF-Initiated Gateway Control Session Termination Procedure with the Trusted Non-3GPP IP Access as specified in TS 23.203 [19]. The Trusted Non-3GPP IP Access will no longer perform any QoS policy or gateway control function associated with the terminated session.

   This step describes the case where there are no QoS rules remaining for that UE at the trusted non-3GPP access and thus the GW control session termination is executed. In case there are still active QoS rules for the UE, the GW control session termination procedure is replaced by a QoS rule provision procedure.

6. The UE terminates the IKEv2 security association for the given PDN as defined in RFC 5996 [9]

7. After IKEv2 SA termination, non-3GPP specific resource release procedure may be executed.

6.5.3 HSS / AAA-initiated Detach Procedure

The Detach procedure when initiated by the HSS/AAA is illustrated in Figure 6.5.3-1. The Detach procedure defined in this clause must be repeated for each PDN.

If the HSS/AAA-initiated detach procedure has been initiated to delete the UE from the Evolved Packet Core, the HSS/AAA server shall initiate the detach procedure for each of the access systems to which the UE is registered.

In the explicit detach procedure steps 2, 3 and 7 of Figure-6.5.3-1, are performed as illustrated. In the implicit detach, steps 2, 3 and 7 of Figure 6.5.3-1, are omitted.

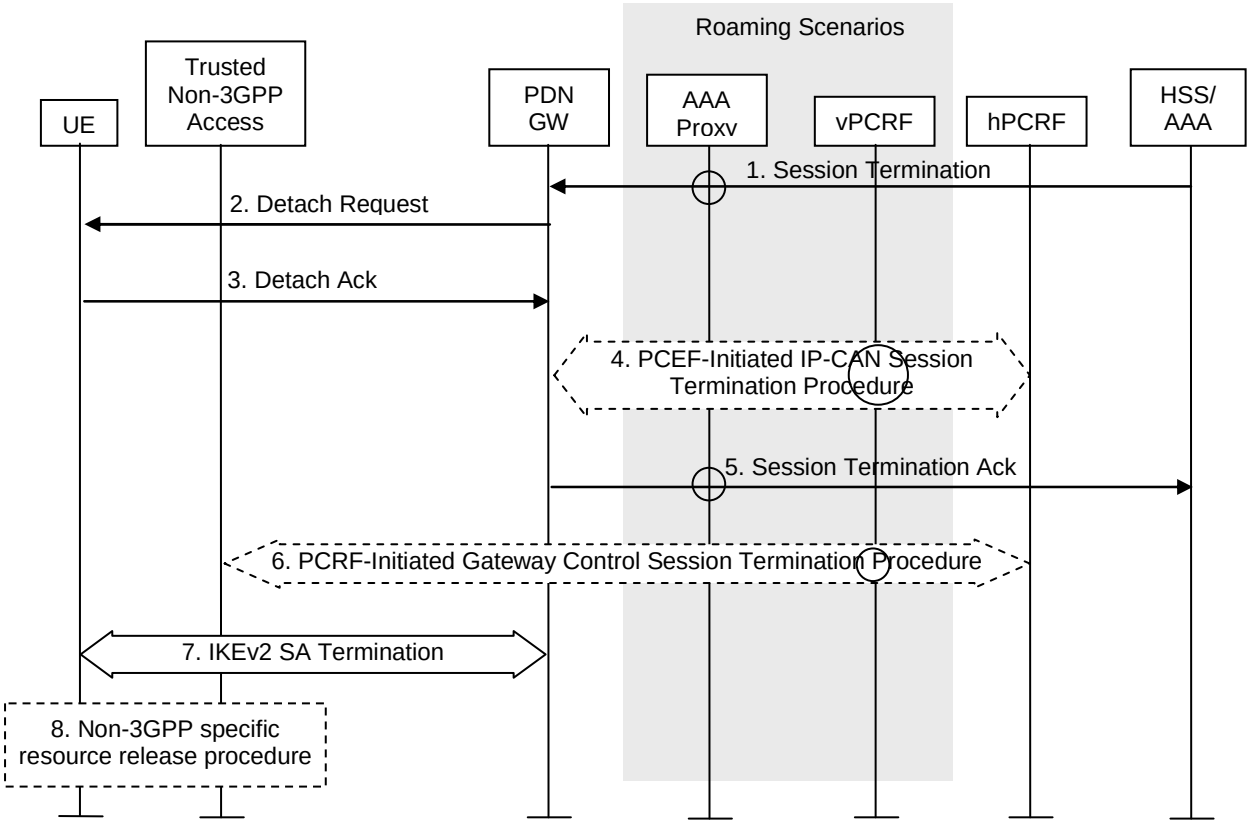


Figure 6.5.3-1: AAA/HSS-initiated S2c detach procedure in Trusted Non-3GPP Access Network

Non-roaming (Figure 4.2.2-1), home routed roaming (Figure 4.2.3-2) and Local Breakout (Figure 4.2.3-4) cases are supported by this procedure. The 3GPP AAA proxy and vPCRF are only used in the case of home routed roaming and Local Breakout. In non-roaming scenarios, the 3GPP AAA proxy and vPCRF are not involved.

If dynamic policy provisioning is not deployed, the optional steps 4 and 6 do not occur. Instead, the PDN GW may employ static configured policies.

1. If the HSS/AAA wants to request the immediate termination of a S2c session for a given UE and a given PDN, it shall send a Session Termination message to the PDN GW. In the roaming case signalling may be routed via a 3GPP AAA Proxy in the VPLMN.

2. The PDN GW shall send a detach request message.

3. The UE shall acknowledge the detach request.

NOTE 1: How the detach request and acknowledge messages are implemented is a stage 3 detail.

4. If there is an active PCC session for the UE, the PDN GW shall execute a PCEF-Initiated IP-CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [19].

5. The PDN GW shall acknowledge the termination of the S2c session to the AAA. If the detach procedure was initiated from the 3GPP AAA Server and if the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server communicates the HSS as described in clause 12.1.2. If the detach procedure was initiated by HSS, the 3GPP AAA Server replies to the HSS as described in clause 12.1.3.

6. The PCRF shall remove any active QoS Policy rule which is referred to the Home Address. The PCRF executes a PCRF-Initiated Gateway Control Session Termination Procedure with the Trusted Non-3GPP IP Access as specified in TS 23.203 [19]. The Trusted Non-3GPP IP Access will no longer perform any QoS policy or gateway control function associated with the terminated session.

   This step describes the case where there are no QoS rules remaining for that UE at the trusted non-3GPP access and thus the GW control session termination is executed. In case there are still active QoS rules for the UE, the GW control session termination procedure is replaced by a QoS rule provision procedure.

7. The PDN GW or the UE terminates the IKEv2 security association for the given PDN as defined in RFC 5996 [9].

8. After IKEv2 SA termination, non-3GPP specific resource release procedure may be executed.

NOTE 2: The HSS/AAA may (e.g. when STa is implemented and/or based on operator's policies) also send a detach indication message to the non-3GPP access. The HSS/AAA should wait to receive acknowledgement(s) from PGW(s) before sending the detach indication to the non-3GPP access. The non-3GPP access detaches the UE and acknowledges the receipt of the detach indication message to the 3GPP AAA Server.

6.5.4 PDN GW-initiated PDN Disconnection Procedure

The PDN Disconnection procedure when initiated by the PDN GW is illustrated in Figure 6.5.4-1.

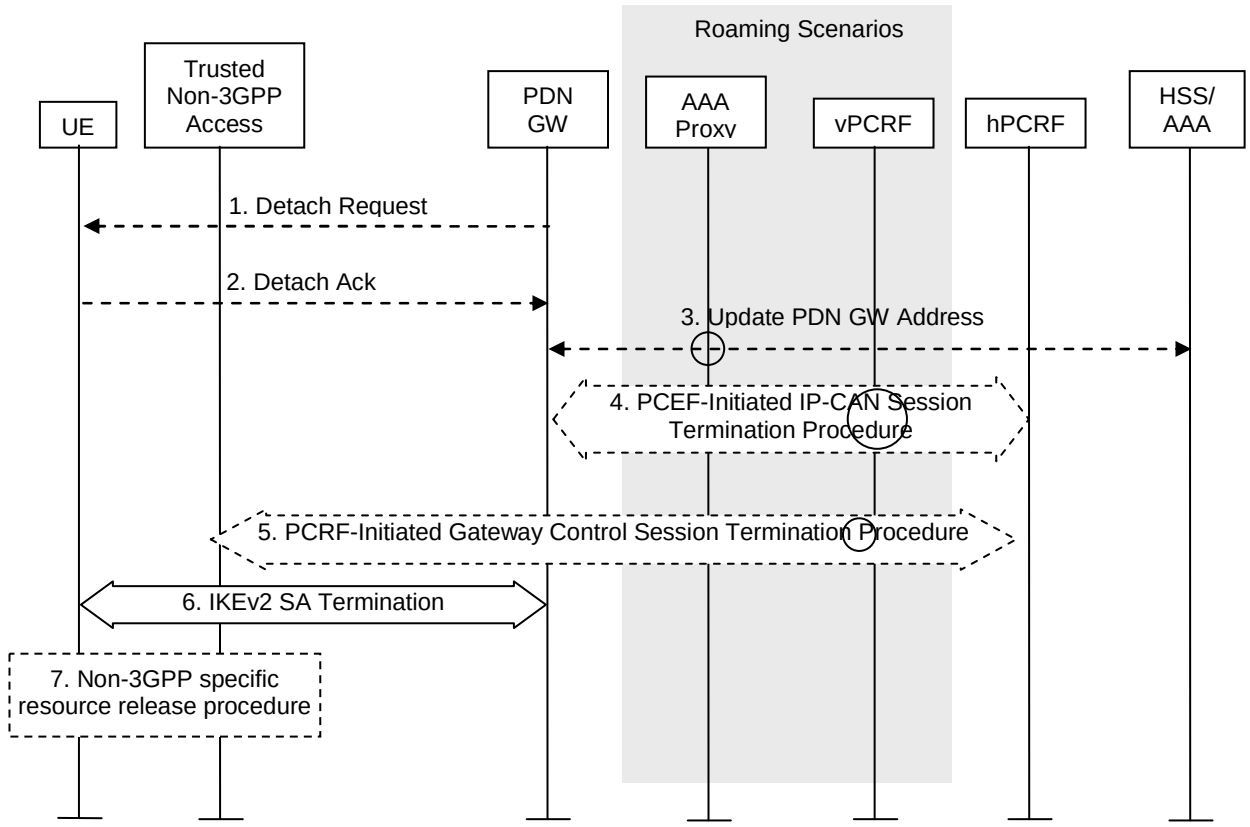


Figure 6.5.4-1: PDN GW- initiated PDN Disconnection S2c procedure in Trusted Non-3GPP Access Network

Non-roaming (Figure 4.2.2-1), home routed roaming (Figure 4.2.3-2) and Local Breakout (Figure 4.2.3-4) cases are supported by this procedure. The 3GPP AAA proxy and vPCRF are only used in the case of home routed roaming and Local Breakout. In non-roaming scenarios, the 3GPP AAA proxy and vPCRF are not involved.

If dynamic policy provisioning is not deployed, the optional step 3 does not occur. Instead, the PDN GW may employ static configured policies.

If the PDN GW-initiated PDN Disconnection Procedure is triggered by the UE binding lifetime expiration (Implicit PDN disconnection procedure), steps 1 and 2 may be omitted.

1. In the explicit detach procedure the PDN GW shall send a detach request message.
2. In the explicit detach procedure, the UE shall acknowledge the detach request.

NOTE: How the detach request and acknowledge messages are implemented is a stage 3 detail.

3. The PDN GW informs the 3GPP AAA Server of the PDN disconnection. If the PDN GW is in the VPLMN, signalling may be routed via a 3GPP AAA Proxy in the VPLMN. If the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server notifies the HSS as described in clause 12.1.2.
4. If there is an active PCC session for the UE, the PDN GW shall execute a PCEF-Initiated IP-CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [19].
5. The PCRF shall remove all active QoS rules which refer to the Home Address. The PCRF executes a Gateway Control and QoS Rules Provision procedure or, if this is the last PDN Connection for the UE, a PCRF-Initiated Gateway Control Session Termination Procedure with the Trusted Non-3GPP IP Access as specified in TS 23.203 [19]. The Trusted Non-3GPP IP Access will no longer perform any QoS policy or gateway control function associated with the terminated PDN Connection.
6. The PDN GW or the UE may terminate the IKEv2 security association for the given PDN as defined in RFC 5996 [9].
7. After IKEv2 SA termination, non-3GPP specific resource release procedure may be executed.

6.6 Network-initiated Dynamic PCC

6.6.1 Network-initiated Dynamic PCC on S2a

If dynamic PCC is deployed, the procedure given in Figure 6.6.1-1 is used by the PCRF to provision rules to the Trusted non-3GPP IP access and for the Trusted non-3GPP IP access to enforce the policy by controlling the resources and configuration in the trusted non-3GPP access. The access specific procedure executed in the trusted non-3GPP access is not within the scope of this specification.

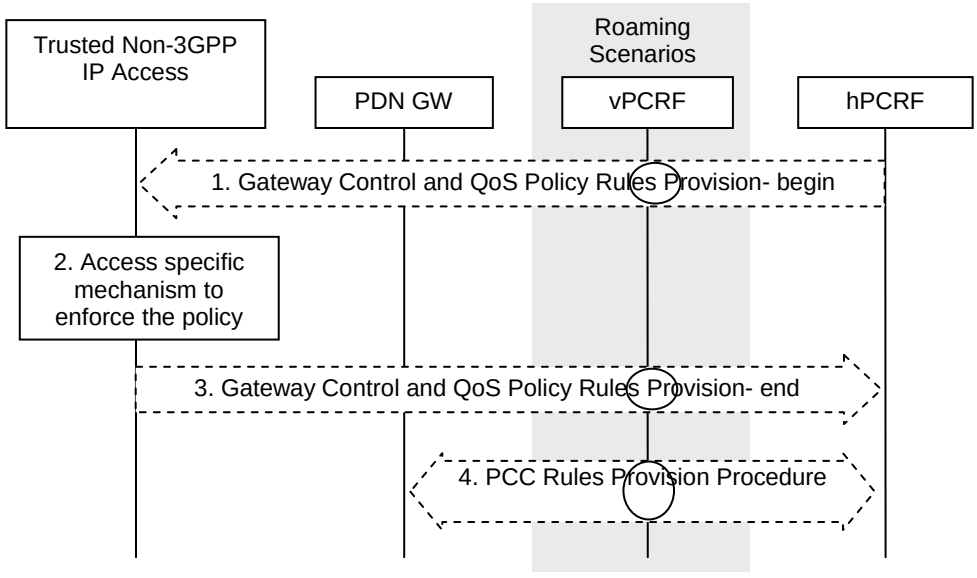


Figure 6.6.1-1: Network-initiated dynamic policy control procedure in Trusted Non-3GPP IP Access for S2a

This procedure concerns both the non-roaming (as Figure 4.2.2-1) and roaming case (as Figure 4.2.3-1). In the roaming case, the vPCRF in the VPLMN forwards messages between the Trusted Non-3GPP IP Access and the hPCRF in the HPLMN. In the case of Local Breakout (as Figure 4.2.3-4), the vPCRF forwards messages sent between the PDN GW and the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

1. The PCRF initiates the Gateway Control and QoS Policy Rules Provision Procedure specified in TS 23.203 [19] by sending a message with the QoS rules and Event Trigger information to the Trusted non-3GPP access network.

2. The Trusted Non-3GPP IP Access enforces the rules provisioned to it, and establish all necessary resources and configuration in the non-3GPP access system, e.g. initiate a dedicated bearer activation, modification or deactivation, if supported. The details of this step are out of the scope of this specification.

3. The Trusted Non-3GPP IP Access responds to the PCRF indicating its ability to enforce the rules provisioned to it in Step 1 and thus completing the GW Control and QoS Rules Provision procedure started in step A.1.

4. The PCRF initiates the PCC Rules Provision Procedure as specified in TS 23.203 [19]. The PCRF provides updated PCC rules to the PCEF for enforcement by means of an PCC Rules Provision procedure specified in TS 23.203 [19].

NOTE: Step 4 may occur before step 1 or performed in parallel with steps 1-3 if acknowledgement of resource allocation is not required to update PCC rules in PCEF. For details please refer to TS 23.203 [19].

6.6.2 Network-initiated Dynamic PCC for S2c over Trusted Non-3GPP IP Access

This clause is related to the case when network-initiated dynamic resource allocation is supported, and it is utilized for the S2c traffic flow aggregates.

The procedure described in this clause may also be used subsequent to the S2c Attach procedure described in clause 6.3.

In this case, the PCRF may push specific PCC rules to the PDN GW and QoS Policy rules to the Trusted Non-3GPP Access system, in case the Access System supports PCC.

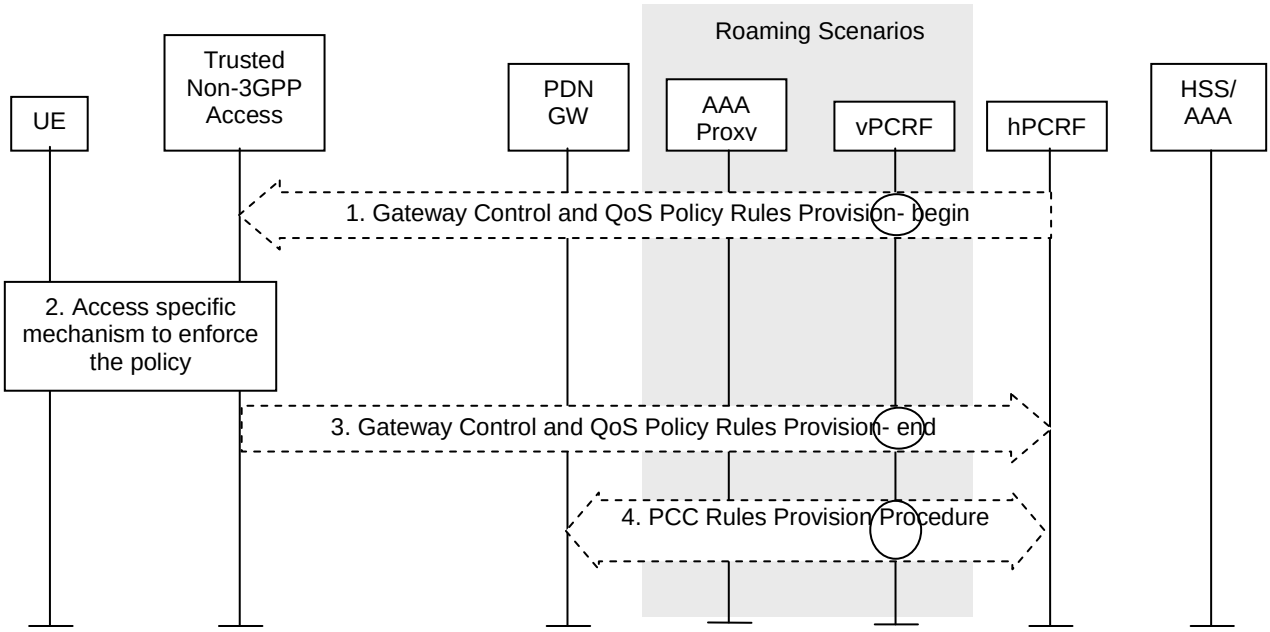


Figure 6.6.2-1: Network-initiated dynamic policy control for S2c over Trusted Non-3GPP IP Access

This procedure concerns both the non-roaming (as Figure 4.2.2-2) and roaming case (as Figure 4.2.3-3). In the roaming case, the vPCRF in the VPLMN forwards messages between the Trusted Non-3GPP IP Access and the hPCRF in the

HPLMN. In the case of Local Breakout (as Figure 4.2.3-4), the vPCRF forwards messages sent between the PDN GW and the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

Steps 1-4 are the same as in steps 1-4 in clause 6.6.1. Step 4 may be skipped in case the PCC rules at the PDN GW are already up-to-date.

6.7 UE-initiated Resource Request and Release

6.7.1 UE-initiated Resource Request and Release on S2a

This procedure is applicable to both PMIPv6 on S2a and DSMIPv6 on S2c.

This clause is related to the case when UE-initiated resource request and release is supported in the Trusted Non-3GPP IP Access, and it is utilized for the S2a/S2c traffic flow aggregates.

Figure 6.7.1-1 depicts the procedure for the roaming and non-roaming cases.

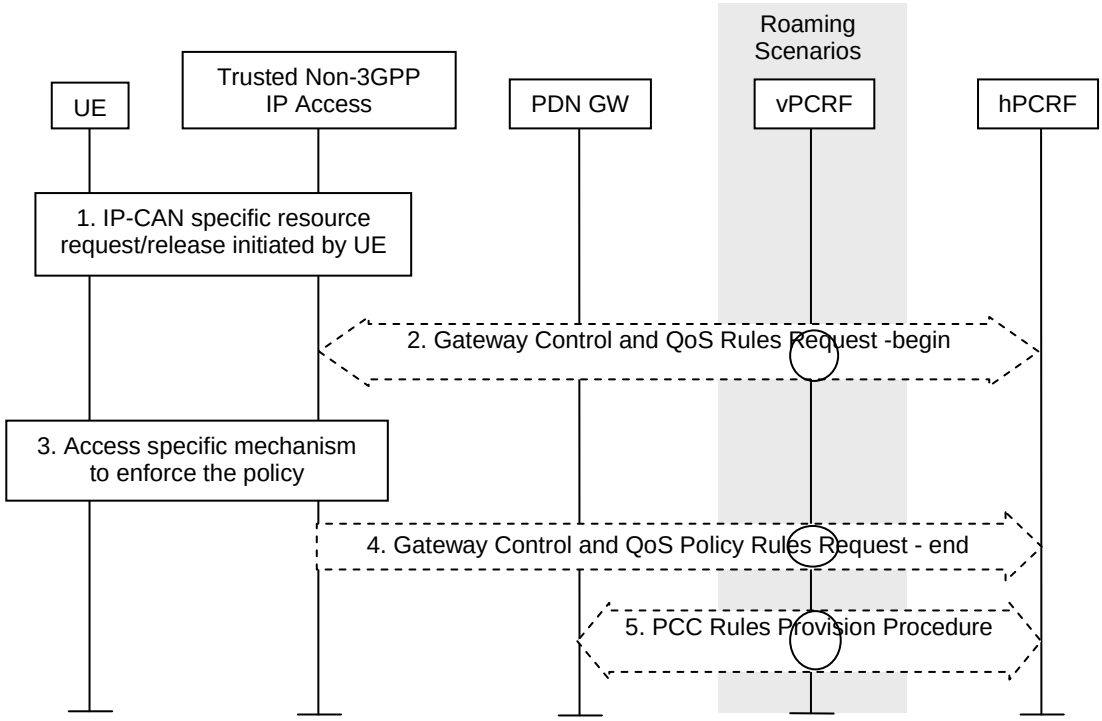


Figure 6.7.1-1: UE-initiated resource request/release with S2a or S2c

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

Both the roaming (Figure 4.2.3-1) and non-roaming (Figure 4.2.2-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the trusted non-3GPP IP access in the VPLMN. The vPCRF receives the Acknowledgment from the trusted non-3GPP IP access and forwards it to the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

1. The trusted non-3GPP IP access receives an IP-CAN specific resource allocation or resource release request initiated by the UE.

2. The trusted non-3GPP IP access initiates the Gateway Control and QoS Policy Rules Request Procedure as specified in TS 23.203 [19]. The trusted non-3GPP IP access provides the UE request or release of resources as an Event Report. The PCRF makes a PCC decision as a result of the Gateway Control and QoS policy request and provides the updated QoS Rules to the trusted non-3GPP IP access.

3. An IP-CAN specific resource allocation or resource release procedure may be triggered by the enforcement of the received policy rules. In this step, a response for the resource request/release is sent to the UE.

4. The trusted non-3GPP IP access indicates to the PCRF whether the requested QoS Policy Rules Provision could be enforced or not and thus completing the GW Control and QoS Rules Provision procedure.

5. The PCRF initiates the Policy and Charging Rules Provision Procedure as specified in TS 23.203 [19] to update the PCC rules in the PDN GW. The updated PCC Rules and Event Triggers include any adjustments to resources due to the decision taken in step 2.

NOTE: Step 5 may be performed in parallel with Steps 2-4 if acknowledgement of resource allocation is not required at the PCRF to update PCC rules in PCEF. For details please refer to TS 23.203 [19].

Step 2 may be omitted if the Trusted non-3GPP IP access has already received authorisation for the UE's request from the PCRF, e.g. QoS rules downloaded at handover.

6.7.2 UE-initiated Resource Request for S2c over Trusted Non-3GPP IP Access

The procedure is specified in clause 6.7.1.

6.8 UE-initiated Connectivity to Additional PDN

6.8.1 UE-initiated Connectivity to Additional PDN with PMIPv6 on S2a

6.8.1.0 General

This procedure is used to request for connectivity to an additional PDN over trusted non-3GPP access with PMIPv6 on S2a when the UE already has active PDN connections over such trusted access. This procedure is also used to request for connectivity to an additional PDN over trusted non-3GPP access with PMIPv6 on S2a when the UE is simultaneously connected to such trusted access and a 3GPP access, and the UE already has active PDN connections over both the accesses.

The procedure is also used for the re-establishment of existing PDN connectivity after the UE performed the handover from 3GPP accesses for the first PDN connection by the Attach procedure.

6.8.1.1 Non-Roaming, Home Routed Roaming and Local Breakout Case

Establishment of connectivity to an additional PDN over trusted access with S2a is supported only for the accesses that support such feature and the UEs that have such capability.

PMIPv6 specification, RFC 5213 [8], is used to setup an IP connectivity between the trusted non-3GPP IP access and the EPC during initial attach. In both roaming and non-roaming cases, S2a is present. It is assumed that MAG exists in the trusted non-3GPP IP access.

There can be more than one PDN connection per APN if both the MAG and the PDN GW support that feature. When multiple PDN connections to a single APN are supported, during the establishment of a new PMIP tunnel, the MAG creates and sends a PDN Connection identity to the PDN GW. The PDN connection identity is unique in the scope of the UE and the APN and within a Trusted non-3GPP access network, i.e. the MN-ID, the APN, and the PDN connection identity together identify a PDN connection within a Trusted non-3GPP access network. In order to be able to identify a specific established PDN connection, both the MAG and the PDN GW shall store the PDN Connection identity. Sending the PDN connection identity is an indication that the MAG supports multiple PDN connections to a single APN and the PDN GW shall be able to indicate if it supports multiple PDN connections to a single APN.

NOTE 1: When multiple PDN connections to a single APN are used, the MN-ID and the APN together is not enough to identify the PDN connection. Therefore between the UE and MAG an access network specific mechanism is needed to differentiate the PDN connections to the same APN. Differentiating the PDN connections within one access is needed in order to operate on the correct PDN connection, e.g. when the PDN connection is removed. Differentiating the PDN connections across accesses, e.g. during handover, is not needed. The specification of such a mechanism is out of scope of 3GPP.

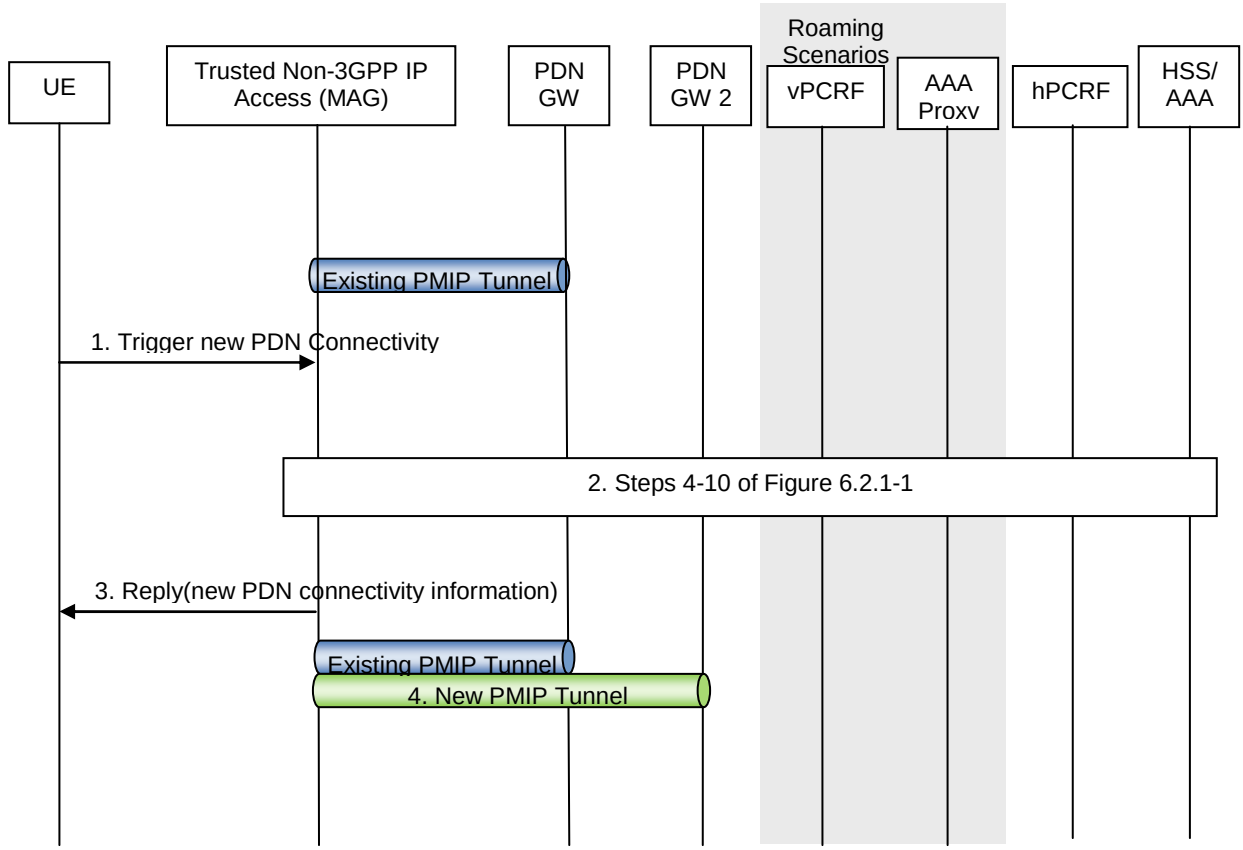


Figure 6.8.1.1-1: Additional PDN connectivity with Network-based MM mechanism over S2a for non-roaming and roaming

The steps in the procedure which are marked as optional occur only if dynamic policy provisioning has been deployed.

In the roaming case, messages are forwarded between the Trusted Non-3GPP IP Access and the hPCRF via the vPCRF. In the case of LBO, messages are forwarded between the PDN GW and the hPCRF via the vPCRF also. Further, in the case of LBO, messages between the PDN GW and the 3GPP AAA Server are sent via the 3GPP AAA Proxy.

1) When the UE wishes to connect to an additional PDN, it sends a trigger indicating that connectivity with that specific PDN is desired. The UE provides information about the new PDN by using an APN. When multiple PDN connections to a single APN are supported then some additional access specific mechanism is needed between the UE and the MAG to differentiate the PDN connections towards the same APN. If supported by the non-3GPP access, the UE may send Protocol Configuration Options in this step using access specific mechanisms. The Protocol Configuration Options provided by the UE may include the user credentials for PDN access authorization. The UE triggers the re-establishment of existing PDN connectivity after the handover by providing a Request Type indicating "Handover" on accesses that support the indication.

NOTE 2: The definition of the trigger that the UE provides to the access network (MAG) is out of scope of 3GPP.

2) At this step the trusted non-3GPP IP access performs PDN GW selection as described in clause 4.5.1. Steps 4 to 10 according to clause 6.2.1 are executed with PDN GW2 instead of PDN GW1.

3) The trusted non-3GPP IP access system sends the reply message to the UE with the allocated IP address from the PDN that the UE indicated at step 1. If supported by the non-3GPP access, the Protocol Configuration Options provided by the PDN GW in step 2 are returned to the UE in this step using access specific mechanisms. Since UE requested for additional PDN connectivity, the UE configures the IP address received from the MAG without deleting its configuration for connectivity with any other previously established PDN. For handover, the UE is returned the IP address the UE obtained before the handover during PDN connectivity establishment.

NOTE 3: The definition of the message used to carry the new connectivity information to the UE is out of scope of 3GPP.

4) The PMIPv6 tunnel is thus set up between the Trusted Non-3GPP IP Access and the PDN GW corresponding to the requested additional PDN while maintaining tunnels previously established for other PDNs.

6.8.1.2 Chained PMIP-based S8-S2a Roaming Case

This clause defines the UE-initiated Connectivity to Additional PDN for PMIP-based S8-S2a chaining. This procedure also applies for PMIP-based S8-S2b chaining.

Multiple PDN connections to a single APN can be established if it is supported by the MAG, the Serving GW and the PDN GW. When multiple PDN connections to a single APN are supported, during the establishment of a new PDN connection, the use of PDN connection identity is used as specified in clause 6.8.1.1 and the Serving GW shall forward the PDN connection identity between the concatenated PMIP tunnels.

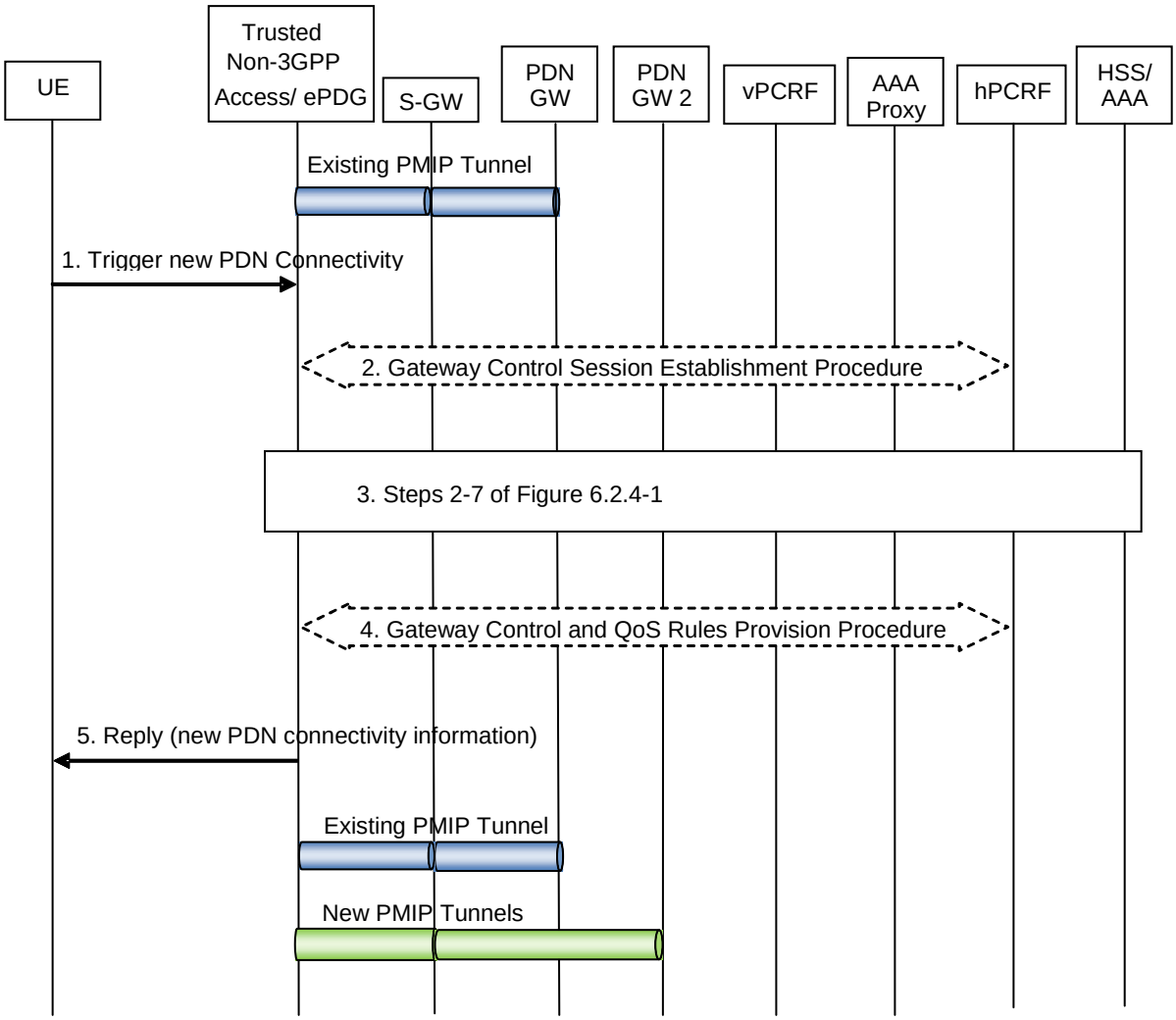


Figure 6.8.1.2-1: Additional PDN connectivity for chained PMIP-based S8-S2a/b roaming scenarios

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

The gateway control signalling in steps 2 and 4 between the gateway and PCRF occur only for Trusted Non-3GPP IP Accesses.

1) When the UE wishes to connect to an additional PDN, it sends a trigger according to step 1 of clause 6.8.1.1 (Figure 6.8.1.1-1).

2) The non-3GPP access gateway initiates the Gateway Control Session Establishment Procedure with the hPCRF by way of the vPCRF, as specified in TS 23.203 [19].

3) Steps 2 to 7 according to clause 6.2.4 (Figure 6.2.4-1) are executed with PDN GW2 instead of PDN GW1.

4) In case the QoS rules have changed, the hPCRF by way of the vPCRF updates the QoS rules at the non-3GPP access gateway by initiating the GW Control Session Modification Procedure, as specified in TS 23.203 [19].

5) The trusted non-3GPP access system or ePDG sends the reply message to the UE according to step 3 of clause 6.8.1.1 (Figure 6.8.1.1-1). If supported by the trusted non-3GPP access system, the Protocol Configuration Option provided by the PDN GW in step 3 are returned to the UE in this step using access specific mechanisms.

6.8.2 UE-initiated Connectivity to Additional PDN with MIPv4 FACoA on S2a

This procedure is used to request for connectivity to an additional PDN over trusted non-3GPP access with MIPv4 FACoA on S2a when the UE already has active PDN connections over such trusted access. This procedure is also used to request for connectivity to an additional PDN over trusted non-3GPP access with MIPv4 FACoA on S2a when the UE is simultaneously connected to such trusted access and a 3GPP access, and the UE already has active PDN connections over both the accesses.

NOTE: The PDN GW treats each MN-ID+APN as a separate binding and may allocate a new IP address for each binding.

Multiple connections to the same APN is supported for MIPv4 FACoA on S2a as the UE and PDN GW distinguish between connections by means of the UE's distinct home addresses for each connection.

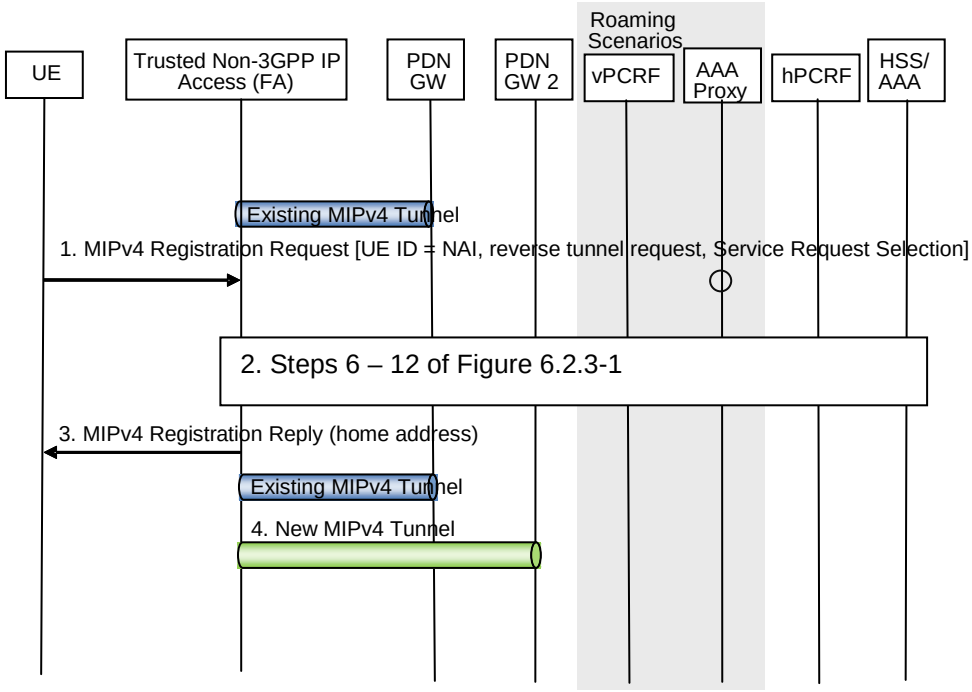


Figure 6.8.2-1: UE-initiated Connectivity to Additional PDN with MIPv4 FACoA on S2a

This procedure applies to the Non-Roaming (Figure 4.2.2-1), Roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the non-3GPP access and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF. In the Roaming and LBO cases, the 3GPP AAA Proxy serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN. In the non-roaming case, the vPCRF is not involved at all.

1) When the UE wishes to connect to an additional PDN, UE sends a Registration Request (RRQ) (MN-NAI, lifetime, APN) RFC 5944 [12] message to the FA as specified in RFC 5944 [12]. Reverse Tunnelling shall be requested. This ensures that all traffic will go through the PDN GW. The RRQ message shall include the NAI-Extension RFC 2794 [34]. The UE may not indicate a specific Home Agent address in the RRQ message, in which case the PDN Gateway/Home Agent is selected by the FA. The UE then receives the IP address of the PDN Gateway in step 3 as part of the Registration Reply (RRP) message. The UE should then include the PDN Gateway address in the Home Agent address field of subsequent RRQ messages. The UE provides information about the new PDN by using an APN as specified in RFC 5446 [39].

2) The trusted non-3GPP IP access performs a PDN GW selection for the new PDN connection. Steps 6-12 of clause 6.2.3 are executed with PDN GW2 instead of PDN GW1. The AAA interactions for obtaining Authentication and Authorization information occur irrespective of whether the UE has a PDN connection with a different APN to the same PDN GW or not.

3) The FA processes the RRP (MN-NAI, Home Address, Home Agent Address, APN) message according to RFC 5944 [12] and sends a corresponding RRP message to the UE.

4) The MIPv4 tunnel is thus set up between the Trusted Non-3GPP IP Access and the PDN GW2 corresponding to the requested additional PDN while maintaining tunnels previously established for other PDNs.

6.8.3 UE-initiated Connectivity to Additional PDN from Trusted Non-3GPP IP Access with DSMIPv6 on S2c

This clause is related to the case when the UE attaches to a Trusted Non-3GPP Access network and host-based mobility management mechanisms are used. Dual Stack MIPv6 [10] is used for supporting mobility over S2c interface. This case describes the scenario when UE adds connectivity to one or more additional PDN at any time after initial attach. Since host-based mobility mechanisms are used, the procedure is similar to the initial attach procedure.

This procedure is also used to request for connectivity to an additional PDN over trusted non-3GPP access with DSMIPv6 on S2c when the UE is simultaneously connected to such trusted access and a 3GPP access, and the UE already has active PDN connections over both the accesses.

NOTE: Based on the MN-ID and APN, the PDN GW may allocate a new IP address/prefix for a new binding.

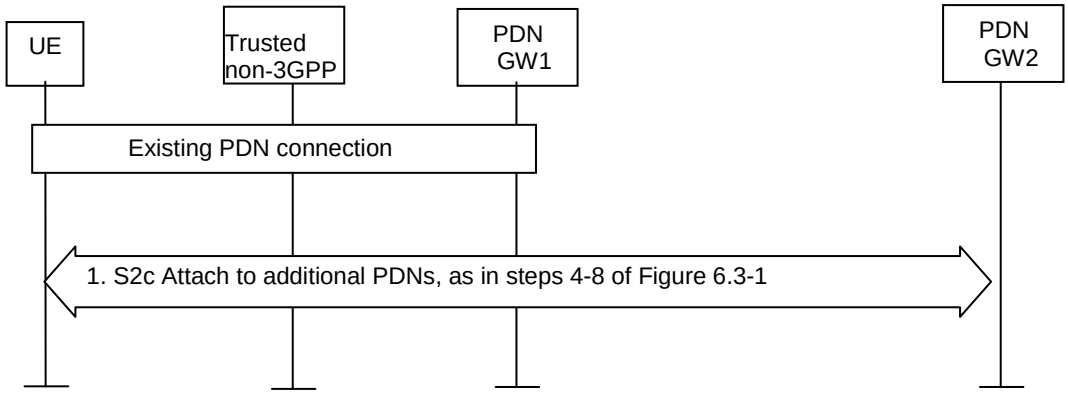


Figure 6.8.3-1: UE-initiated connectivity to multiple PDNs from Trusted Non-3GPP IP Access with DSMIPv6

When the initial attachment is performed, the UE performs procedures described in clause 6.3, Figure 6.3-1, to obtain connectivity with a PDN GW and a specific PDN. If at any time, the UE wants to obtain connectivity with additional PDNs, it repeats steps 4-8 of Figure 6.3-1.

1). The UE performs PDN GW discovery for the new PDN and repeats steps 4-8 of clause 6.3, Figure 6.3-1 for each additional PDN the UE wants to connect to. This step can be performed and be repeated at any time after the initial attach for one or multiple PDNs.

If the UE discovers a different PDN GW for the additional PDN connectivity, when the current PDN GW could provide access to the additional PDN, the PDN GW reallocation procedure may be used, as defined in clause 6.10.

6.9 Void

6.10 PDN GW reallocation upon attach on S2c

The PDN GW reallocation procedure depicted in figure 6.10-1 can be used by the HSS/AAA to force the assignment of a new PDN GW to the UE upon attach with DSMIPv6 in a trusted or untrusted non-3GPP IP access. The decision on whether to trigger PDN GW reallocation is taken by the HSS/AAA according to the principles described in clause 4.5.2.

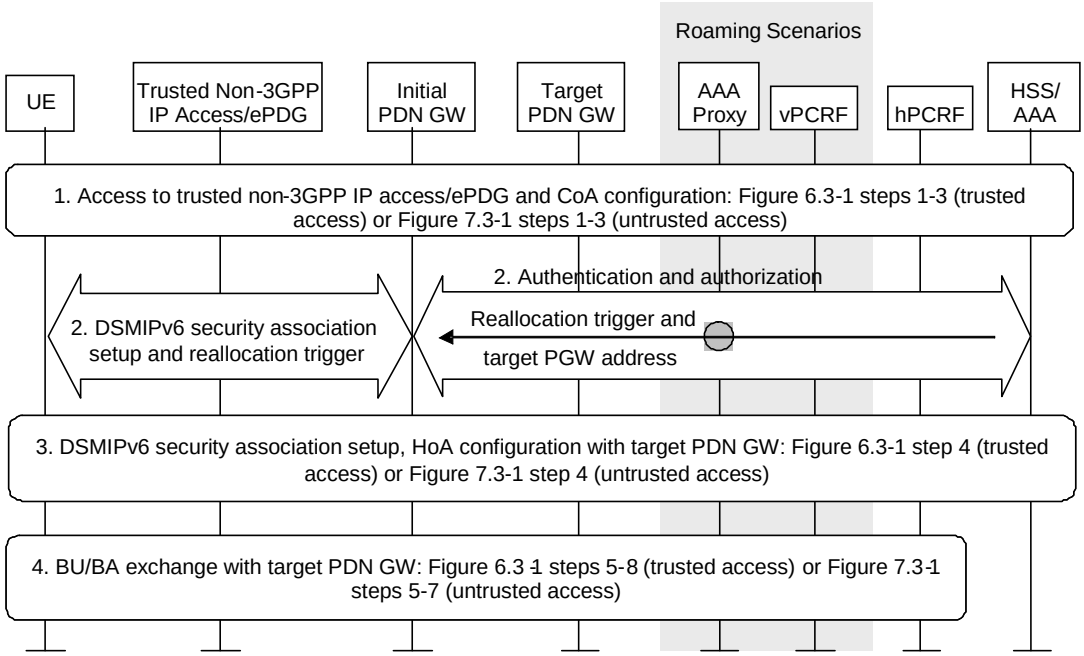


Figure 6.10-1: PDN GW reallocation upon attach on S2c

The following is a detailed description of the involved steps:

1) The UE authenticates in the trusted non-3GPP access, or establishes the IPsec tunnel with the ePDG, and obtains a local IP address to be used as care-of address for DSMIPv6.

2) The UE establishes the DSMIPv6 SA with the initially discovered PDN GW. This implies an AAA exchange with the HSS/AAA. The HSS/AAA triggers the reallocation of the PDN GW and the APN associated with the UE's PDN Connection by piggybacking a reallocation indication and the target PDN GW identity in the AAA exchange. In the signalling from the PDN-GW to the UE, the PDN-GW indicates reallocation, assigns no IPv6 prefix to the UE and includes the IP address of the target PDN GW.

   If the target PDN GW identity is stored in the HSS in form of the IP address, then this IP address can be transferred to the UE directly. If the target PDN GW identity is stored in the HSS in form of the PDN GW FQDN, the initial PDN GW shall derive the IP address of the HA functionality of the target PDN GW from the PDN GW FQDN provided by the AAA server and provide it to the UE.

3) The UE establishes the DSMIPv6 SA with the target PDN GW provided by the network during step 2.

4) The UE performs the DSMIPv6 registration with the target PDN GW.

NOTE 1: In case the UE performs DSMIPv6 bootstrapping for an existing PDN connection, the UE includes its IPv6 Home Address during step 2.

NOTE 2: The DSMIPv6 SA between the UE and the initial PDN GW may be implicitly removed by the UE and the initial PDN GW any time after step 2, before expiry of the SA.

6.11 S2c Bootstrapping via DSMIPv6 Home Link over a Trusted Access

When the UE is connected on a trusted non-3GPP access considered to be DSMIPv6 home link for the UE based on clause 4.5.6, the UE may trigger the establishment of S2c IKEv2 SA, e.g. to optimize future handovers to other accesses using S2c. For each PDN connection, the S2c IKEv2 SA establishment has to be performed separately.

NOTE: A trusted non-3GPP access can be defined as DSMIPv6 Home Link in addition to the 3GPP access.

Once the UE is attached to the PDN over the trusted non-3GPP access, the procedure describing the bootstrapping is in clause 15.1.

6.12 PDN GW initiated Resource Allocation Deactivation

6.12.1 PDN GW initiated Resource Allocation Deactivation with S2a PMIP

This procedure is performed to release all the resources associated with the PDN address, for example, due to IP-CAN session modification requests from the PCRF or due to handover from Non-3GPP to 3GPP. When it is performed for an handover, the connections associated with the PDN address are released, but the PDN address is kept in the PDN GW.

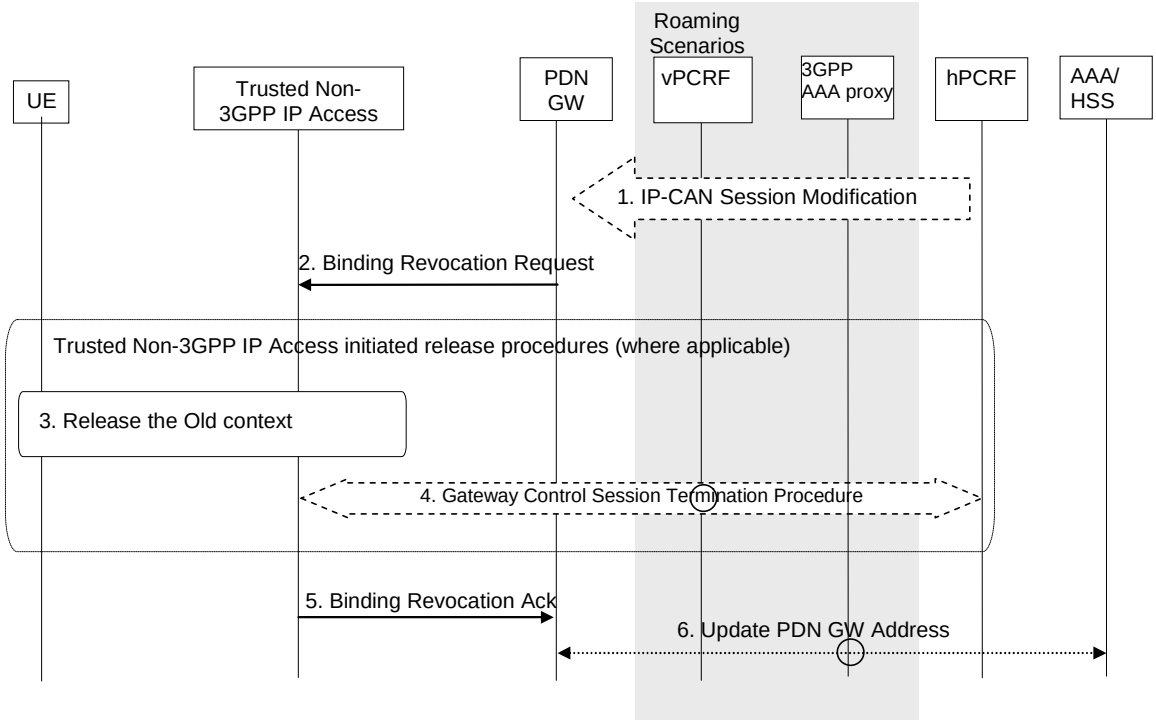


Figure 6.12.1-1: PDN GW Initiated Binding Revocation with S2a PMIP

This procedure applies to the Non-Roaming (Figure 4.2.2-1), Roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the non-3GPP IP access and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

The optional interaction steps between the gateways and the PCRF in the procedures in figure 6.12.1-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

1. If dynamic PCC is deployed, the PDN GW initiated Resource Allocation Deactivation procedure may for example be triggered due to 'IP CAN session Modification procedure', as defined in TS 23.203 [19]. In this case, the resources associated with the PDN connection in the PDN GW are released.

   The PDN GW initiated Resource Allocation Deactivation can also be triggered during handovers from Non-3GPP to 3GPP.

2. The PDN GW sends a Binding Revocation Indication message to the trusted non-3GPP IP access.

3. The resources may be released in the trusted non-3GPP IP access, according to an access specific, trusted non-3GPP IP access initiated, release mechanism.

4. If the resources are released in the trusted non-3GPP IP access, the trusted non-3GPP IP access initiates a Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [19].

5. The trusted non-3GPP IP access returns a Binding Revocation Acknowledgement message to the PDN GW.

6. In the case where the resources corresponding to the PDN connection are released in PDN GW, the PDN GW informs the 3GPP AAA Server of the PDN disconnection. If the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server notifies the HSS as described in clause 12.1.2.

NOTE: For some accesses, the resources may be released independently of deactivation from the PDN GW.

6.12.2 PDN GW initiated Resource Allocation Deactivation with S2a MIPv4

This procedure is performed to release all resource allocations associated with the PDN address, for example, due to IP-CAN session modification requests from the PCRF or due to handover without optimization from Non-3GPP to 3GPP. When it is performed for an handover, the connections associated with the PDN address are released, but the PDN address is kept in the PDN GW.

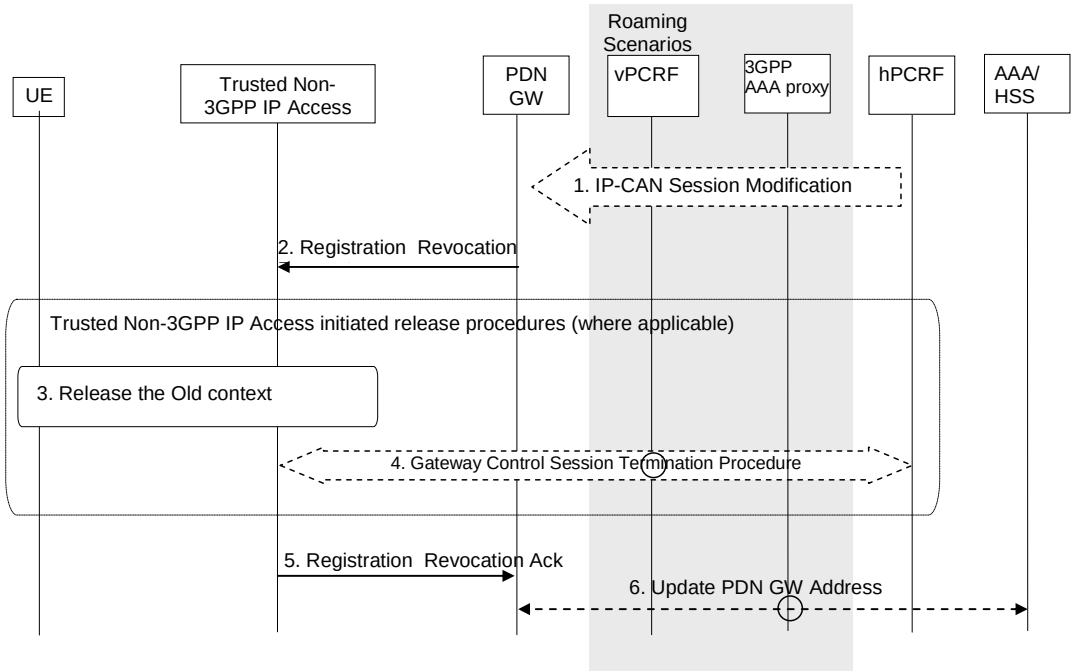


Figure 6.12.2-1: PDN GW Initiated Registration Revocation over S2a MIPv4 interface

This procedure applies to the Non-Roaming (Figure 4.2.2-1), Roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-4) cases. For the Roaming and Local Breakout cases, the vPCRF forwards messages between the non-3GPP access and the hPCRF. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

The optional interaction steps between the gateways and the PCRF in the procedures in figure 6.12.2-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

1. If dynamic PCC is deployed, the PDN GW initiated Resource Allocation Deactivation procedure may for example be triggered due to 'IP CAN session Modification procedure' as defined in TS 23.203 [19]. In this case the resources associated with the PDN connection in the PDN GW are released.

   The PDN GW initiated Resource Allocation Deactivation can also be triggered during handovers from Non-3GPP to 3GPP.

2. If the revocation support has been negotiated, the PDN GW sends a Registration Revocation message to the trusted non-3GPP IP access as defined in RFC 3543 [25].

3. The resources may be released in the trusted non-3GPP IP access, according to an access specific, trusted non-3GPP IP access initiated, release mechanism.

4. The Trusted Non-3GPP Access Network detects the UE's leaving and initiates a Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [19]. The Trusted Non-3GPP Access Network no longer applies QoS policy to service data flows for this UE.

5. The trusted non-3GPP IP access returns a Registration Revocation Acknowledgement message to the PDN GW.

6. In the case where the resources corresponding to the PDN connection are released in PDN GW, the PDN GW informs the 3GPP AAA Server of the PDN disconnection. If the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server notifies the HSS as described in clause 12.1.2.

NOTE: For some accesses, the resources may be released independently of deactivation from the PDN GW.

6.12.3 PDN GW initiated Resource Allocation Deactivation for Chained PMIP-based S8-S2a Roaming

This clause defines the PDN GW initiated resource allocation deactivation for chained PMIP-based S8-S2a roaming. This procedure also applies for PMIP-based S8-S2b chaining.

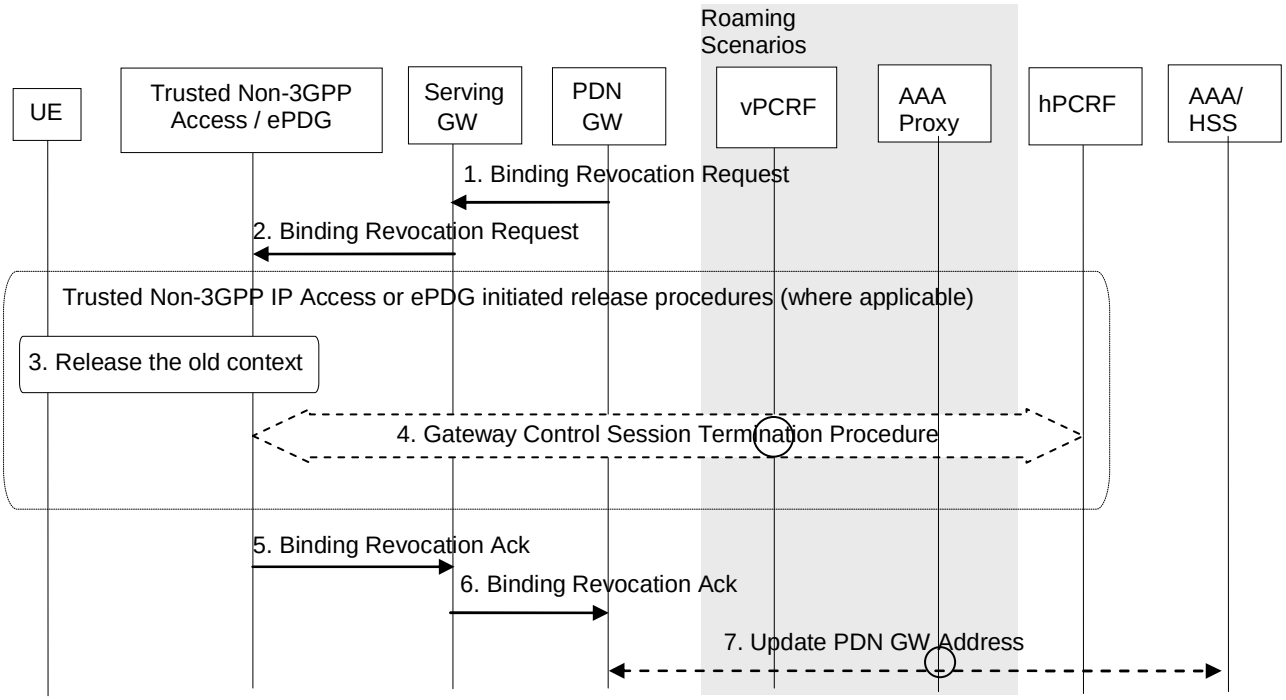


Figure 6.12.3-1: PDN GW Initiated Binding Revocation for Chained PMIP-based S8-S2a Roaming Case

The optional interaction step between the gateways and the PCRF in the procedures in figure 6.12.3-1 occur only if dynamic policy provisioning is deployed. Otherwise policies may be statically configured in the gateway.

1. The PDN GW sends a Binding Revocation Indication message to the MAG function in the Serving GW.

2. The Serving GW sends a corresponding Binding Revocation Indication message to the MAG function of the trusted non-3GPP IP access or ePDG.

3. The trusted non-3GPP IP access or ePDG may release allocated resources in the non-3GPP IP access according to access specific release mechanisms.

4. In case a Gateway Control Session between the trusted non-3GPP access or ePDG and hPCRF exists, the Gateway Control Session Termination procedure, as specified in TS 23.203 [19], is performed.

5. The MAG function of the trusted non-3GPP IP access or ePDG returns a Binding Revocation Acknowledgement message to the Serving GW.

6. The MAG function of the Serving GW or ePDG sends a corresponding Binding Revocation Acknowledgement message to the PDN GW.

7. In the case where the resources corresponding to the PDN connection are released in the PDN GW, the PDN GW informs the 3GPP AAA Server of the PDN disconnection. If the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server notifies the HSS as described in clause 12.1.2.

NOTE: For some accesses, the resources may be released independently of deactivation from the PDN GW.

6.12.4 Void

6.13 PDN GW initiated IPv4 address Delete Procedure

This procedure is initiated by the PDN GW when the UE releases the IPv4 address using DHCPv4 procedure or the lease for the IP address has expired. The procedure is used to delete the IPv4 address from the PDN connection bearer context.

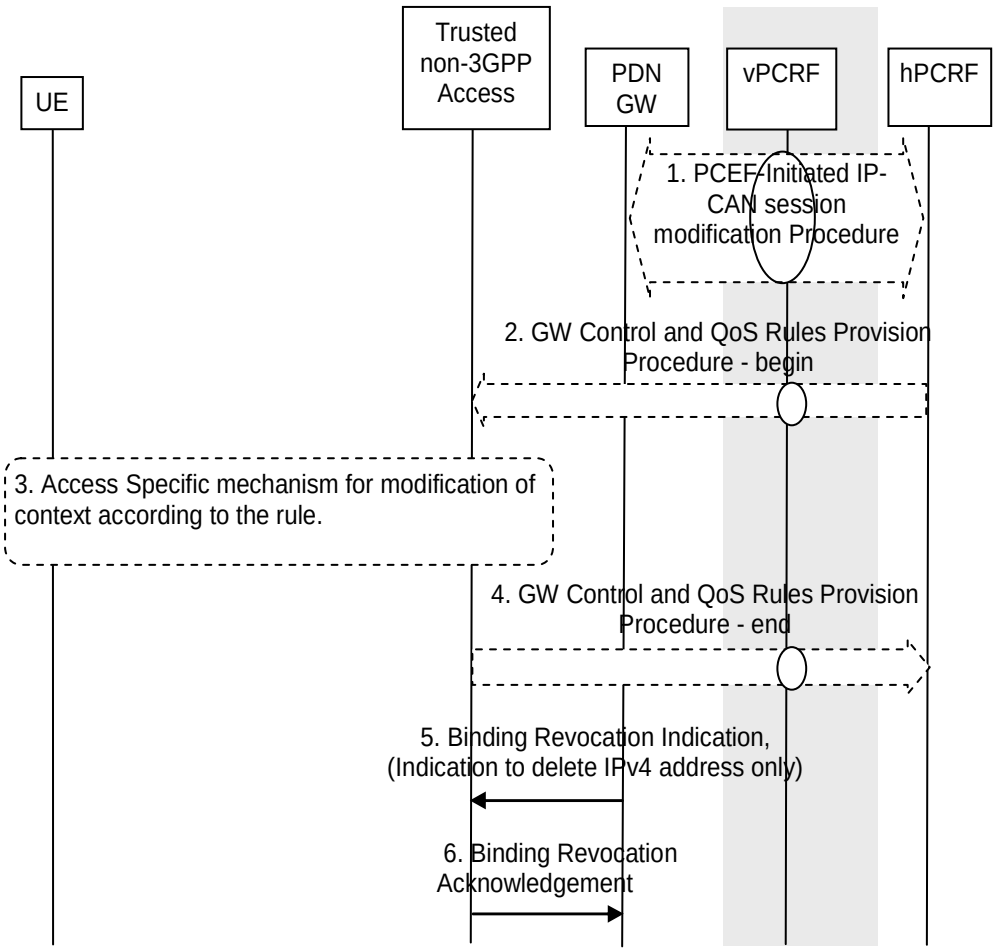


Figure 6.13-1: PDN GW initiated IPv4 address Delete Procedure

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured in the gateway.

The roaming (Figure 4.2.3-1), Local Breakout (Figure 4.2.3-4) and non-roaming (Figure 4.2.2-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, relaying the PCC messages between the hPCRF

in the HPLMN to the BBERF/PCEF in the VPLMN. In the non-roaming case, the vPCRF is not involved at all. In the Roaming and LBO cases, the 3GPP AAA Proxy serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN.

1. The PCEF initiates the IP-CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19]. The PDN GW provides the information to enable the PCRF to uniquely identify the IP-CAN session.

2. In case QoS rules have to be modified, e.g. change of SDF filters, the PCRF initiates a GW Control and QoS rules provision procedure as described in TS 23.203 [19] to inform the Trusted non-3GPP access of the updated QoS rules.

3. The Trusted non-3GPP Access initiates the "Network-initiated Dynamic PCC on S2a" procedure to release the bearers.

4. The trusted non-3GPP access informs the PCRF of the success of the QoS rules enforcement, thus ending the GW Control and QoS rules provision procedure described in TS 23.203 [19].

5. The PDN GW sends a Binding Revocation Indication (PDN address) message to the trusted non-3GPP access to revoke the IPv4 address.

6. The trusted non-3GPP access returns a Binding Revocation Acknowledgement message to the PDN GW.

6.14 Non-3GPP access initiated IPv4 address Delete Procedure

This procedure is initiated by the Trusted non-3GPP access when the UE releases the IPv4 address using DHCPv4 procedure or the lease for the IP address has expired. The procedure is used to delete the IPv4 address from the PDN connection and bearer context.

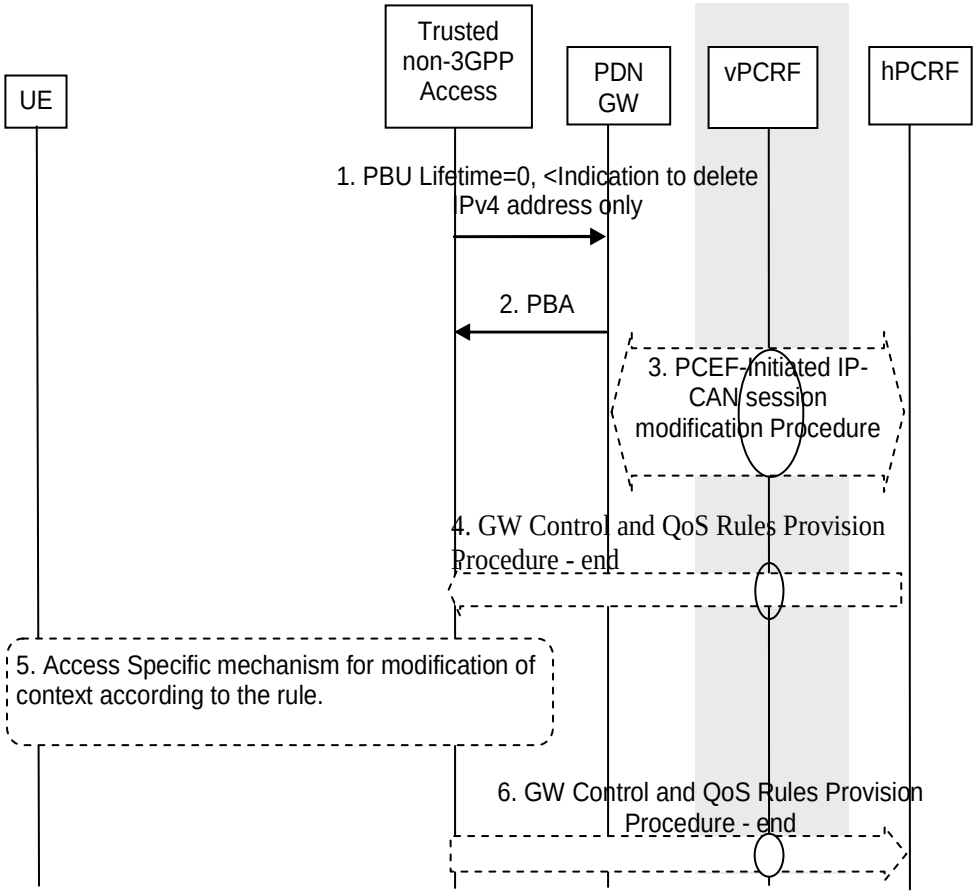


Figure 6.14-1: Non-3GPP access initiated IPv4 address Delete Procedure

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured in the gateway.

The roaming (Figure 4.2.3-1), Local Breakout (Figure 4.2.3-4) and non-roaming (Figure 4.2.2-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, relaying the PCC messages between the hPCRF in the HPLMN to the BBERF/PCEF in the VPLMN. In the non-roaming case, the vPCRF is not involved at all. In the Roaming and LBO cases, the 3GPP AAA Proxy serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN.

1. The MAG in the Trusted Non-3GPP IP Access sends a Proxy Binding Update (MN NAI, APN, lifetime=0, IPv4 only indication) message to the PDN GW with lifetime value set to zero, indicating de-registration. The MN NAI identifies the UE to deregister from the PDN GW. The indication for IPv4 only informs the UE that only the IPv4 address from BCE is to be deleted. The APN is needed in order to determine which PDN GW to de-register the UE from, as some PDNs may support multiple PDNs.

2. The PDN GW modifies the existing entry to delete the IPv4 address implied in the Proxy Binding Update message from its Binding Cache and releases all associated resources, and then sends a Proxy Binding Ack (MN NAI, APN, lifetime=0, IPv4 only indicator) message to the MAG in trusted non-3GPP access.

3. The PDN-GW initiates the PCEF initiated IP-CAN session modification procedure as described in TS 23.203 [19] to inform the PCRF of the deleted IPv4 address. If PCC rules have changed the PCRF provides the updated PCC rules to the PDN-GW as part of this procedure.

4. In case QoS rules have to be modified, e.g. change of SDF filters, the PCRF initiates a GW Control and QoS rules provision procedure as described in TS 23.203 [19] to inform the S-GW of the updated QoS rules.

5. An IP-CAN specific or resource release procedure may be triggered by the enforcement of the received policy rules.

6. The Trusted non-3GPP access informs the PCRF of the success of the QoS rules enforcement, thus ending the GW Control and QoS rules provision procedure described in TS 23.203 [19].

6.15 IPv4 Home Address Release Procedure for S2c

This procedure is initiated by the UE to release an IPv4 Home Address previously registered at the PDN GW.

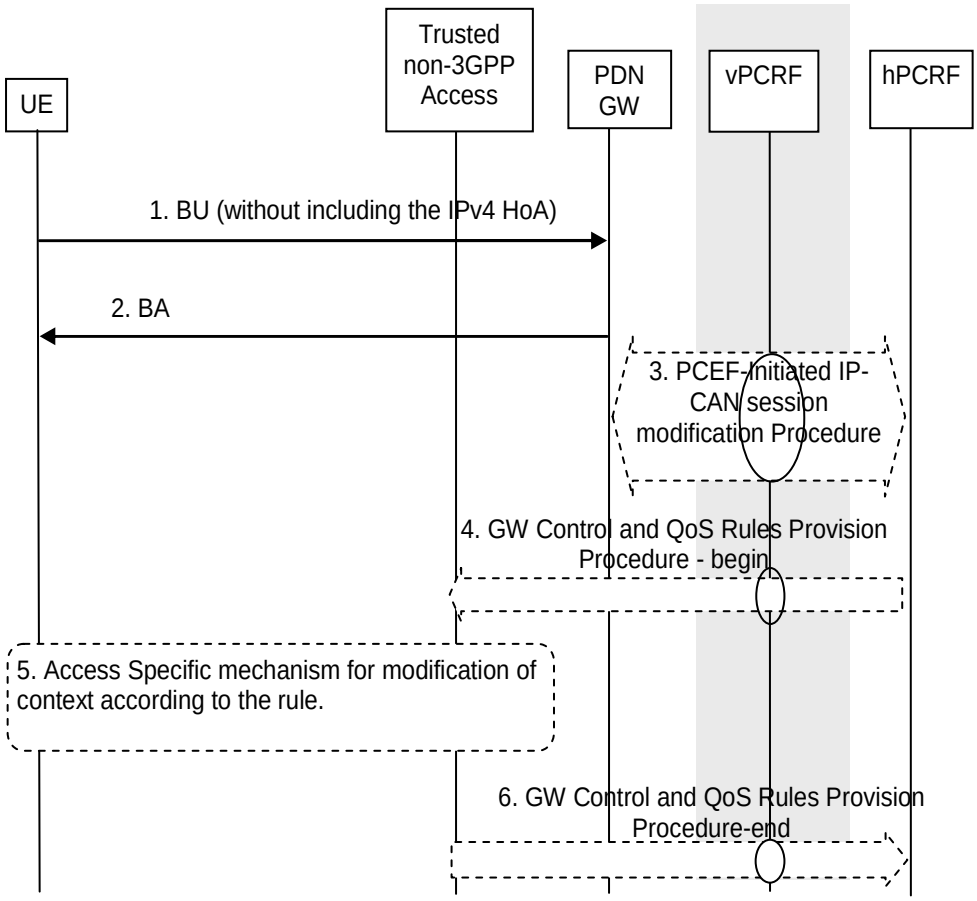


Figure 6.15-1: IPv4 Home Address Release Procedure for S2c

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured in the gateway.

The roaming (Figure 4.2.3-1), Local Breakout (Figure 4.2.3-4) and non-roaming (Figure 4.2.2-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, relaying the PCC messages between the hPCRF in the HPLMN to the BBERF/PCEF in the VPLMN. In the non-roaming case, the vPCRF is not involved at all. In the Roaming and LBO cases, the 3GPP AAA Proxy serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN.

1. If the UE has previously registered IPv4 home address and wants to release it, the UE sends a Binding Update (IPv6 HoA, lifetime) message to the PDN GW without including the IPv4 HoA, indicating de-registration for the IPv4 Home Address only.

2. The PDN GW modifies the existing entry to delete the IPv4 home address implied in the Binding Update message from its Binding Cache and releases all associated resources, and then sends a Binding Ack message to the UE.

3. The PDN-GW initiates the PCEF initiated IP-CAN session modification procedure as described in TS 23.203 [19] to inform the PCRF of the deleted IPv4 address. If PCC rules have changed the PCRF provides the updated PCC rules to the PDN-GW as part of this procedure.

4. In case QoS rules have to be modified, e.g. change of SDF filters, the PCRF initiates a GW Control and QoS rules provision procedure as described in TS 23.203 [19] to inform the S-GW of the updated QoS rules.

5. An IP CAN specific or resource release procedure may be triggered by the enforcement of the received policy rules.

6. The Trusted non-3GPP access informs the PCRF of the success of the QoS rules enforcement, thus ending the GW Control and QoS rules provision procedure described in TS 23.203 [19].

6.16 Enhanced security support for S2c

6.16.1 General

Optionally UE and PDN GW may support integrity protection and/or confidentiality protection of user plane traffic exchanged over the S2c tunnel when the UE is in a trusted non-3GPP access.

6.16.2 Activation of enhanced security for S2c

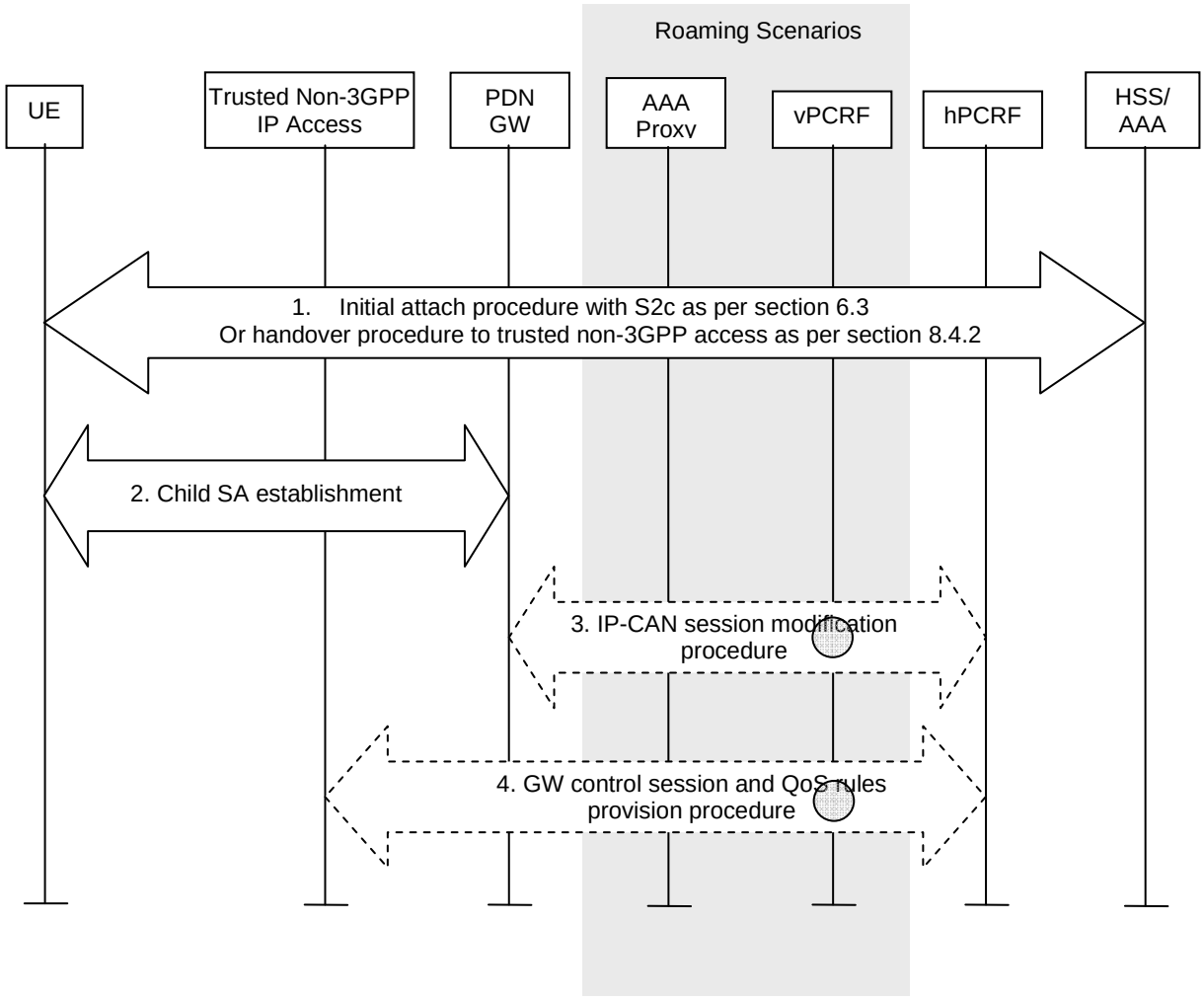


Figure 6.16.1-1: Enhanced security support activation

1) The UE performs an initial attach procedure to a trusted non-3GPP access with S2c as described in clause 6.3 or performs a handover procedure to a trusted non-3GPP access as specified in clause 8.4.2. At the end of this step the UE is connected to a trusted non-3GPP access via S2c.

2) At any time when the UE is connected to a trusted non-3GPP access the UE or the PDN GW may trigger the creation of a child IPsec Security Association for protecting the traffic sent via the S2c reference point. The child SA is created as specified in RFC 4877 [22]. The child SA may provide user plane integrity protection. Additionally, the same child SA may be used also for user plane confidentiality protection.

3) The PDN GW initiates an IP-CAN session modification procedure to provide to the PCRF new tunnel information.

4) Based on the tunnel information provided by the PDN GW, the PCRF initiates a QoS rules provision procedure to the trusted non-3GPP access indicating the new tunnel information.

NOTE 1: If confidentiality protection is activated, the usage of PCC for per UE and/or per IP flow QoS differentiation in the trusted non-3GPP access is not possible in this Release of the specification.

NOTE 2: If confidentiality protection is activated, in roaming scenarios the traffic collected by the VPLMN for legal interception purposes is encrypted.

NOTE 3: If the establishment of the child IPsec Security Association fails, based on operator's policies and user's settings the UE or the PDN GW may terminate the S2c session using the PDN disconnection procedures specified in clause 6.5.

6.16.3 De-activation of enhanced security for S2c

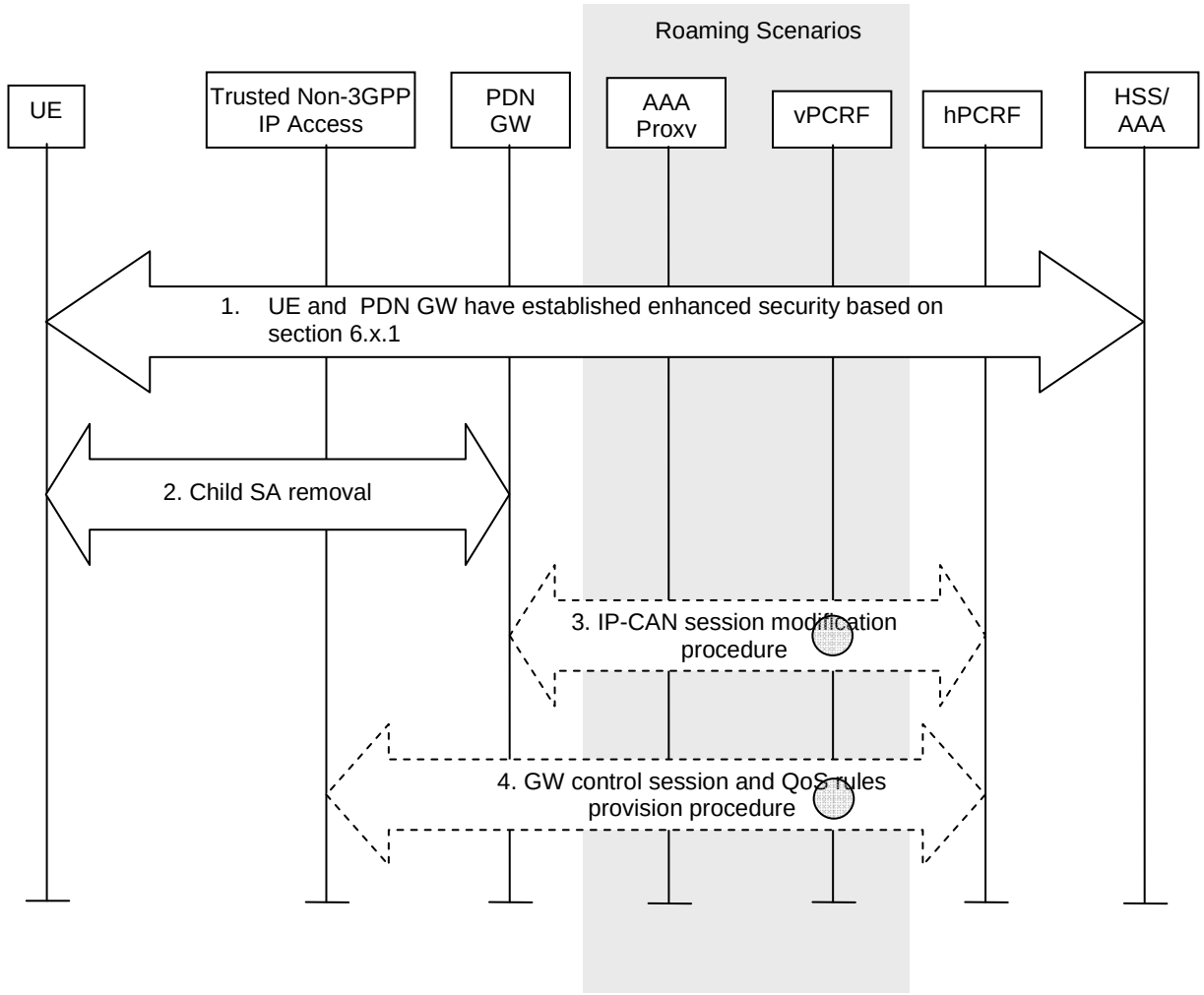


Figure 6.16.2-1: Enhanced security support de-activation

1) The UE and the PDN GW have established enhanced security based on clause 6.16.1. As a result user plane traffic exchanged through S2c is integrity protected and/or confidentiality protected.

2) At any time the UE or the PDN GW may trigger the removal of a child IPsec Security Association for protecting the traffic sent via the S2c reference point. The child SA is removed as specified in RFC 4877 [22].

NOTE: Integrity protection and/or confidentiality protection can be de-activated also after the handover to another access and not only from the trusted non-3GPP access it was activated.

3) The PDN GW initiates an IP-CAN session modification procedure to provide to the PCRF new tunnel information.

4) Based on the tunnel information provided by the PDN GW, the PCRF initiates a QoS rules provision procedure to the trusted non-3GPP access indicating the new tunnel information.

7 Functional Description and Procedures for Un-trusted Non-3GPP IP Accesses

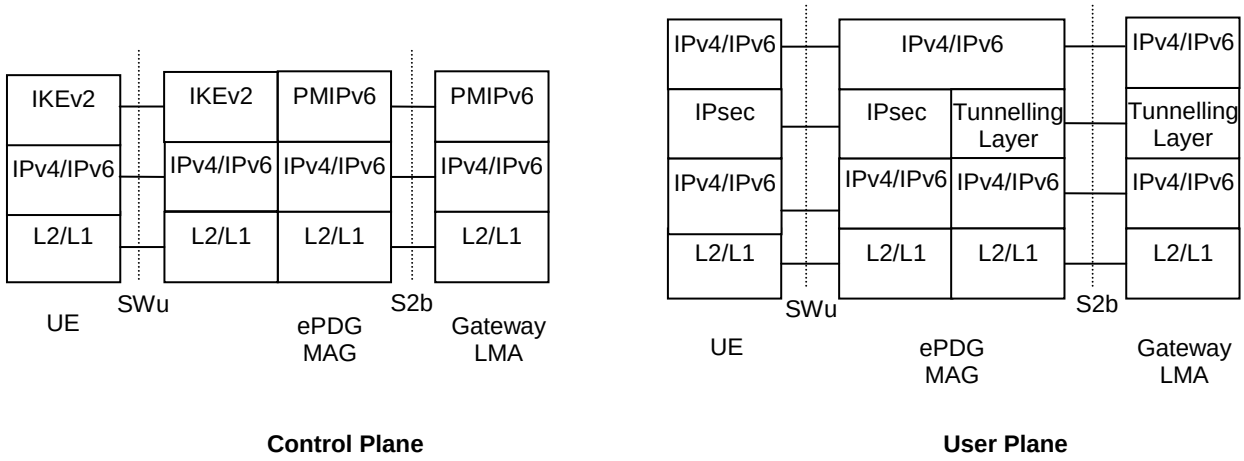
7.1 Control and User Plane Protocol Stacks

7.1.1 Protocol Options for S2b

The following protocol may be supported on S2b:

- PMIPv6;
- GTP.

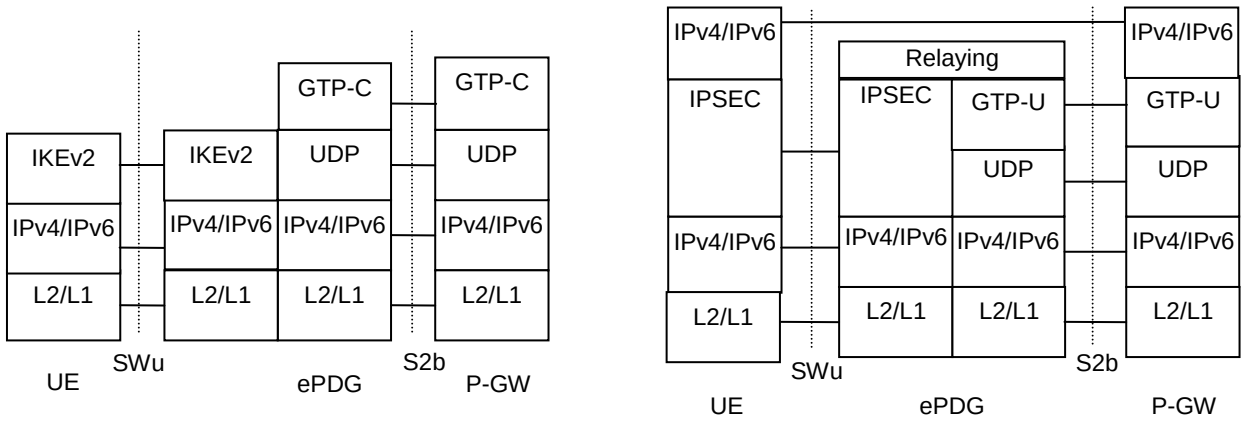
Figures 7.1.1-1 and 7.1.1-2 illustrate the control plane for Mobility Management (MM) and the user plane on S2b for the PMIPv6 and GTP variants of S2b respectively.



Legend:

- According to terms defined in PMIPv6 specification, RFC 5213 [8], the functional entities terminating both the control and user planes are denoted MAG in the non-3GPP IP access and LMA in the Gateway. LMA includes also the function of a Home Agent.
- The MM control plane stack is PMIPv6 (RFC 5213 [8]) over IPv6/IPv4.
- The user plane carries remote IPv4/v6 packets over either an IPv4 or an IPv6 transport network. Between the UE and the ePDG, packets are encapsulated using IPSEC RFC 3948 [48].
- The tunnelling layer implements GRE encapsulation applicable for PMIPv6.
- **IPv4/IPv6:** This refers to network layer protocols. On the ePDG MAG user plane this includes termination of the UE-MAG IP messages that may be handled by the ePDG (e.g. DHCP) and forwarding of user plane IP packets between the UE-MAG point-to-point logical link and the S2b tunnel for the UE.

Figure 7.1.1-1: Protocols for MM control and user planes of S2b for the PMIPv6 option



Control Plane **User Plane**

Legend:

- **GPRS Tunnelling Protocol for the control plane (GTP-C):** This protocol tunnels signalling messages between the ePDG and the P-GW (S2b).
- **GPRS Tunnelling Protocol for the user plane (GTP-U):** This protocol tunnels user data between the ePDG and the P-GW in the backbone network. GTP shall encapsulate all end user IP packets.
- **UDP/IP:** These are the backbone network protocols used for routing user data and control signalling.

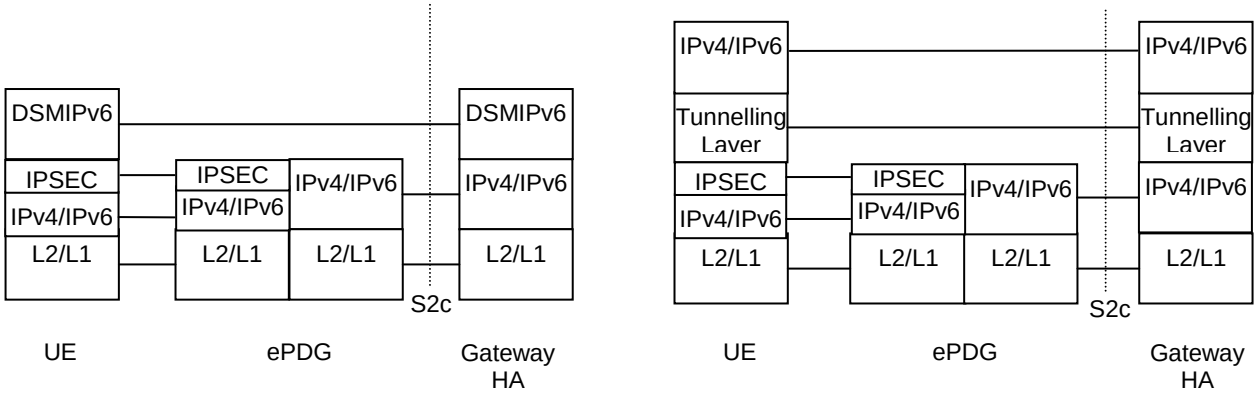
Figure 7.1.1-2: Protocols for MM control and user planes of S2b for the GTP option

7.1.2 Protocol Options for S2c over Un-trusted Non-3GPP IP Accesses

The following protocols shall be supported for S2c over un-trusted non-3GPP IP accesses:

- DSMIPv6, with IPsec and IKEv2 used to secure mobility signalling, as specified in RFC 4877 [22].

The figure below illustrates the control plane for Mobility Management (MM) and the user plane.



Control Plane **User Plane**

Legend:

- According to terms defined in DSMIPv6 [10], the functional entities terminating both the control and user planes are denoted MN (Mobile Node) in the UE, and HA (Home Agent) in the Gateway.
- The MM control plane stack is DSMIPv6 [10] over IPv6/IPv4.
- The user plane carries remote IPv4/v6 packets over either an IPv4 or an IPv6 transport network. Between the UE and the ePDG, packets are encapsulated using IPSEC RFC 3948 [48].
- The tunnelling layer implements IP encapsulation applicable for MIPv6 as defined in DSMIPv6 [10]. In some cases the tunnelling layer may be transparent.

Figure 6.1.2-1: Protocols for MM control and user planes of S2c for the DSMIPv6 option

7.2 Initial Attach on S2b

7.2.1 Initial Attach with PMIPv6 on S2b

This clause is related to the case when the UE powers-on in an untrusted non-3GPP IP access network via the PMIP based S2b interface.

PMIPv6 specification, RFC 5213 [8], is used to setup a PMIPv6 tunnel between the ePDG and the PDN GW. It is assumed that MAG is collocated with ePDG. The IPsec tunnel between the UE and the ePDG provides a virtual point-to-point link between the UE and the MAG functionality on the ePDG.

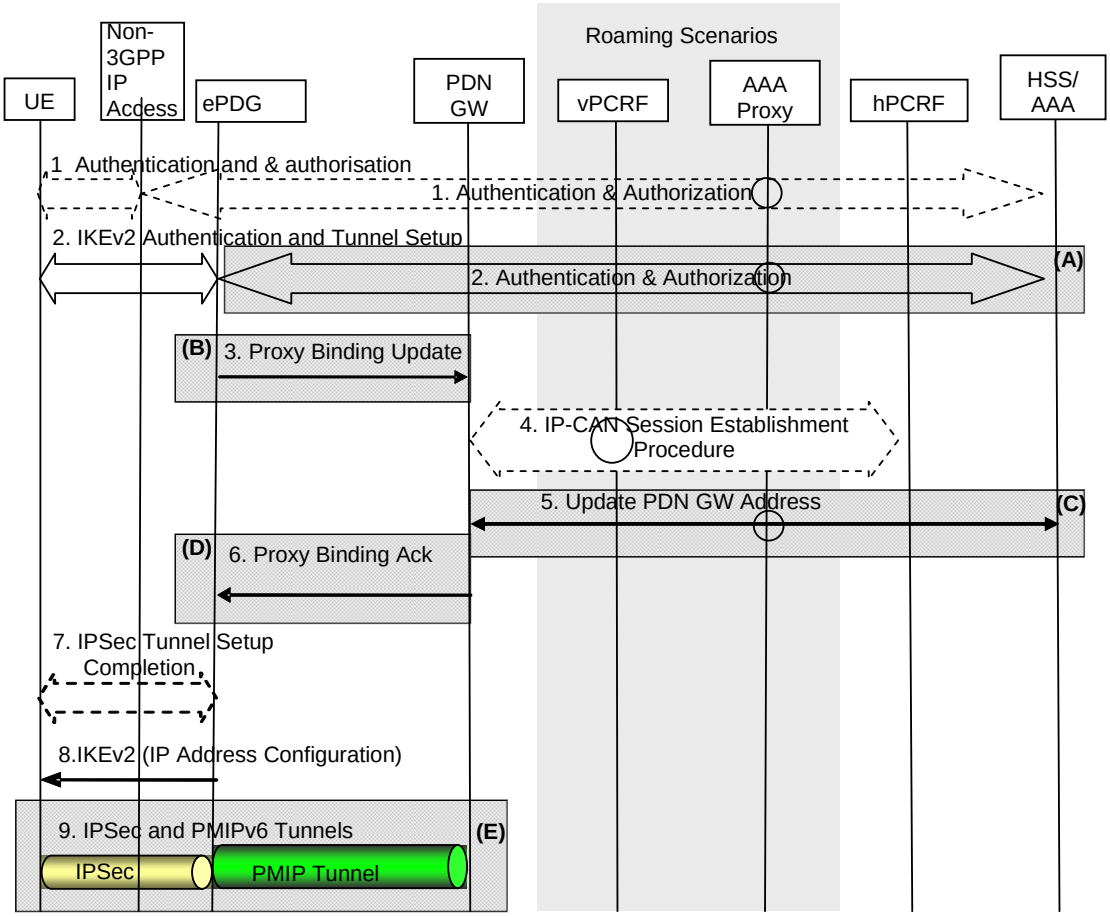


Figure 7.2.1-1: Initial attachment over PMIP based S2b for roaming, non-roaming and LBO

NOTE 1: For GTP based S2b, procedure steps (A) to (E) are defined in clause 7.2.4.

NOTE 2: Before the UE initiates the setup of an IPsec tunnel with the ePDG it configures an IP address from an untrusted non-3GPP IP access network. This address is used for sending all IKEv2 [9] messages and as the source address on the outer header of the IPsec tunnel.

The home routed roaming (Figure 4.2.3-1), LBO (Figure 4.2.3-4) and non-roaming (Figure 4.2.2-1) scenarios are depicted in the figure.

- In the LBO case, the 3GPP AAA Proxy acts as an intermediary, forwarding messages from the 3GPP AAA Server in the HPLMN to the PDN GW in the VPLMN and visa versa. Messages between the PDN GW in the VPLMN and the hPCRF in the HPLMN are forwarded by the vPCRF in the VPLMN.

- In the home routed roaming and non-roaming case, the vPCRF and the 3GPP AAA Proxy are not involved.

If dynamic policy provisioning is not deployed, the optional step 3 does not occur. Instead, the PDN GW may employ static configured policies.

This procedure is also used to establish the first PDN connection over an untrusted non-3GPP access with PMIPv6 on S2b when the UE already has active PDN connections only over a 3GPP access and wishes to establish simultaneous PDN connections to different APNs over multiple accesses.

The UE may be authenticated and authorised to access the Untrusted Non-3GPP Access network with an access network specific procedure. These procedures are outside the scope of 3GPP.

1) The Access authentication procedure between UE and the 3GPP EPC may be performed as defined by TS 33.402 [45]. In the roaming case signalling may be routed via a 3GPP AAA Proxy in the VPLMN. As part of the AAA exchange for network access authentication, the AAA/HSS and/or the 3GPP AAA Proxy may return to the Non-3GPP IP Access a set of home/visited operator's policies to be enforced on the usage of local IP address, or IPv6 prefix, allocated by the access system upon successful authentication. Subscription data is provided to the Non-3GPP IP Access by the HSS/AAA in this step.

2) The IKEv2 tunnel establishment procedure is started by the UE. The UE may indicate in a notification part of the IKEv2 authentication request that it supports MOBIKE. The ePDG IP address to which the UE needs to form IPsec tunnel is discovered via DNS query as specified in clause 4.5.4. The UE may request connectivity to a specific PDN providing an APN, that is conveyed with IKEv2 as specified in TS 33.402 [45]. For networks supporting multiple mobility protocols, if there was any dynamic IPMS decision involved in this step, the decision is stored in the 3GPP AAA Server. The PDN GW information is returned as part of the reply from the 3GPP AAA Server to the ePDG as described in clause 4.5.1. If the UE has provided an APN the ePDG verifies that it is allowed by subscription. If the UE has not provided an APN the ePDG uses the default APN. The PDN GW selection takes place at this point as described in clause 4.5.1. This may entail an additional name resolution step, issuing a request to a DNS Server. If there is no requested IP address in the CFG_Request from the UE to the ePDG which indicates the attach is an initial attach, the ePDG may perform a new PDN GW selection procedure as described in clause 4.5.1, e.g. to allocate a PDN GW that allows for more efficient routeing. The UE shall indicate the type of address(es) (IPv4 address or IPv6 prefix /address or both) in the CFG_Request sent to the ePDG during IKEv2 message exchange. If the PDN requires an additional authentication and authorisation with an external AAA Server, the UE includes the authentication credentials in this step as specified in RFC 4739 [50] and in TS 33.402 [45]. As part of the IKEv2 tunnel establishment procedure, the ePDG may request the UE to provide its IMEI(SV). In that case the UE shall signal its IMEI(SV) to the ePDG. The ePDG forwards the IMEI(SV) received from the UE to the 3GPP AAA Server (over SWm).

3) The ePDG sends the Proxy Binding Update (MN-NAI, Lifetime, APN, Access Technology Type, Handover Indicator, GRE key for downlink traffic, UE Address Info, Charging Characteristics, Additional Parameters, IMEI(SV) if available) message to the PDN GW. Access Technology Type option is set to a value matching the characteristics of the non-3GPP IP access. Handover Indicator is set to indicate attachment over a new interface. The proxy binding update message shall be secured. The MN NAI identifies the UE. The Lifetime field must be set to a nonzero value in the case of a registration and a zero value in the case of a de-registration. The APN is used by the PDN GW to determine which PDN to establish connectivity for, in the case that the PDN GW supports multiple PDN connectivity. The ePDG creates and includes a PDN connection identity if the ePDG supports multiple PDN connections to a single APN. The UE Address Info shall be set based on the CFG_Request in step 1 and subscription profile in the same way as the PDN type is selected during the E-UTRAN Initial Attach in TS 23.401 [4]. The Additional Parameters include the authentication credentials for an additional authentication and authorization with an external AAA server if it was provided by the UE in step 2. The PDN GW performs the authentication and authorization with the external AAA server if it is required to get access for the given APN as specified in TS 33.402 [45].

4) The PDN GW initiates the IP CAN Session Establishment Procedure with the PCRF, as specified in TS 23.203 [19]. If available, the PCRF provides the APN-AMBR and Default Bearer QoS to the PDN GW in the response message.

5) The selected PDN GW informs the 3GPP AAA Server of the PDN GW identity. The 3GPP AAA Server then informs the HSS of the PDN GW identity and APN associated with the UE's PDN Connection. The message includes information that identifies the PLMN in which the PDN GW is located. This information is registered in the HSS as described in clause 12. The PDN GW shall only use the APN-AMBR and Default Bearer QoS received from the 3GPP AAA server in this step if these parameters have not been received in step 4.

6) The PDN GW processes the proxy binding update and creates a binding cache entry for the UE. The PDN GW allocates an IP address for the UE. The PDN GW then sends a Proxy Binding Ack (MN NAI, UE Address Info, GRE Key for uplink traffic, Charging ID) message to the ePDG, including the IP address(es) allocated for the UE (identified by the MN NAI). If the corresponding Proxy Binding Update contains the PDN connection

identity, the PDN GW shall acknowledge if multiple PDN connections to the given APN are supported. The Charging ID is assigned for the PDN connection for charging correlation purposes.

NOTE 3: If UE requests for both IPv4 address and IPv6 prefix, both are allocated. If the PDN GW operator dictates the use of IPv4 address only or IPv6 prefix only for this APN, the PDN GW shall allocate the only IPv4 address or only IPv6 prefix to the UE. If the UE requests for only IPv4 address or IPv6 prefix only one address/prefix is allocated accordingly.

NOTE 4: The ePDG learns from the PBA whether the PDN GW supports multiple PDN connection to the same APN or not.

7) After the Proxy Binding Update is successful, the ePDG is authenticated by the UE and indicates to the UE that the authentication and authorization with the external AAA server is successful.

8) The ePDG sends the final IKEv2 message with the IP address in IKEv2 Configuration payloads. The ePDG also includes the identity of the associated PDN (APN) in the IDr payload of IKEv2. In case the UE provided APN to the ePDG in the earlier steps, the ePDG shall not change the provided APN.

9) IP connectivity from the UE to the PDN GW is now setup. Any packet in the uplink direction is tunnelled to the ePDG by the UE using the IPSec tunnel. The ePDG then tunnels the packet to the PDN GW. From the PDN GW normal IP-based routing takes place. In the downlink direction, the packet for UE (HoA) arrives at the PDN GW. The PDN GW tunnels the packet based on the binding cache entry to the ePDG. The ePDG then tunnels the packet to the UE via proper IPsec tunnel.

7.2.2 Void

7.2.3 Initial Attach Procedure with PMIPv6 on S2b and Chained S2b and PMIP-based S8

This procedure is described in clause 6.2.4.

7.2.4 Initial Attach with GTP on S2b

This clause is related to the case when the UE powers-on in an untrusted non-3GPP IP access network via the GTP based S2b interface.

GTPv2 (see TS 29.274 [57]) is used to setup GTP tunnel(s) between the ePDG and the PDN GW. The IPsec tunnel between the UE and the ePDG provides a virtual point-to-point link between the UE and the ePDG.

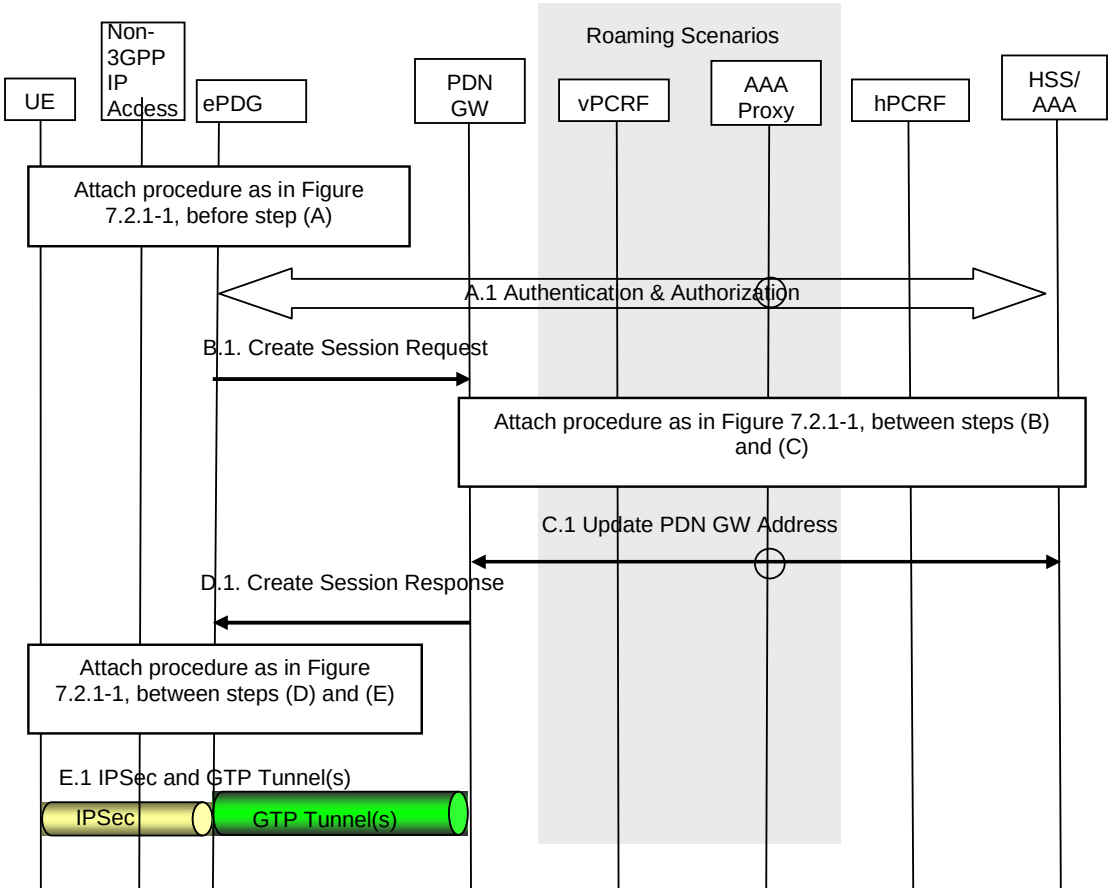


Figure 7.2.4-1: Initial attachment over GTP based S2b for roaming, non-roaming and LBO

The home routed roaming (Figure 4.2.3-1), LBO (Figure 4.2.3-4) and non-roaming (Figure 4.2.2-1) scenarios are depicted in the figure.

- In the LBO case, the 3GPP AAA Proxy acts as an intermediary, forwarding messages from the 3GPP AAA Server in the HPLMN to the PDN GW in the VPLMN and visa versa. Messages between the PDN GW in the VPLMN and the hPCRF in the HPLMN are forwarded by the vPCRF in the VPLMN.

- In the home routed roaming and non-roaming case, the vPCRF and the 3GPP AAA Proxy are not involved.

This procedure is also used to establish the first PDN connection over an untrusted non-3GPP access with GTP on S2b when the UE already has active PDN connections only over a 3GPP access and wishes to establish simultaneous PDN connections to different APNs over multiple accesses.

The UE may be authenticated and authorised to access the Untrusted Non-3GPP Access network with an access network specific procedure. These procedures are outside the scope of 3GPP.

A.1) Step A.1 is the same as Step A of clause 7.2.1, with the following addition:

- upon a successful authorization, the 3GPP AAA server returns the following additional informations, regardless of which protocol variant the ePDG will select on S2b : APN-AMBR, static QoS Profile and Trace Information (Trace Reference, Trace Type, Trigger Id, OMC Identity) if applicable. When the 3GPP AAA server has WLAN Location Information about the UE, it provides it over SWm to the ePDG together with the Age of this information. The WLAN Location information is provided to the ePDG only when the 3GPP AAA server considers that location information coming from the WLAN AN used by the UE is trustable.

NOTE 1: Sending the static QoS profile to the ePDG enables the ePDG to enforce QoS policies based on information received via AAA infrastructure as specified in clause 4.3.4. When GTP is used over S2b, this also allows the PGW to receive the QoS parameters possibly modified by the 3GPP AAA Proxy (when the ePDG is located in the VPLMN) to enforce QoS limitations according to the local policies and the roaming agreement with the home operator. The ePDG does not perform rate enforcement based on APN-AMBR.

NOTE 2: This also allows to align the GTP operations on S5/S8/S2b, i.e. the PGW receives those parameters within GTP signalling on all GTP interfaces.

B.1) The ePDG sends a Create Session Request (IMSI, APN, RAT type, ePDG TEID for control plane, PDN Type, PDN Address, EPS Bearer Identity, Default EPS Bearer QoS, ePDG Address for the user plane, ePDG TEID of the user plane, APN-AMBR, Selection Mode, Dual Address Bearer Flag, Trace Information, Charging Characteristics, Additional Parameters, IMEI(SV), User Location Information) message to the PGW. The RAT type indicates the non-3GPP IP access technology type. The PDN Type shall be set based on the CFG_Request in step 1 and subscription profile in the same way as the PDN type is selected during the E-UTRAN Initial Attach in TS 23.401 [4]. The ePDG shall set the Dual Address Bearer Flag when the PDN type is set to IPv4v6 and all SGSNs which the UE may be handed over to are Release 8 or above supporting dual addressing, which is determined based on node pre-configuration by the operator. The ePDG shall include Trace Information if PDN GW trace is activated. The Additional Parameters include the authentication credentials for an additional authentication and authorization with an external AAA server if it was provided by the UE before this step. The ePDG shall provide the IMEI(SV) if available; The PDN GW performs the authentication and authorization with the external AAA server if it is required to get access for the given APN. The User Location Information shall include UE local IP address and optionally UDP source port number (if NAT is detected). It may also include WLAN Location Information (and its Age) the ePDG may have received from the 3GPP AAA server about the UE.

NOTE 3: The UE local IP address is the source address on the outer header of the IPsec tunnel to the ePDG.

The PGW creates a new entry in its bearer context table and generates a Charging Id. The new entry allows the PGW to route user plane PDUs between the ePDG and the packet data network and to start charging.

NOTE 4: The EPS Bearer Identity and Default EPS Bearer QoS parameters convey the S2b bearer identity and the default S2b bearer QoS.

C.1) Step C.1 is the same as Step C of clause 7.2.1, with the following addition:

- when informing the 3GPP AAA Server of the PDN GW identity, the selected PDN GW also indicates the selected S2b protocol variant (here GTP); this allows the option for the 3GPP AAA Server or 3GPP AAA Proxy not to return to the PDN GW PMIP specific parameters (e.g. static QoS Profile, Trace Information, APN-AMBR) if GTP is used over S2b; the PDN GW shall ignore those parameters if received from the 3GPP AAA Server or 3GPP AAA Proxy.

- The PDN GW forwards to the PCRF in the IP-CAN Session Establishment procedure following information extracted from User Location Information it may have received from the ePDG:

  - The UE local IP address

  - WLAN location information in conjunction with the Age of this information,

D.1) The PDN GW returns a Create Session Response (PDN GW Address for the user plane, PDN GW TEID of the user plane, PDN GW TEID of the control plane, PDN Type, PDN Address, EPS Bearer Identity, EPS Bearer QoS, APN-AMBR, Charging ID, Cause) message to the ePDG, including the IP address(es) allocated for the UE. The PDN GW selects the PDN type to be used in the same way as done during the E-UTRAN Initial Attach in TS 23.401 [4].

The PGW may initiate the creation of dedicated bearers on GTP based S2b (like it may do it on GTP based S5/S8 for an Attach on 3GPP access).

NOTE 5: If the UE requests for both IPv4 address and IPv6 prefix, both are allocated. If the PDN GW operator dictates the use of IPv4 address only or IPv6 prefix only for this APN, the PDN GW shall allocate the only IPv4 address or only IPv6 prefix to the UE. If the UE requests for only IPv4 address or IPv6 prefix only one address/prefix is allocated accordingly.

E.1) Step E.1 is the same as Step E of clause 7.2.1, but with GTP tunnel(s).

7.2.5 Initial Attach for emergency session (GTP on S2b)

When the UE needs to establish an IMS emergency session over Untrusted WLAN access, the procedure described in this clause applies. The Initial Attach for emergency session follows the same steps that the Initial Attach for a non

emergency session, so only the differences with regard to the procedures described in clauses 7.2.1 and 7.2.4 are documented.

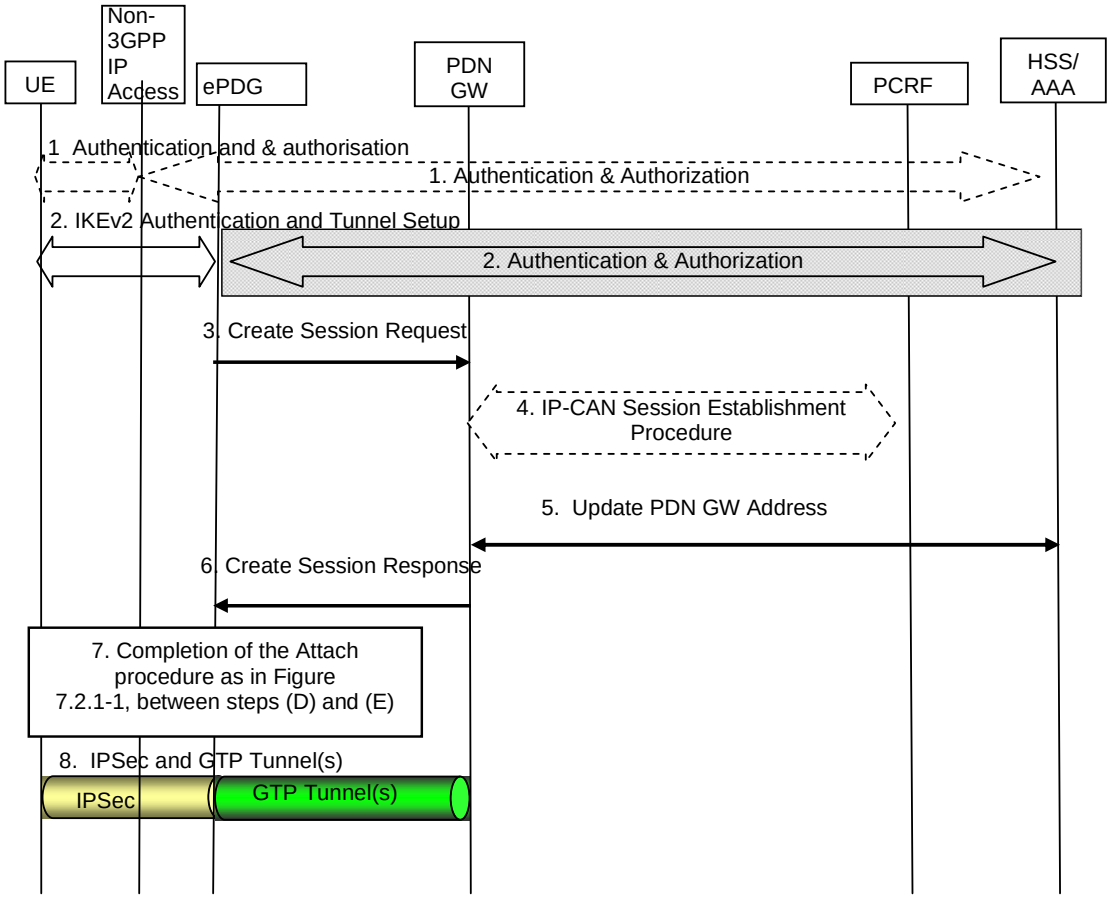


Figure 7.2.5-1: Initial attachment for emergency services over GTP based S2b

1) As in step 1 of Figure 7.2.1 with following modifications:

   As part of procedures for Authentication and Authorization on an Access Point based on USIM credentials, the 3GPP AAA server may store WLAN Location Information defined in clause 4.5.7.2.8.

2) The UE releases any connectivity it may have over Un-trusted access to EPC per the procedure defined in clause 7.4.3. The UE does not need to wait the procedure defined in clause 7.4.3 to be completed to proceed with following steps: the UE shall select an ePDG that supports emergency services as defined in clause 4.5.4a and initiate an IKEv2 tunnel establishment procedure as in step 2 of clause 7.2.1 but with following specificities:

   - The UE provides an indication that the EPC access is for emergency services.The indication is used by the 3GPP AAA server to give precedence to this session in case of signalling congestion (over SWx). The indication is used by the ePDG to apply specific policies related with emergency PDN connection (e.g. stored in Emergency Configuration Data).

   - Any APN received by the ePDG from the UE is ignored as the ePDG uses its Emergency Configuration Data to determine the APN to be associated with the emergency PDN connection and possibly to determine the PDN GW to use.

NOTE: No procedure for additional authentication and authorisation with an external AAA Server as specified in RFC 4739 [50] and in TS 33402 [45] is expected.

   - Upon a successful authorization by the 3GPP AAA server, the ePDG stores subscription information received from the 3GPP AAA but does not use this information for the emergency PDN connection. It instead uses Emergency Configuration Data to get information on the APN and possibly PDN GW and / or QoS (APN-AMBR, default QoS) to use for the emergency PDN connection.

3) The ePDG sends a Create Session Request message to the PGW as described in step B.1 of clause 7.2.4 but with following specificities:

   - No parameter sent in the Create Session Request message is related with the user subscription. Parameters in the Emergency Configuration Data are used instead.

   - No Additional Parameters are provided for additional authentication and authorisation with an external AAA Server.

   - The PDN GW deduces the emergency related policies to apply from the APN received in the Create Session Request message.

4) As Step 4 of clause 7.2.1, with the following specificities:

   - The PCRF deduces the emergency related policies to apply from the APN received in the IP-CAN Session Establishment message.

5) As in step C.1 of clause 7.2.4, with the following specificities:

   - The PDN GW sends an Emergency indication over S6b in order for the 3GPP AAA server to be able to apply specific policies for emergency services. For instance, the 3GPP AAA server does not update the HSS with the identity of the PDN GW in that case.

6) As in step D.1 of clause 7.2.4.

7) As in step E.1 of clause 7.2.4, with the following specificities:

   - No APN is provided by the ePDG in the IDr payload of the final IKEv2 message.

7.3 Initial Attach Procedure for S2c in Untrusted Non-3GPP IP Access

This clause is related to the case when the UE powers-on in an untrusted network and host-based mobility management mechanism is used to establish IP connectivity and to perform inter-access Handover. Dual Stack MIPv6 [10] is used for supporting mobility over S2c interface.

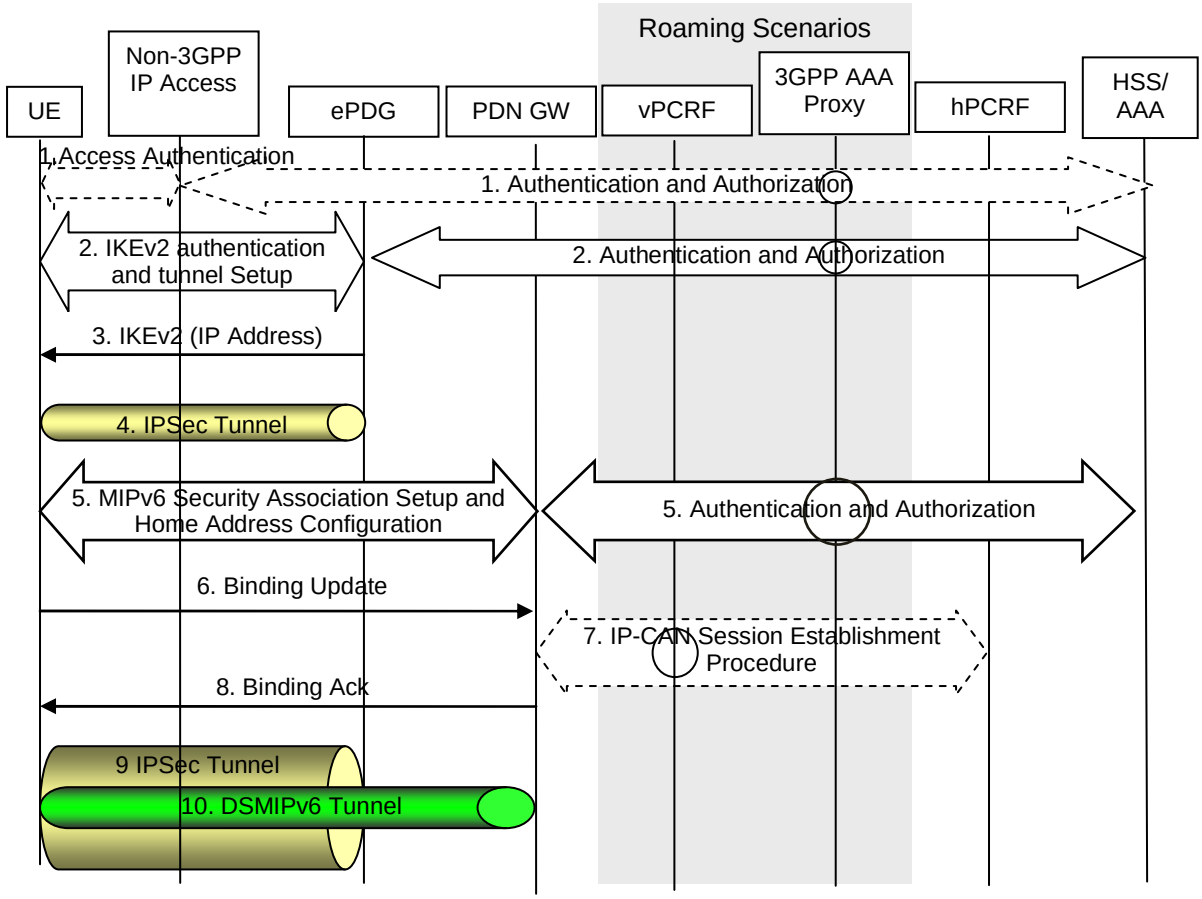


Figure 7.3-1: Initial attachment from Untrusted Non-3GPP IP Access with DSMIPv6

The non-roaming (Figure 4.2.2-2), Roaming (Figure 4.2.3-3) and LBO (Figure 4.2.3-5) are all covered in this procedure. In the Roaming and LBO case, the ePDG communicates with the 3GPP AAA Server by way of the 3GPP AAA Proxy, functioning as a relay for AAA messages. In the LBO case, the PDN GW in the VPLMN interacts with the PCRF by means of the vPCRF. In the non-roaming case, the 3GPP AAA Proxy and vPCRF are not involved.

This procedure is also used to establish the first PDN connection over an untrusted non-3GPP access with DSMIPv6 on S2c when the UE already has active PDN connections only over a 3GPP access and wishes to establish simultaneous PDN connections to different APNs over multiple accesses.

If dynamic policy provisioning is not deployed, the optional step 6 does not occur. Instead, the PDN GW may employ static configured policies.

1) The Access authentication procedure between UE and the 3GPP EPC may be performed as defined by TS 33.402 [45]. As part of the AAA exchange for network access authentication, the AAA/HSS and/or the 3GPP AAA Proxy may return to the Non-3GPP IP Access a set of home/visited operator's policies to be enforced on the usage of local IP address, or IPv6 prefix, allocated by the access system upon successful authentication. Subscription data is provided to the Non-3GPP IP Access by the HSS/AAA in this step. After the authentication, UE is configured with Local IP Address from the access network domain. This address is used for sending all IKEv2 [9] messages and as the source address on the outer header of the IPsec tunnel between the UE and the ePDG.

2) The IKEv2 tunnel establishment procedure is started by the UE. The UE may indicate in a notification part of the IKEv2 authentication request that it supports MOBIKE. The ePDG IP address to which the UE needs to form IPsec tunnel is discovered via DNS query as specified in clause 4.5.4. The procedure is as described in TS 33.402 [45].

3) The ePDG sends the final IKEv2 message with the assigned IP address in IKEv2 Configuration payloads.

4) IPsec Tunnel between the UE and ePDG is now setup.

5) A security association is established between UE and PDN GW to secure the DS-MIPv6 messages between UE and PDN GW. This step is performed as specified in step 4 of clause 6.3. During this step an IPv6 home network prefix is assigned by the PDN GW to the UE as defined in RFC 5026 [40]. After the IPv6 home network prefix is assigned, UE constructs a home address from it via auto-configuration.

6) The UE sends the Binding Update (IP Addresses (HoA, CoA)) message to the PDN GW. The Binding Update is as specified in RFC 5555 [10]. The UE may request an IPv4 Home Address in this step. The UE shall inform the PDN GW that the whole home prefix shall be moved.

7) The PDN GW executes a IP-CAN Session Establishment Procedure with the PCRF as specified in TS 23.203 [19]. The message from the PDG GW includes at least the HoA and the CoA. The message may also include a permanent UE identity and an APN string.

   The PCRF decides on the PCC rules and Event Triggers and provisions them to the PDN GW. The PDN GW installs the received PCC rules.

8) The PDN GW processes the binding update and creates a binding cache entry for the UE. The PDN GW allocates an IPv4 home address for the UE if requested by the UE in step 5 and allowed by the subscription profile received as it is specified in the E-UTRAN attach procedure in TS 23.401 [4]. The PDN GW then sends a Binding Ack to the UE, including the IPv4 home address allocated for the UE.

9) The IP Connectivity is now setup.

7.4 Detach and PDN Disconnection for S2b

7.4.1 UE/ePDG-initiated Detach Procedure and UE-Requested PDN Disconnection with PMIPv6 on S2b

7.4.1.1 Non-Roaming, Home Routed Roaming and Local Breakout Case

The procedure in this clause applies to Detach Procedures, initiated by UE or ePDG initiated detach procedure, and to the UE-requested PDN disconnection procedure when PMIPv6 is used on the S2b interface.

The UE can initiate the Detach procedure, e.g. when the UE is power off. The ePDG should initiate the Detach procedure due to administration reason or the IKEv2 tunnel releasing, when the ePDG should initiate the Detach procedure is implementation specific based on local operator policies.

For multiple PDN connectivity, this detach procedure shall be repeated for each PDN connected.

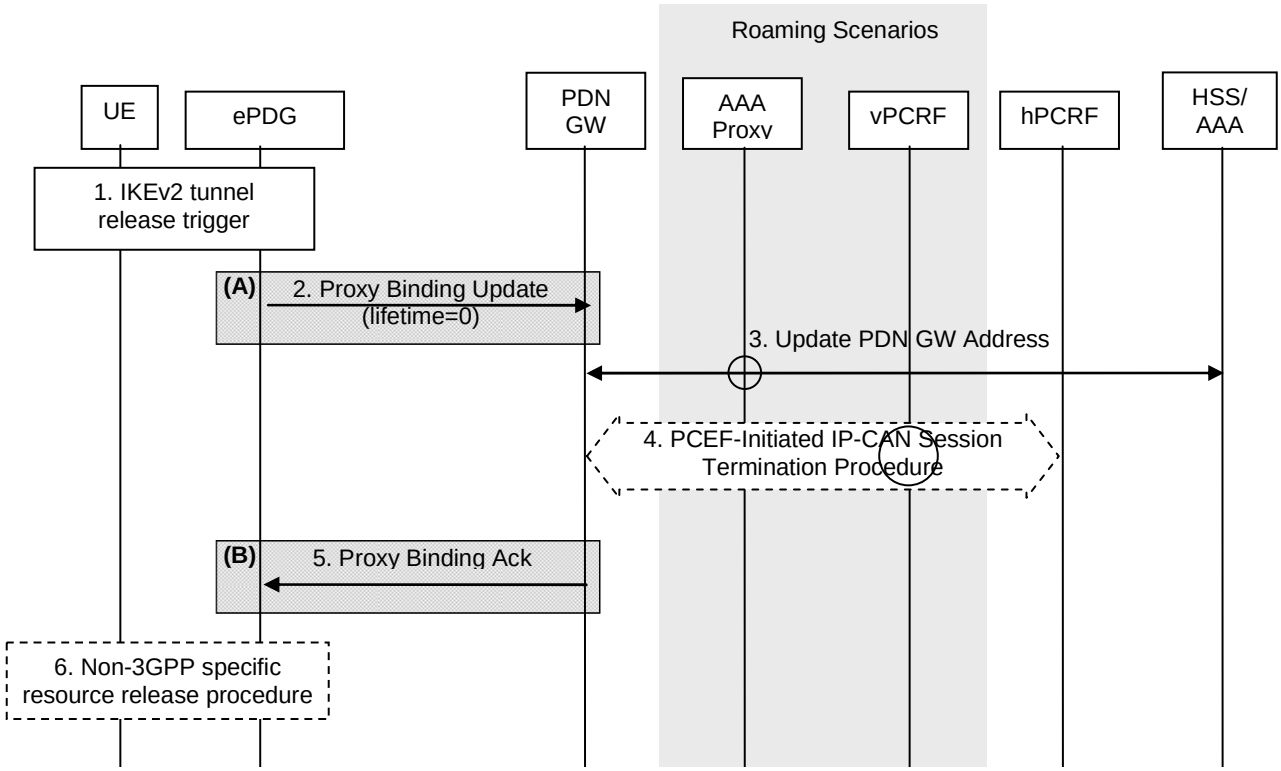


Figure 7.4.1-1: UE/ePDG-initiated detach procedure with PMIPv6 on S2b

NOTE: For GTP based S2b, procedure steps (A) and (B) are defined in clause 7.4.3.1.

The home routed roaming (Figure 4.2.3-1), LBO (Figure 4.2.3-4) and non-roaming (Figure 4.2.2-1) scenarios are depicted in the figure. In the LBO case, the 3GPP AAA Proxy acts as an intermediary, forwarding messages from the 3GPP AAA Server in the HPLMN to the PDN GW in the VPLMN and visa versa. Messages between the PDN GW in the VPLMN and the hPCRF in the HPLMN are forwarded by the vPCRF in the VPLMN. In the non-roaming case, the vPCRF and the 3GPP AAA Proxy are not involved.

If dynamic policy provisioning is not deployed, the optional step 4 does not occur. Instead, the PDN GW may employ static configured policies.

1) IKEv2 tunnel release triggers PMIP tunnel release.

2) The MAG in the ePDG should send a Proxy Binding Update (MN NAI, APN, lifetime=0) message to the PDN GW. When the MAG in the ePDG should send a Proxy Binding Update message to the PDN GW is implementation specific based on local operator policies. The MN NAI identifies the UE. When only one PDN connection to the given APN is allowed the APN is needed in order to determine which PDN to deregister the UE from, as some PDN GWs may support multiple PDNs. When multiple PDN connections to the given APN are supported, the APN and the PDN connection identity are needed in order to determine which PDN to deregister the UE from. The lifetime value set to zero, indicates this is a PMIP de-registration.

3) The PDN GW informs the 3GPP AAA Server of the PDN disconnection. If the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server notifies the HSS as described in clause 12.1.2.

4) The PDN GW deletes the IP CAN session associated with the UE and executes a PCEF-Initiated IP-CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [19].

5) The PDN GW deletes all existing entries for the indicated HoA from its Binding Cache and sends a Proxy Binding Ack (MN NAI, lifetime=0) message to the MAG in the ePDG. The PDN GW sends a Proxy Binding Ack message to the ePDG. The MN NAI value and the lifetime=0 values indicate that the UE has been successfully deregistered.

6) Non-3GPP specific resource release procedure is executed.

7.4.1.2 Chained PMIP-based S8-S2b Roaming Case

This procedure is described in clause 6.4.1.2.

7.4.2 HSS/AAA-initiated Detach Procedure with PMIPv6 on S2b

7.4.2.1 Non-Roaming, Home Routed Roaming and Local Breakout Case

HSS/AAA-initiated detach procedure when PMIPv6 is used on the S2b interface is illustrated in Figure 7.4.2-1. The HSS can initiate the procedure e.g. when the user's subscription is removed. The 3GPP AAA Server can initiate the procedure, e.g. instruction from O&M, timer for re-authentication/re-authorization expired.

If the HSS/AAA-initiated detach procedure has been initiated to delete the UE from the Evolved Packet Core, the HSS/AAA server shall initiate the detach procedure for each of the access systems to which the UE is registered.

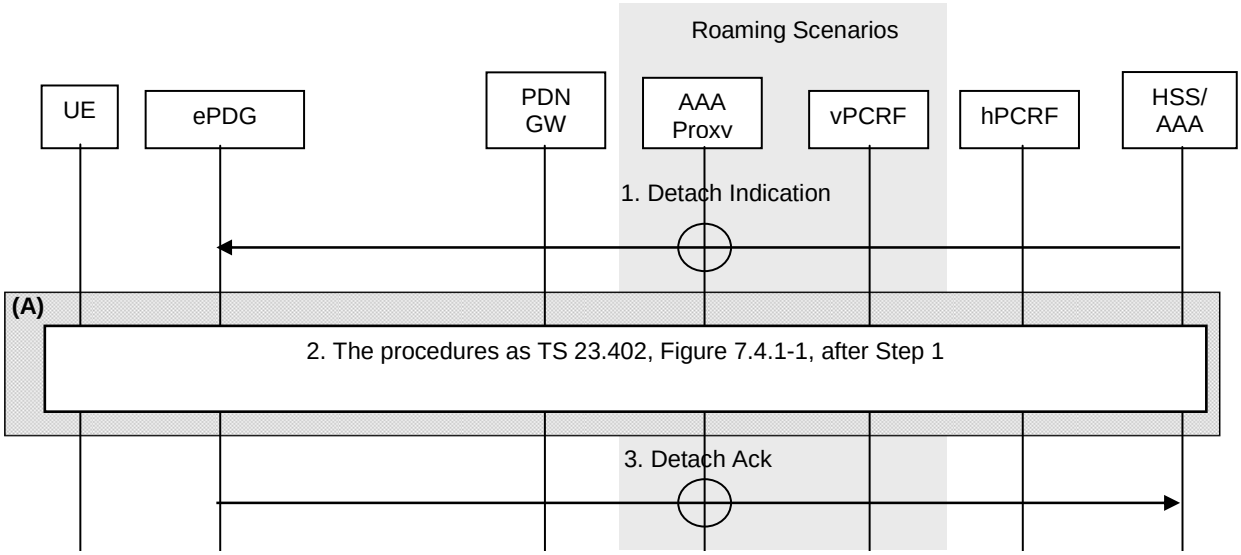


Figure 7.4.2-1: HSS/AAA-initiated detach procedure with PMIPv6 on S2b

NOTE 1: For GTP based S2b, procedure step (A) is defined in clause 7.4.4.1.

NOTE 2: AAA proxy and vPCRF are only used in the case of home routed roaming (Figure 4.2.3-1) and local breakout (Figure 4.2.3-4).

1) The HSS/AAA sends a detach indication message to the ePDG to detach a specific UE.

2) This include the procedure after step1 as Figure 7.4.1-1.

   For multiple PDN connectivity, this step shall be repeated for each PDN connected.

3) The ePDG sends a Detach Ack message to the 3GPP AAA Server. If the detach procedure was initiated from the 3GPP AAA Server and if the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server notifies the HSS as described in clause 12.1.2. If the detach procedure was initiated by HSS, the 3GPP AAA Server replies to the HSS as described in clause 12.1.3.

NOTE 3: The HSS/AAA may also send a detach indication message to the PDN GW. The PDN GW does not remove the PMIP tunnels on S2b, since the ePDG is responsible for removing the PMIP tunnels on S2b. The PDN GW acknowledges the receipt of the detach indication message to the 3GPP AAA Server.

7.4.2.2 Chained PMIP-based S8-S2b Roaming Case

This procedure is described in clause 6.4.2.2.

7.4.3 UE/ePDG-initiated Detach Procedure and UE-Requested PDN Disconnection with GTP on S2b

7.4.3.1 Non-Roaming, Home Routed Roaming and Local Breakout Case

This clause describes the UE-requested PDN disconnection procedure when GTP is used on the S2b interface.

The UE can initiate the Detach procedure, e.g. when the UE is power off. The ePDG should initiate the Detach procedure due to administration reason or the IKEv2 tunnel releasing. When the ePDG initiates the Detach procedure is implementation specific based on local operator policies.

For multiple PDN connectivity, this detach procedure shall be repeated for each PDN connected.

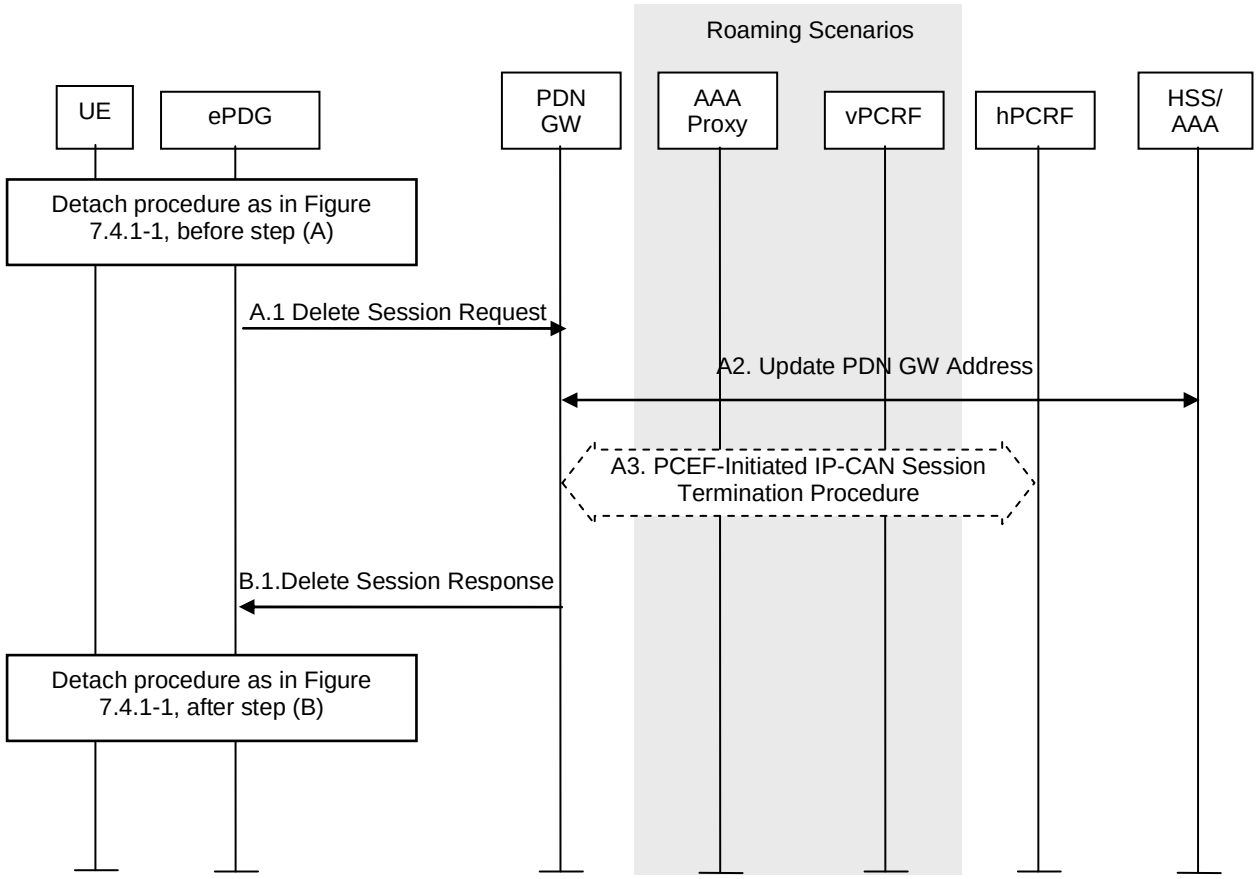


Figure 7.4.3-1: UE/ePDG-initiated detach procedure with GTP on S2b

The home routed roaming (Figure 4.2.3-1), LBO (Figure 4.2.3-4) and non-roaming (Figure 4.2.2-1) scenarios are supported as specified in clause 7.4.1.

A.1) The ePDG should release this particular PDN connection and should send a Delete Session Request (Linked EPS Bearer ID, UWAN Release Cause if available, User Location Information) message for this PDN connection to the PDN GW. When the ePDG should release this particular PDN connection and should send a Delete Session Request is implementation specific based on local operator policies. UWAN Release Cause is only sent by the ePDG to the PDN GW if this is permitted according to ePDG operator's policy.

The User Location Information shall include UE local IP address and optionally UDP source port number (if NAT is detected). It may also include WLAN Location Information (and its Age) the ePDG may have received from the 3GPP AAA server about the UE. When the PDN GW receives no WLAN Location Information from the ePDG it shall delete any such information it may have stored for the PDN connection.

NOTE : The UE local IP address is the source address on the outer header of the IPsec tunnel to the ePDG.

A.2) Same as step 3 of clause 7.4.1.1.

A.3) The PDN GW deletes the IP-CAN session associated with the UE and executes a PCEF-Initiated IP-CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [19]. If received from the ePDG, the PDN GW shall also forward the UWAN Release Cause, and PCRF shall forward it to the Application Function as specified in TS 23.203 [19]. If requested by the PCRF, the PDN GW forwards to the PCRF following information extracted from User Location Information it may have received from the ePDG:

- WLAN location information in conjunction with the Age of this information,
- The UE local IP address.

B.1) The PDN GW acknowledges with a Delete Session Response (Cause) message.

7.4.4 HSS/AAA-initiated Detach Procedure with GTP on S2b

7.4.4.1 Non-Roaming, Home Routed Roaming and Local Breakout Case

HSS/AAA-initiated detach procedure when GTP is used on the S2b interface is illustrated in Figure 7.4.4-1. The HSS can initiate the procedure e.g. when the user's subscription is removed. The 3GPP AAA Server can initiate the procedure, e.g. instruction from O&M, timer for re-authentication/re-authorization expired.

If the HSS/AAA-initiated detach procedure has been initiated to delete the UE from the Evolved Packet Core, the HSS/AAA server shall initiate the detach procedure for each of the access systems to which the UE is registered.

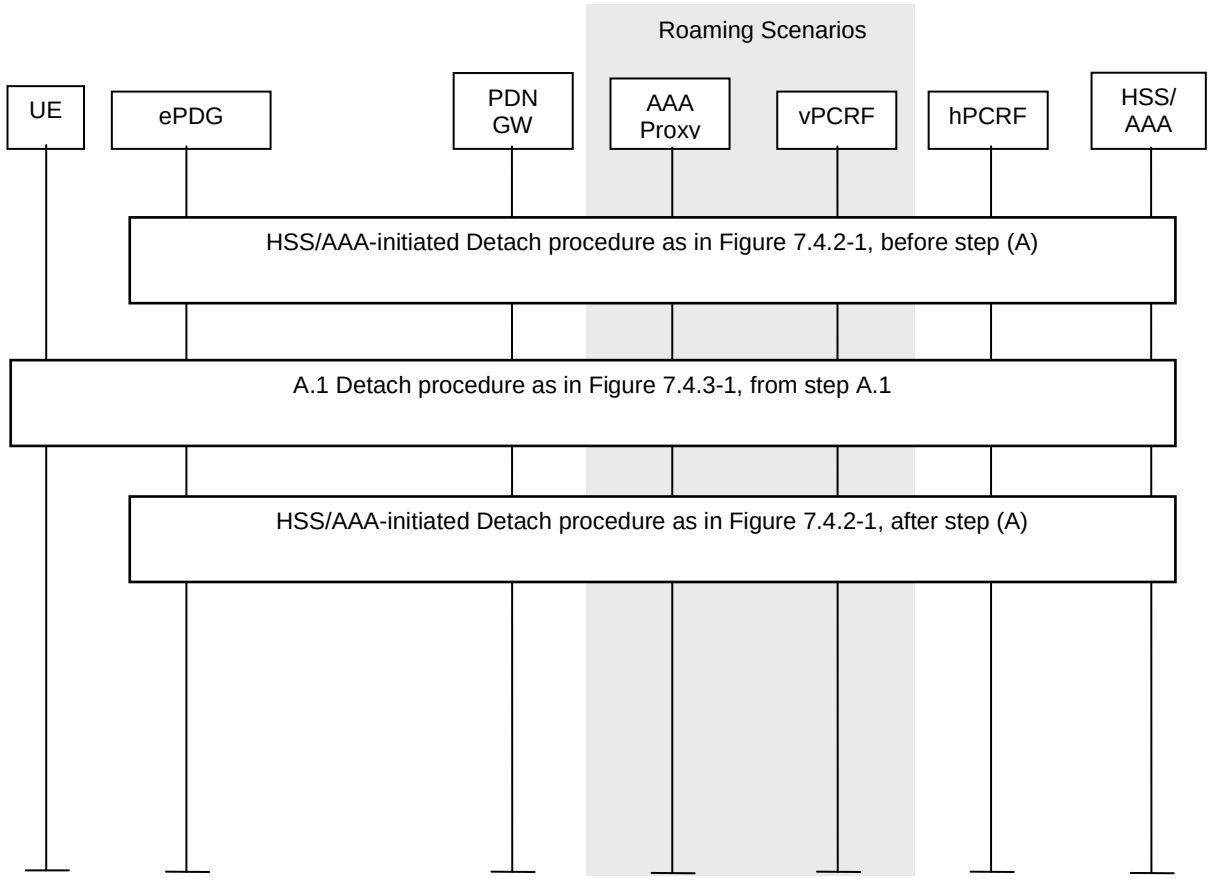


Figure 7.4.4-1: HSS/AAA-initiated detach procedure with GTP on S2b

A.1) For multiple PDN connectivity, this step shall be repeated for each PDN connected. This step does not apply to a PDN connection set-up for emergency services.

NOTE: The HSS/AAA may also send a detach indication message to the PDN GW. The PDN GW does not remove the GTP tunnels on S2b, since the ePDG is responsible for removing those tunnels on S2b. The PDN GW acknowledges the receipt of the detach indication message to the 3GPP AAA Server.

7.5 Detach and PDN Disconnection for S2c in Un-trusted Non-3GPP IP Access

7.5.1 General

This clause is related to the cases where at least one DSMIPv6 PDN disconnection procedure is performed. In case of detach the DSMIPv6 PDN disconnection is executed for all the existing PDNs connections, while in the case of disconnecting a single PDN connection the DSMIPv6 PDN disconnection is executed only for the individual PDN connection.

The DSMIPv6 PDN disconnection procedure is on a per PDN basis and allows:

- the UE to inform the network that it requests to release a S2c based PDN connection; and
- the network to inform the UE that a S2c based PDN connection is disconnected.

The UE may be disconnected from a PDN either explicitly or implicitly:

- Explicit PDN disconnection: The network or the UE explicitly requests detach and signal with each other;
- Implicit PDN disconnection: The network disconnects the UE from a PDN, without notifying the UE. This is typically the case when the network presumes that it is not able to communicate with the UE, e.g. due to radio conditions.

Three PDN disconnection procedures are provided when the UE accesses the EPS through S2c:

- UE-Initiated PDN disconnection Procedure;
- AAA/HSS- initiated detach Procedure.
- PDN GW-initiated PDN disconnection Procedure.

7.5.2 UE-Initiated PDN disconnection Procedure

The PDN disconnection procedure when initiated by the UE is illustrated in Figure 7.5.2-1. In case of detaching the UE from EPS, the procedure defined in this clause must be repeated for each PDN.

In the non-roaming case, none of the optional entities in Figure 7.5.2-1 are involved. The optional entities are involved in other cases. In the roaming cases, however, the 3GPP AAA Proxy relays all interaction between the 3GPP AAA Server in the HPLMN and the PDN GW in the VPLMN.

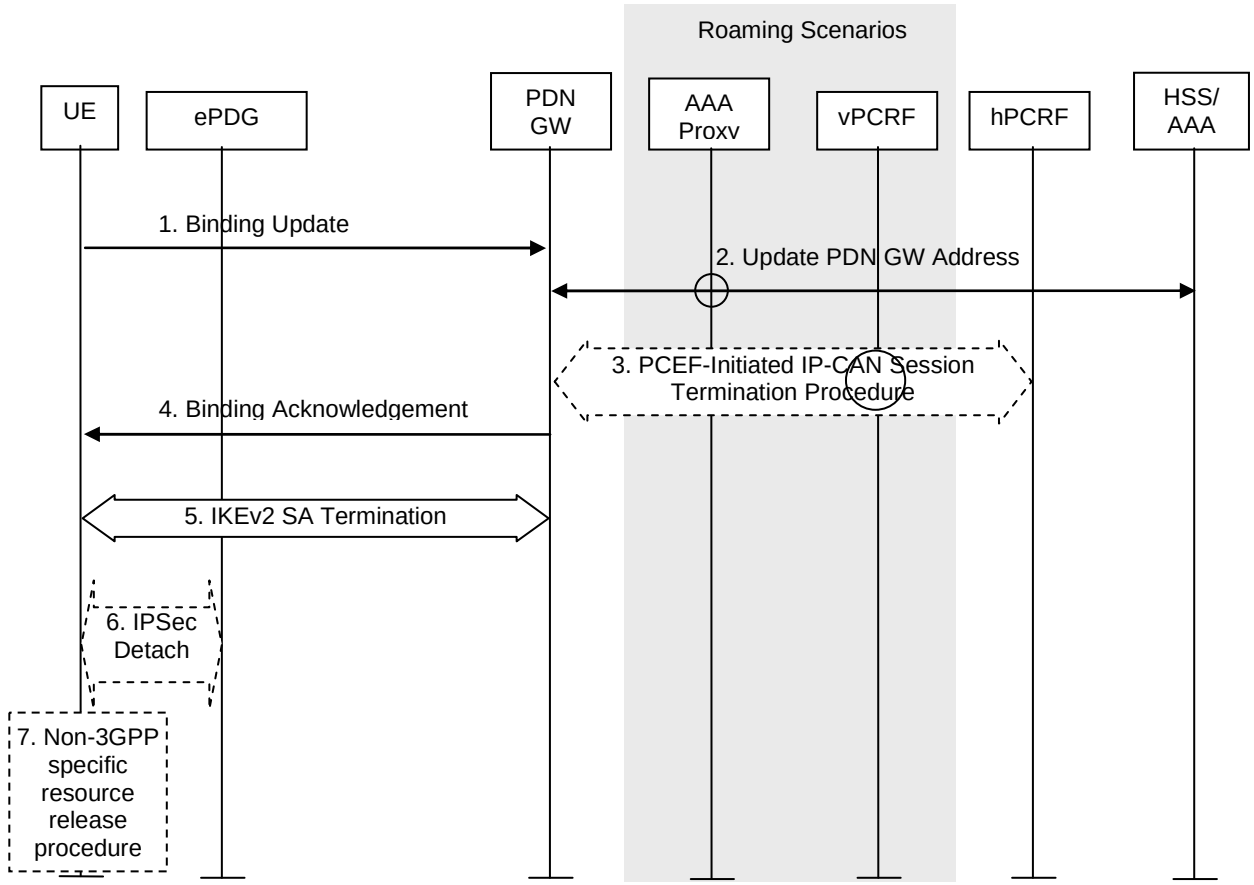


Figure 7.5.2-1: UE-initiated S2c PDN disconnection procedure in Untrusted Non-3GPP Access Network

Non-roaming (figure 4.2.2-2), home routed roaming (figure 4.2.3-3) and Local Breakout (figure 4.2.3-4) cases are supported by this procedure. The AAA proxy and vPCRF are only used in the case of home routed roaming and Local Breakout. In non-roaming scenarios, the AAA proxy and vPCRF are not involved.

If dynamic policy provisioning is not deployed, the optional step 3 does not occur. Instead, the PDN GW may employ static configured policies.

1. If the UE wants to terminate a S2c session, it shall send a de-registration Binding Update (Lifetime=0, IP Addresses (HoA, CoA)) message to the PDN GW as specified in RFC 5555 [10].

2. The PDN GW informs the 3GPP AAA Server of the PDN disconnection. If the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server notifies the HSS as described in clause 12.1.2.

3. If there is an active PCC session for the UE, the PDN GW executes a PCEF-Initiated IP-CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [19].

4. The PDN GW shall send a Binding Acknowledgement to the UE as specified in RFC 5555 [10].

5. The UE terminates the IKEv2 security association for the given PDN as defined in RFC 5996 [9].

6. If after step 5 the UE has no other PDN sessions, the UE should terminate the IPSEC tunnel to the ePDG according to RFC 5996 [9].

7. After IPsec tunnel termination, non-3GPP specific resource release procedure may be executed.

7.5.3 HSS / AAA-initiated Detach Procedure

The Detach procedure when initiated by the HSS/AAA is illustrated in Figure 7.5.3-1. The Detach procedure defined in this clause must be repeated for each PDN.

If the HSS/AAA-initiated detach procedure has been initiated to delete the UE from the Evolved Packet Core, the HSS/AAA server shall initiate the detach procedure for each of the access systems to which the UE is registered.

In the implicit detach, steps 2, 3 and 6 of Figure 7.5.3-1, are omitted.

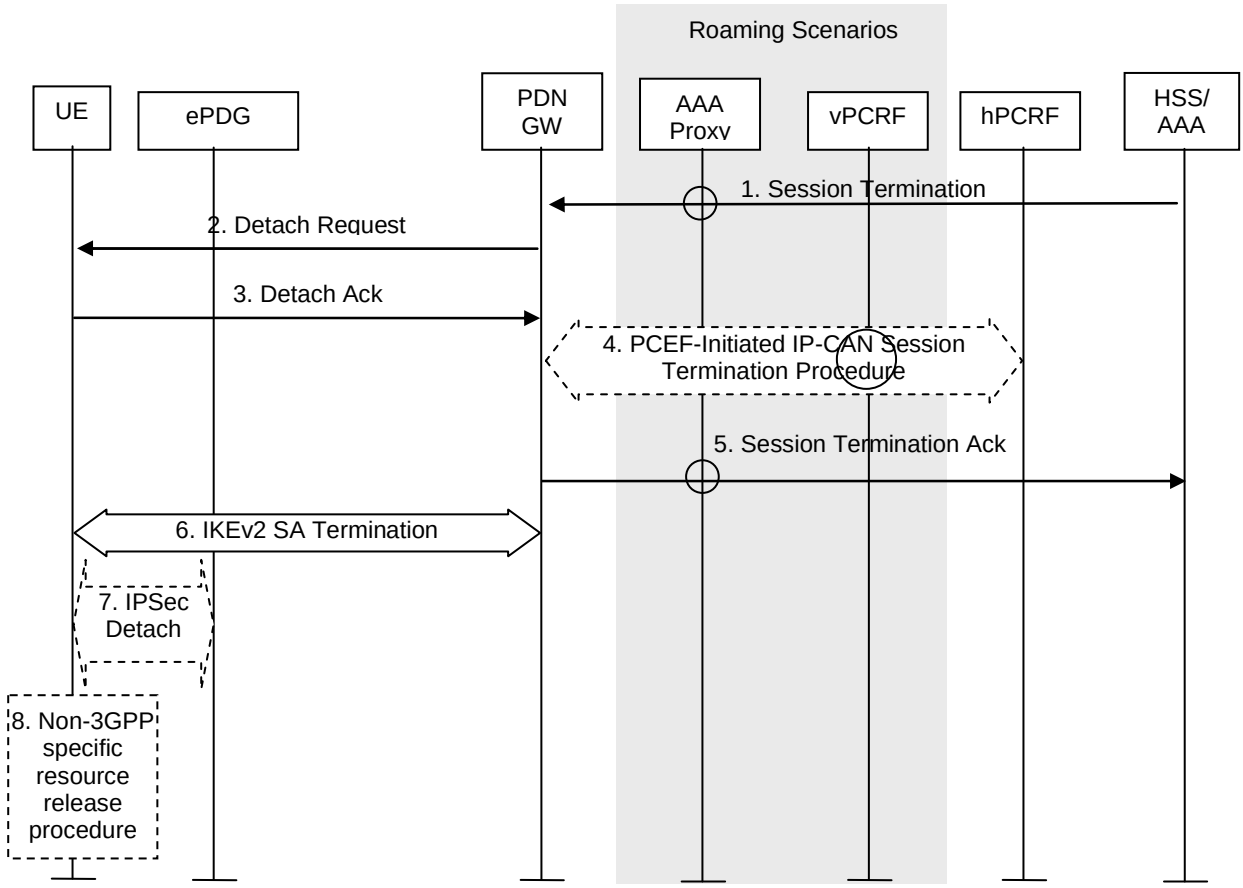


Figure 7.5.3-1: AAA/HSS-initiated S2c detach procedure in Untrusted Non-3GPP Access Network

Non-roaming (Figure 4.2.2-2), home routed roaming (figure 4.2.3-3) and Local Breakout (figure 4.2.3-4) cases are supported by this procedure. The AAA proxy and vPCRF are only used in the case of home routed roaming and Local Breakout. In non-roaming scenarios, the AAA proxy and vPCRF are not involved.

If dynamic policy provisioning is not deployed, the optional step 4 does not occur. Instead, the PDN GW may employ static configured policies.

1. If the HSS/AAA wants to request the immediate termination of a S2c session for a given UE and a given PDN, it shall send a Session Termination message to the PDN GW.

2. The PDN GW sends a detach request message.

3. The UE shall acknowledge the detach request.

NOTE 1: How the detach request and acknowledge messages are implemented is a stage 3 issue.

4. If there is an active PCC session for the UE, the PDN GW executes a PCEF-Initiated IP-CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [19].

5. The PDN GW shall acknowledge the termination of the S2c session to the 3GPP AAA Server. If the detach procedure was initiated from the 3GPP AAA Server and if the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server notifies the HSS as described in clause 12.1.2. If the detach procedure was initiated by HSS, the 3GPP AAA Server replies to the HSS as described in clause 12.1.3.

6. The PDN GW or the UE terminates the IKEv2 security association for the given PDN as defined in RFC 5996 [9].

7. If after step 6 the UE has no other PDN sessions, the UE should terminate the IPSEC tunnel to the ePDG according to RFC 5996 [9].

8. After IPsec tunnel termination, non-3GPP specific resource release procedure may be executed.

NOTE 2: The HSS/AAA may also send a detach indication message to ePDG. The HSS/AAA should wait to receive acknowledgement(s) from PDN GW(s) before sending the detach indication message to the ePDG. The ePDG releases the IPSEC tunnels to the UE and acknowledges the receipt of the detach indication message to the 3GPP AAA Server.

7.5.4 PDN GW-initiated PDN Disconnection Procedure

The PDN Disconnection procedure when initiated by the PDN GW is illustrated in Figure 7.5.4-1.

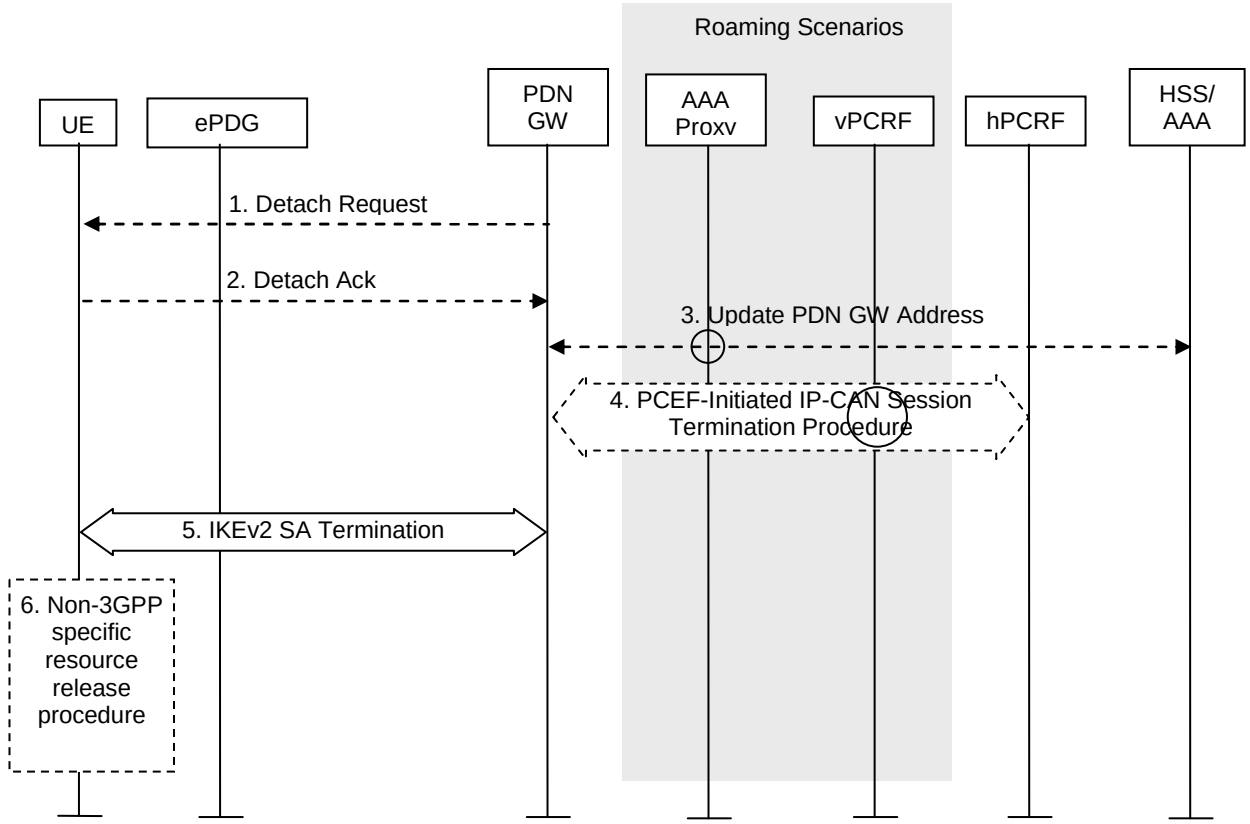


Figure 7.5.4-1: PDN GW- initiated PDN Disconnection S2c procedure in Untrusted Non-3GPP Access Network

Non-roaming (Figure 4.2.2-1), home routed roaming (Figure 4.2.3-2) and Local Breakout (Figure 4.2.3-4) cases are supported by this procedure. The 3GPP AAA proxy and vPCRF are only used in the case of home routed roaming and Local Breakout. In non-roaming scenarios, the 3GPP AAA proxy and vPCRF are not involved.

If dynamic policy provisioning is not deployed, the optional step 3 does not occur. Instead, the PDN GW may employ static configured policies.

static configured policies.

If the PDN GW-initiated PDN Disconnection Procedure is triggered by the UE binding lifetime expiration (Implicit PDN disconnection procedure), steps 1 and 2 may be omitted.

1. In the explicit detach procedure the PDN GW shall send a detach request message.

2. In the explicit detach procedure, the UE shall acknowledge the detach request.

NOTE: How the detach request and acknowledge messages are implemented is a stage 3 detail.

3. The PDN GW informs the 3GPP AAA Server of the PDN disconnection. If the PDN GW is in the VPLMN, signalling may be routed via a 3GPP AAA Proxy in the VPLMN. If the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server notifies the HSS as described in clause 12.1.2.

4. If there is an active PCC session for the UE, the PDN GW shall execute a PCEF-Initiated IP CAN Session Termination Procedure with the PCRF as specified in TS 23.203 [19].

5. The PDN GW or the UE may terminate the IKEv2 security association for the given PDN as defined in RFC 5996 [9].

6. After IKEv2 SA termination, non-3GPP specific resource release procedure may be executed.

7.6 UE-initiated Connectivity to Additional PDN

7.6.1 UE-initiated Connectivity to Additional PDN with PMIPv6 on S2b

NOTE: The PDN GW treats each MN-ID+APN as a separate binding and may allocate a new IP address/prefix for each binding.

This clause is related to the case when the UE has an established PDN connection over untrusted non-3GPP access with PMIPv6 on S2b and wishes to establish one or more additional PDN connections over such untrusted access. This procedure is also used to request for connectivity to an additional PDN over untrusted non-3GPP access with PMIPv6 on S2b when the UE is simultaneously connected to such untrusted access and a 3GPP access, and the UE already has active PDN connections over both the accesses. Since PMIPv6 is used to establish connectivity with the additional PDN, the UE establishes a separate SWu instance (i.e. a separate IPSec tunnel) for each additional PDN.

There can be more than one PDN connection per APN if both the ePDG and the PDN GW support that feature. When multiple PDN connections to a given APN are supported, during the establishment of a new PDN connection, the ePDG creates and sends a PDN Connection identity to the PDN GW. The PDN connection identity is unique in the scope of the UE and the APN within an ePDG, i.e. the MN-ID, the APN, and the PDN connection identity together identify a PDN connection within an ePDG. In order to be able to identify a specific established PDN connection, both the ePDG and the PDN GW shall store the PDN Connection identity. Sending the PDN connection identity is an indication that the ePDG supports multiple PDN connections to a single APN and the PDN GW shall be able to indicate if it supports multiple PDN connections to a single APN. Between the UE and the ePDG the IPSec SA associated with the PDN connection identifies the PDN connection.

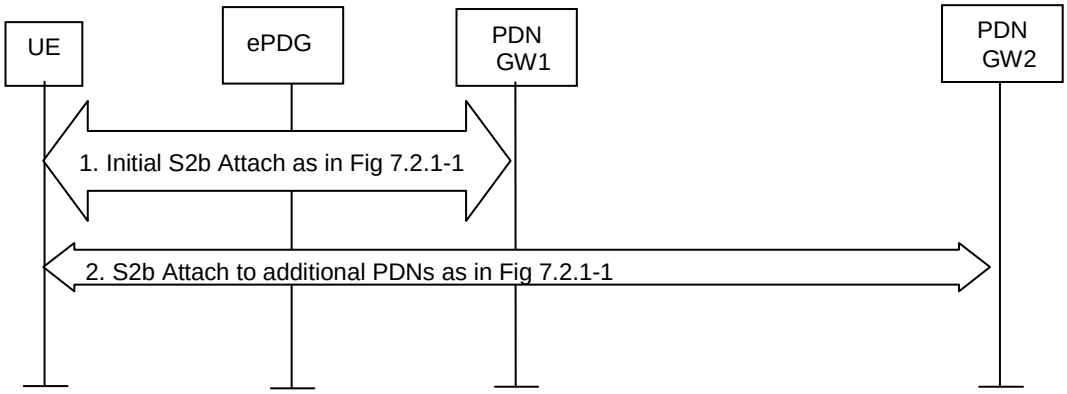


Figure 7.6.1-1: UE-initiated connectivity to additional PDN from Un-trusted Non-3GPP IP Access with PMIPv6

1) The UE has performed the Initial S2b Attach procedure as defined in clause 7.2.1, Figure 7.2.1-1 and has an established PDN connection.

2) The UE repeats the procedure of clause 7.2.1, Figure 7.2.1-1 for each additional PDN the UE wants to connect to, with the following exceptions:

   a) The IKEv2 tunnel establishment procedure for each additional PDN connection is initiated with the ePDG that was selected in step 1;

b) The APN information corresponding to the requested PDN connection is conveyed with IKEv2 as specified in TS 33.402 [45];

c) For network supporting multiple mobility protocols, if there was any dynamic IPMS decision in step 1, the AAA/HSS enforces the same IPMS decision for each additional PDN connection.

7.6.2 UE-initiated Connectivity to Additional PDN from Un-trusted Non-3GPP IP Access with DSMIPv6 on S2c

This clause is related to the case when the UE powers-on in an untrusted network and host-based mobility management mechanism is used for obtaining connectivity. Dual Stack MIPv6 [10] is used for supporting mobility over S2c interface. This case covers the scenario when UE obtains connectivity with one or more additional PDNs at any time after initial attach Since host-based mobility mechanisms are used, the procedure is similar to the initial attach procedure. This procedure is also used to request for connectivity to an additional PDN over untrusted non-3GPP access with DSMIPv6 on S2c when the UE is simultaneously connected to such untrusted access and a 3GPP access, and the UE already has active PDN connections over both the accesses.

NOTE: Based on the MN-ID and APN, the PDN GW may allocate a new IP address/prefix for a new binding.

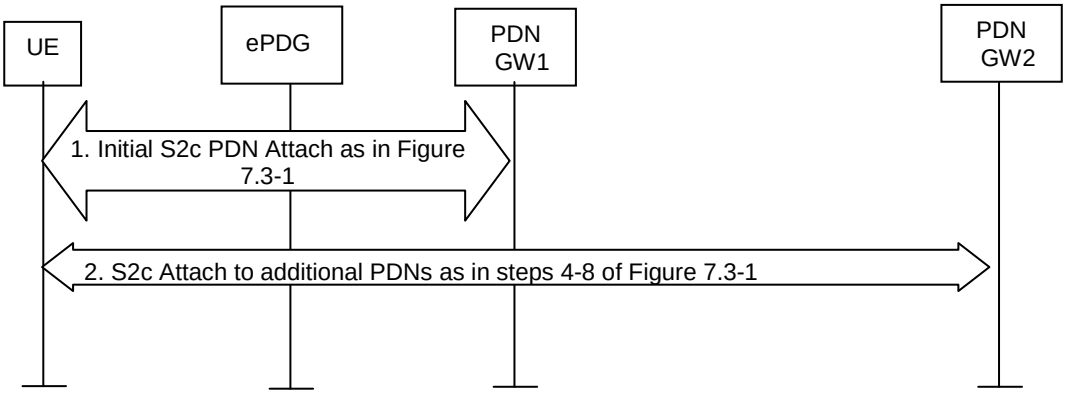


Figure 7.6.2-1: UE-initiated connectivity to additional PDN from Un-trusted Non-3GPP IP Access with DSMIPv6

When the initial attachment is performed, the UE performs procedures described in clause 7.3, Figure 7.3-1, to obtain connectivity with a PDN GW and a specific PDN. If at any time the UE wants to obtain connectivity with additional PDNs, since DSMIPv6 is used to obtain connectivity, the UE repeats only steps 4-8 of Figure 7.3-1.

1) The UE performs initial S2c PDN Attach procedure as defined in clause 7.3, Figure 7.3-1.

2) The UE repeats steps 4-8 of clause 7.3, Figure 7.3-1 for each additional PDN the UE wants to connect to. This step can be performed and repeated at any time after step 1 for one or multiple PDNs.

7.6.3 UE-initiated Connectivity to Additional PDN with GTP on S2b

NOTE: The PDN GW treats each IMSI+APN as a separate PDN connection and may allocate a new IP address/prefix for each PDN connection.

This clause is related to the case when the UE has an established PDN connection over untrusted non-3GPP access with GTP on S2b and wishes to establish one or more additional PDN connections over such untrusted access. This procedure is also used to request for connectivity to an additional PDN over untrusted non-3GPP access with GTP on S2b when the UE is simultaneously connected to such untrusted access and a 3GPP access, and the UE already has active PDN connections over both the accesses. Since GTP is used to establish connectivity with the additional PDN, the UE establishes a separate SWu instance (i.e. a separate IPSec tunnel) for each additional PDN.

There can be more than one PDN connection per APN when GTP is used between the ePDG and the PDN GW. During the establishment of a new PDN connection, the ePDG allocates and sends a default EPS bearer ID to the PDN GW. The default EPS bearer ID is unique in the scope of the UE within an ePDG, i.e. the IMSI and the default EPS bearer ID together identify a PDN connection within an ePDG. In order to be able to identify a specific established PDN

connection, both the ePDG and the PDN GW shall store the default EPS bearer ID. Between the UE and the ePDG the IPSec SA associated with the PDN connection identifies the PDN connection.

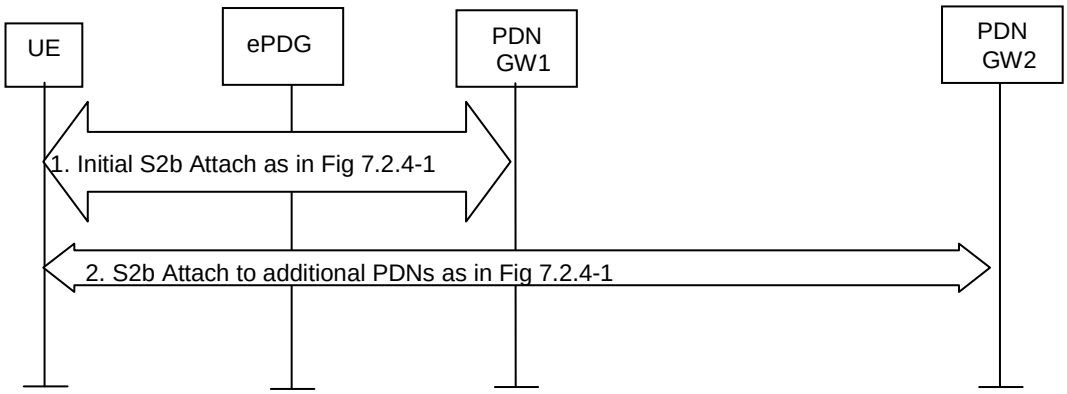


Figure 7.6.3-1: UE-initiated connectivity to additional PDN from Un-trusted Non-3GPP IP Access with GTP

1) The UE has performed the Initial GTP based S2b Attach procedure as defined in clause 7.2.4, Figure 7.2.4-1 and has an established PDN connection.

2) The UE repeats the procedure of clause 7.2.4, Figure 7.2.4-1 for each additional PDN the UE wants to connect to, with the following exceptions:

   a) The IKEv2 tunnel establishment procedure for each additional PDN connection is initiated with the ePDG that was selected in step 1;

   b) The APN information corresponding to the requested PDN connection is conveyed with IKEv2 as specified in TS 33.402 [45];

   c) For network supporting multiple mobility protocols, if there was any dynamic IPMS decision in step 1, the AAA/HSS enforces the same IPMS decision for each additional PDN connection.

7.7 Void

7.8 S2c Bootstrapping via DSMIPv6 Home Link over an Un-Trusted Access

When the UE is connected on an un-trusted non-3GPP access considered to be DSMIPv6 home link for the UE based on clause 4.5.6, the UE may trigger the establishment of S2c IKEv2 SA, e.g. to optimize future handovers to other accesses using S2c. For each PDN connection, the S2c IKEv2 SA establishment has to be performed separately.

NOTE: An un-trusted non-3GPP access can be defined as DSMIPv6 Home Link in addition to the 3GPP access.

Once the UE is attached to the PDN over the un-trusted non-3GPP access, the procedure describing the bootstrapping is in clause 15.1.

7.9 PDN GW initiated Resource Allocation Deactivation

7.9.1 PDN GW initiated Resource Allocation Deactivation with PMIPv6 on S2b

This procedure is performed to release all the resources associated with the PDN address, for example, due to IP CAN session modification requests from the PCRF or due to handover Non-3GPP to 3GPP. When it is performed for an handover, the connections associated with the PDN address are released, but the PDN address is kept in the PDN GW.

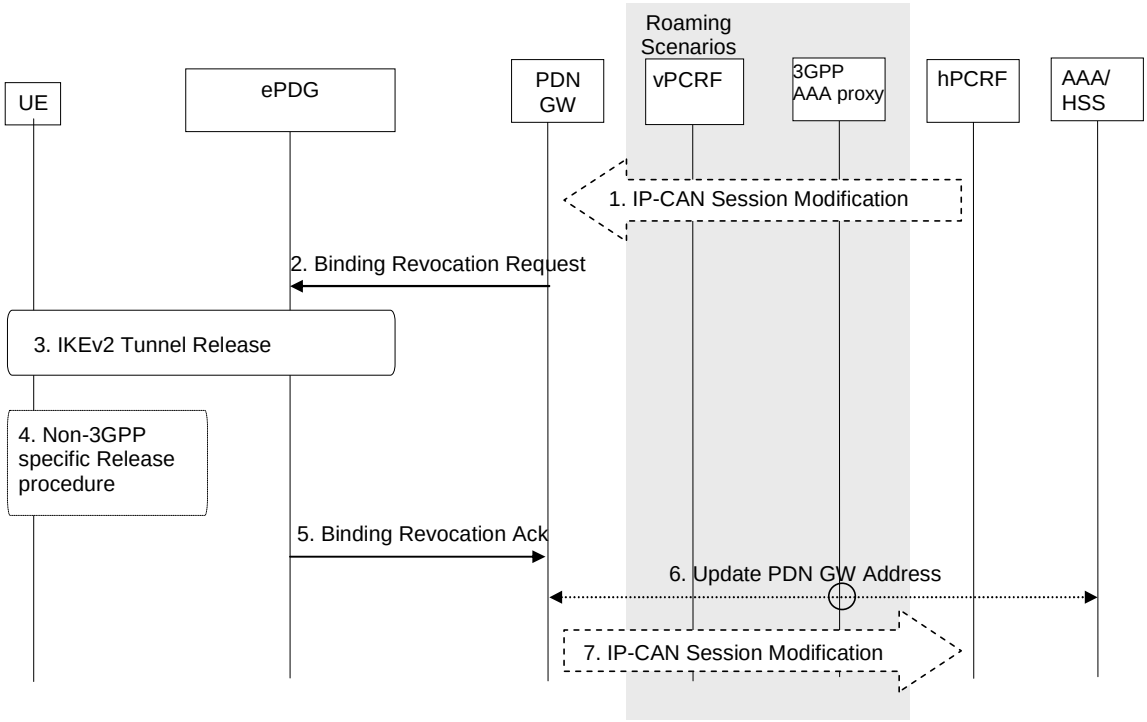


Figure 7.9-1: PDN GW Initiated Resource Allocation Deactivation with PMIPv6 on s2b

The PDN GW initiated resource allocation deactivation procedure for S2b PMIP reference point is defined in the following.

1. If dynamic PCC is deployed, the PDN GW initiated Resource Allocation Deactivation procedure may for example be triggered due to 'IP CAN session Modification procedure', as defined in TS 23.203 [19]. In this case, the resources associated with the PDN connection in the PDN GW are released.

   The PDN GW initiated Resource Allocation Deactivation can also be triggered during handovers from Non-3GPP to 3GPP.

2. The PDN GW sends a Binding Revocation Indication message to the trusted non-3GPP IP access.

3. The IKEv2 tunnel release is triggered from the ePDG if all bearers belonging to the PDN connection are released.

4. The resources may be released in the non-3GPP IP access.

5 The ePDG send a Buinding Revocation Acknowledgement message to the PDN GW.

6. In the case where the resources corresponding to the PDN connection are released in PDN GW, the PDN GW informs the 3GPP AAA Server of the PDN disconnection. If the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server notifies the HSS as described in clause 12.1.2.

7. The PDN GW indicates to the PCRF whether the requested PCC decision was successfully enforced by completing the PCRF-initiated IP CAN Session Modification procedure or the PCEF initiated IP-CAN Session Modification procedure as defined in TS 23.203 [19], proceeding after the completion of IP CAN bearer signalling.

7.9.2 PDN GW initiated Resource Allocation Deactivation with GTP on S2b

This procedure can be used to deactivate a dedicated bearer or deactivate all bearers belonging to a PDN address, for example, due to IP CAN session modification requests from the PCRF or due to handover from Non-3GPP to 3GPP access. If the default bearer belonging to a PDN connection is deactivated, the PDN GW deactivates all bearers belonging to the PDN connection.

When it is performed for a handover, the connections associated with the PDN address are released, but the PDN address is kept in the PDN GW.

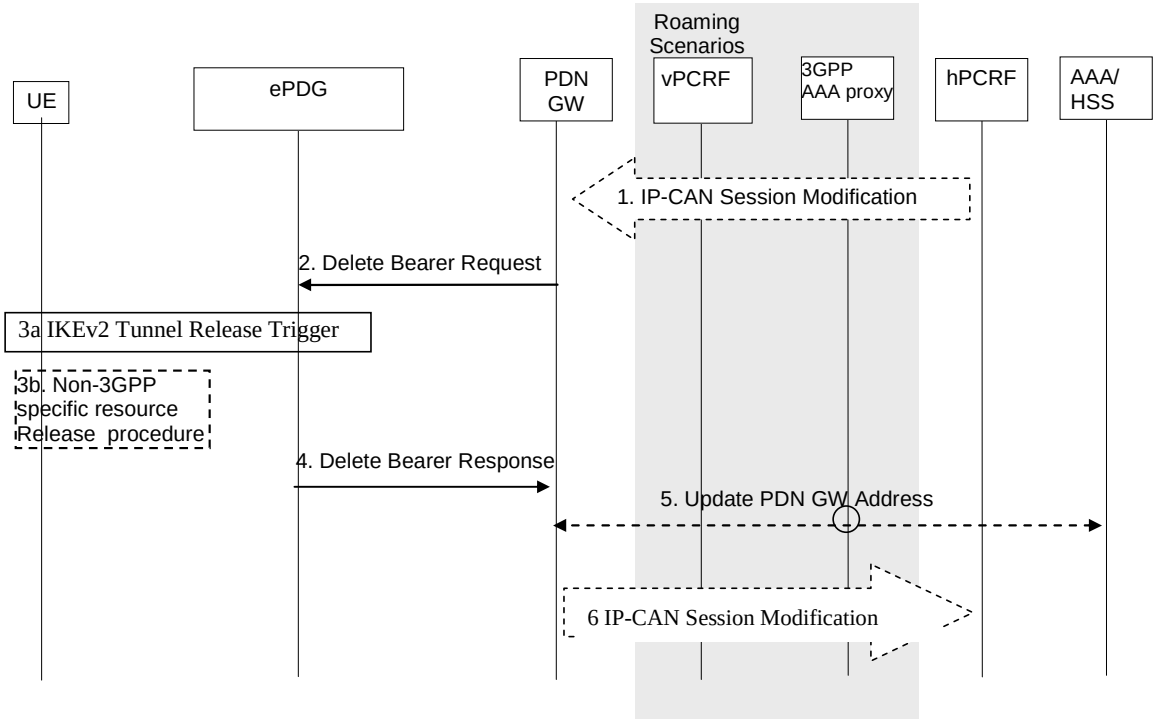


Figure 7.9.2-1: PDN GW Initiated Bearer Deactivation with GTP on S2b

This procedure applies to the Non-Roaming (Figure 4.2.2-1), Roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-4) cases. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF. In the non-roaming and home routed roaming cases, the vPCRF is not involved at all.

The optional interaction steps between the PDN GW and the PCRF in the procedures in figure 7.9.2.1-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured within the PDN GW.

1. If dynamic PCC is deployed, the PDN GW initiated Bearer Deactivation procedure may for example be triggered due to 'IP CAN session Modification procedure', as defined in TS 23.203 [19]. In this case, the resources associated with the PDN connection in the PDN GW are released. The PCRF may also include a request to provide the User Location Info to the PDN GW.

   The PDN GW initiated Resource Allocation Deactivation can also be triggered during handovers from Non-3GPP to 3GPP.

2. The PDN GW sends a Delete Bearer Request message (EPS Bearer Identity or Linked EPS Bearer Identity, Cause) to the ePDG. The Linked EPS Bearer Identity shall be present and set to the identity of the default bearer associated with the PDN connection if the PDN GW requests to release all the bearers of the PDN connection. Otherwise, the EPS Bearer Identity shall be present and set to the identity of the dedicated S2b bearer(s) to release if the PDN GW requests to deactivate dedicated S2b bearer(s).

3a. The IKEv2 tunnel release is triggered from the ePDG if all bearers belonging to the PDN connection are released.

3b. The resources may be released in the non-3GPP IP access.

4. The ePDG deletes the bearer contexts related to the Delete Bearer Request, and acknowledges the bearer deactivation to the PDN GW by sending a Delete Bearer Response (EPS Bearer Identity, User Location Information) message.

   The User Location Information shall include UE local IP address and optionally UDP source port number (if NAT is detected). It may also include WLAN Location Information (and its Age) the ePDG may have received from the 3GPP AAA server about the UE. When the PDN GW receives no WLAN Location Information from the ePDG it shall delete any such information it may have stored for the PDN connection.

NOTE: The UE local IP address is the source address on the outer header of the IPsec tunnel to the ePDG.

5. In the case where the resources corresponding to the PDN connection are released in PDN GW, the PDN GW informs the 3GPP AAA Server of the PDN disconnection. If the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server notifies the HSS as described in clause 12.1.2.

6. The PDN GW deletes the bearer context related to the deactivated EPS bearer. If the dedicated bearer deactivation procedure was triggered by receiving a PCC decision message from the PCRF, the PDN GW indicates to the PCRF whether the requested PCC decision was successfully enforced by completing the PCRF-initiated IP CAN Session Modification procedure or the PCEF initiated IP-CAN Session Modification procedure as defined in TS 23.203 [19], proceeding after the completion of IP CAN bearer signalling. If requested by the PCRF, the PDN GW forwards to the PCRF following information extracted from User Location Information it may have received from the ePDG:

   - WLAN location information in conjunction with the Age of this information,
   - The UE local IP address.

7.10 Dedicated S2b bearer activation with GTP on S2b

The dedicated bearer activation procedure for GTP based S2b is depicted in figure 7.10-1.

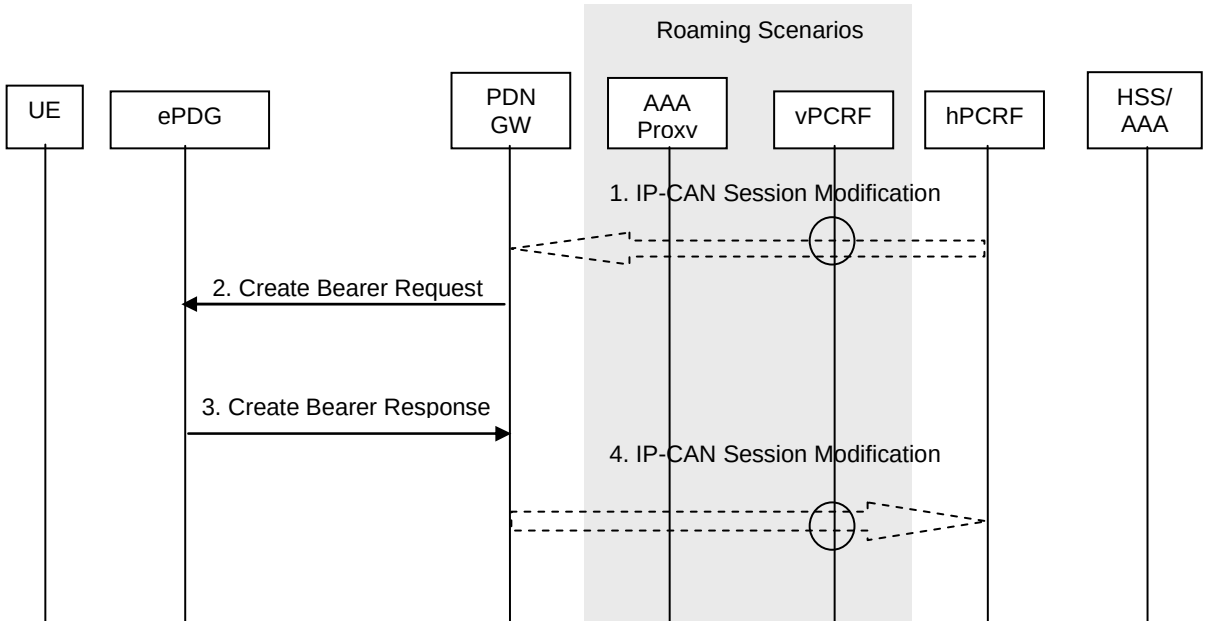


Figure 7.10-1: Dedicated S2b Bearer Activation Procedure with GTP on S2b

1. If dynamic PCC is deployed, the PCRF sends a PCC decision provision (QoS policy) message to the PDN GW. This corresponds to the initial steps of the PCRF-Initiated IP CAN Session Modification procedure or to the PCRF response in the PCEF initiated IP-CAN Session Modification procedure as defined in TS 23.203 [19], up to the point that the PDN GW requests IP CAN Bearer Signalling. If dynamic PCC is not deployed, the PDN GW may apply local QoS policy. The PCRF may also include a request to provide the User Location Info to the PDN GW.

2. The PDN GW uses this QoS policy to assign the EPS Bearer QoS, i.e., it assigns the values to the bearer level QoS parameters QCI, ARP, GBR and MBR. If this dedicated bearer is created as part of the handover from 3GPP access with GTP-based S5/S8, then the PDN GW applies the Charging ID already in use for the corresponding dedicated bearer while the UE was in 3GPP access (i.e. bearer with the same QCI and ARP as in 3GPP access). Otherwise, the PGW generates a new Charging Id for the dedicated bearer. The PDN GW sends a Create Bearer Request message (IMSI, EPS Bearer QoS, TFT, PDN GW Address for the user plane, PDN GW TEID of the user plane, Charging Id, LBI) to the ePDG. The Linked EPS Bearer Identity (LBI) is the EPS Bearer Identity of the default bearer.

3. The ePDG selects an EPS Bearer Identity, which has not yet been assigned to the UE. The ePDG then stores the EPS Bearer Identity and links the dedicated bearer to the default bearer indicated by the Linked EPS Bearer Identity (LBI). The ePDG uses the uplink packet filter (UL TFT) to determine the mapping of uplink traffic flows to the S2b bearer. The ePDG then acknowledges the S2b bearer activation to the PGW by sending a Create Bearer Response (EPS Bearer Identity, ePDG Address for the user plane, ePDG TEID of the user plane, User Location Information) message.

   The User Location Information shall include UE local IP address and optionally UDP source port number (if NAT is detected). It may also include WLAN Location Information (and its Age) the ePDG may have received from the 3GPP AAA server about the UE. When the PDN GW receives no WLAN Location Information from the ePDG it shall delete any such information it may have stored for the PDN connection.

NOTE: The UE local IP address is the source address on the outer header of the IPsec tunnel to the ePDG.

4. If the dedicated bearer activation procedure was triggered by a PCC Decision Provision message from the PCRF, the PDN GW indicates to the PCRF whether the requested PCC decision (QoS policy) could be enforced or not, allowing the completion of the PCRF-Initiated IP CAN Session Modification procedure or the PCEF initiated IP-CAN Session Modification procedure as defined in TS 23.203 [19], after the completion of IP CAN bearer signalling. If requested by the PCRF, the PDN GW forwards to the PCRF following information extracted from User Location Information it may have received from the ePDG:

   - WLAN location information in conjunction with the Age of this information,

   - The UE local IP address.

NOTE 1: The exact signalling of step 1 and 4 (e.g. for local break-out) is outside the scope of this specification. This signalling and its interaction with the dedicated bearer activation procedure are to be specified in TS 23.203 [19]. Steps 1 and 4 are included here only for completeness.

NOTE 2: This procedure does not aim at providing QoS differentiation over untrustred non 3GPP access networks. It is used to establish the same number of bearers on S2b that were or will be established when the UE hands over from/to a 3GPP access.

7.11 S2b bearer modification with GTP on S2b

7.11.1 PDN GW initiated bearer modification

The PDN GW initiated bearer modification procedure for a GTP based S2b is depicted in figure 7.11.1-1. This procedure is used to update the TFT for an active default or dedicated S2b bearer, or in cases when one or several of the EPS Bearer QoS parameters QCI, GBR, MBR or ARP are modified (including the QCI or the ARP of the default S2b bearer e.g. due to the HSS Initiated Subscribed QoS Modification procedure, as described in clause 7.11.2).

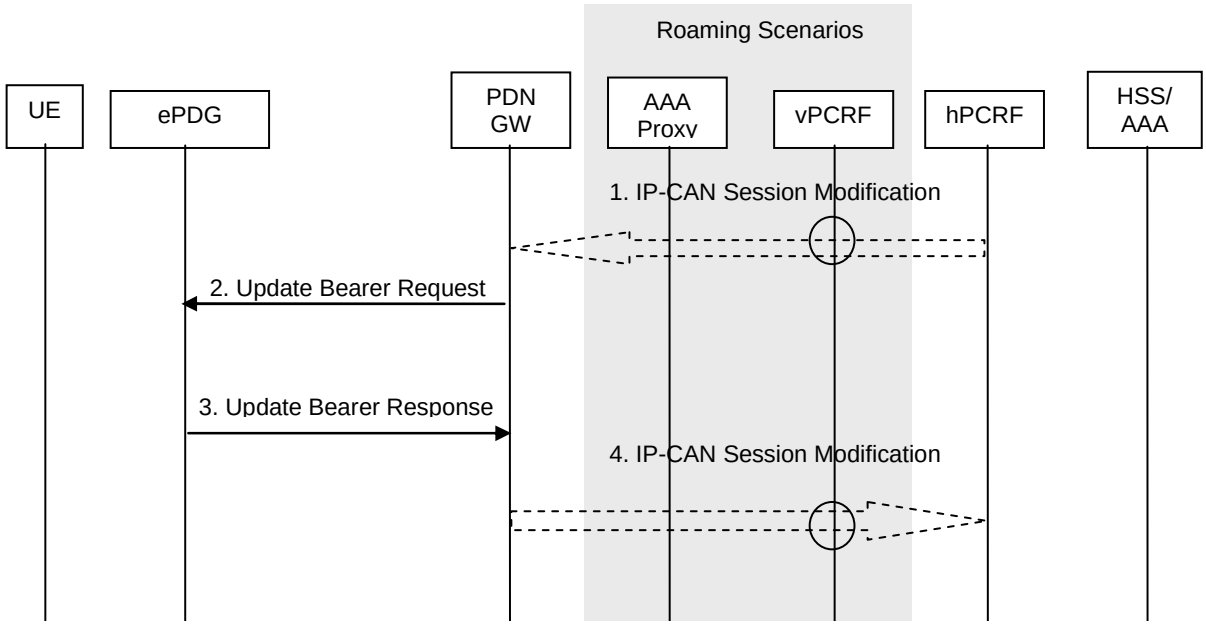


Figure 7.11.1-1: S2b Bearer Modification Procedure with GTP on S2b

1. If dynamic PCC is deployed, the PCRF sends a PCC decision provision (QoS policy) message to the PDN GW. This corresponds to the initial steps of the PCRF-Initiated IP CAN Session Modification procedure or to the PCRF response in the PCEF initiated IP-CAN Session Modification procedure as defined in TS 23.203 [19], up to the point that the PDN GW requests IP CAN Bearer Signalling. If dynamic PCC is not deployed, the PDN GW may apply local QoS policy. The PCRF may also include a request to provide the User Location Info to the PDN GW.

2. The PDN GW uses this QoS policy to determine that a service data flow shall be aggregated to or removed from an active S2b bearer or that the authorized QoS of a service data flow has changed. The PDN GW generates the TFT and updates the EPS Bearer QoS to match the traffic flow aggregate. The PDN GW then sends the Update Bearer Request (EPS Bearer Identity, EPS Bearer QoS, TFT) message to the ePDG.

3. The ePDG uses the uplink packet filter (UL TFT) to determine the mapping of traffic flows to the S2b bearer and acknowledges the S2b bearer modification to the PGW by sending an Update Bearer Response (EPS Bearer Identity, User Location Information) message.

   The User Location Information shall include UE local IP address and optionally UDP source port number (if NAT is detected). It may also include WLAN Location Information (and its Age) the ePDG may have received from the 3GPP AAA server about the UE. When the PDN GW receives no WLAN Location Information from the ePDG it shall delete any such information it may have stored for the PDN connection.

NOTE 1: The UE local IP address is the source address on the outer header of the IPsec tunnel to the ePDG.

4. If the Bearer modification procedure was triggered by a PCC Decision Provision message from the PCRF, the PDN GW indicates to the PCRF whether the requested PCC decision (QoS policy) could be enforced or not by sending a Provision Ack message allowing the completion of the PCRF-Initiated IP CAN Session Modification procedure or the PCEF initiated IP-CAN Session Modification procedure as defined in TS 23.203 [19], after the completion of IP CAN bearer signalling. If requested by the PCRF, the PDN GW forwards to the PCRF following information extracted from User Location Information it may have received from the ePDG:

   - WLAN location information in conjunction with the Age of this information,

   - The UE local IP address.

NOTE 2: The exact signalling of step 1 and 4 (e.g. for local break-out) is outside the scope of this specification. This signalling and its interaction with the bearer activation procedure are to be specified in TS 23.203 [19]. Steps 1 and 4 are included here only for completeness.

7.11.2 HSS Initiated Subscribed QoS Modification

The HSS Initiated Subscribed QoS Modification for a GTP-based S2b is depicted in figure 7.11.2-1. This procedure does not apply to PDN connections for emergency services.

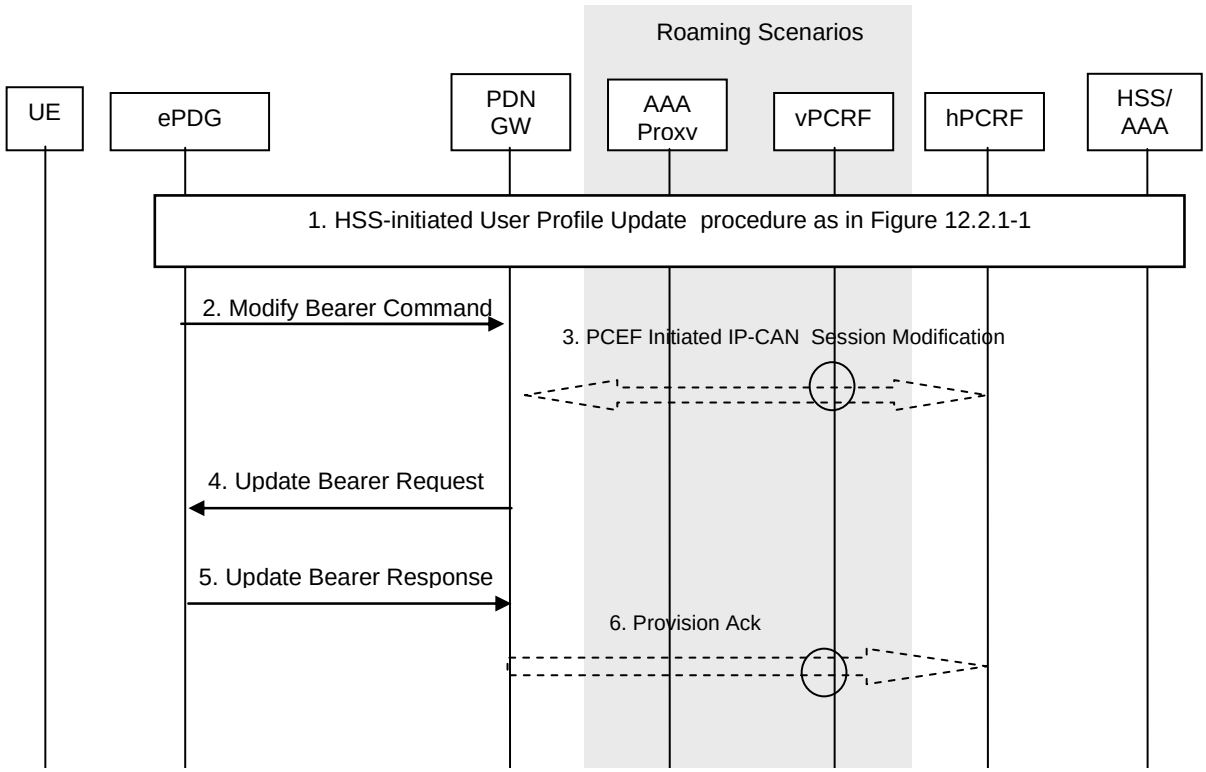


Figure 7.11.2-1: HSS Initiated Subscribed QoS Modification

1. The HSS updates the User Profile as specified in clause 12.2.1.

2. If the QCI and/or ARP and/or subscribed APN-AMBR has been modified and there is a related active PDN connection with the modified QoS Profile, the ePDG sends the Modify Bearer Command (EPS Bearer Identity, EPS Bearer QoS, APN AMBR) message to the PGW. The EPS Bearer Identity identifies the default bearer of the affected PDN connection. The EPS Bearer QoS contains the EPS subscribed QoS profile to be updated.

3. If PCC infrastructure is deployed, the PDN GW informs the PCRF about the updated EPS Bearer QoS. The PCRF sends new updated PCC decision to the PDN GW. This corresponds to the PCEF-initiated IP CAN Session Modification procedure as defined in TS 23.203 [19].

   The PCRF may modify the APN-AMBR and the QoS parameters (QCI and ARP) associated with the default bearer in the response to the PDN GW as defined in TS 23.203 [19].

4. The PDN GW modifies the default bearer of each PDN connection corresponding to the APN for which subscribed QoS has been modified. If the subscribed ARP parameter has been changed, the PDN GW shall also modify all dedicated S2 bearers having the previously subscribed ARP value unless superseded by PCRF decision. The PDN GW then sends the Update Bearer Request (EPS Bearer Identity, EPS Bearer QoS, TFT, APN AMBR) message to the ePDG.

5. The ePDG acknowledges the bearer modification to the PDN GW by sending an Update Bearer Response (EPS Bearer Identity) message. If the bearer modification fails the PDN GW deletes the concerned S2b Bearer.

8. The PDN GW indicates to the PCRF whether the requested PCC decision was enforced or not by sending a Provision Ack message.

8 Handovers without Optimizations Between 3GPP Accesses and Non-3GPP IP Accesses

8.1 Common Aspects for Handover without Optimizations for Multiple PDNs

This clause describes the common aspects of handover for connectivity with multiple PDNs.

The support of multiple PDNs has the following impacts on the handover procedures for single PDN connectivity:

- Upon handover from 3GPP access to non-3GPP access, and from non-3GPP access to 3GPP access, if the UE has multiple PDN connections to different APNs in the source access and the UE is capable of routing different simultaneously active PDN connections through different access networks, the UE may transfer from the source to the target access all the PDN connections that were active in source access before handover or only a subset of them, with the restriction that multiple PDN connections to the same APN shall be kept in one access.

- Upon handover from 3GPP access to non-3GPP access, and from non-3GPP access to another non-3GPP access, using S2a or S2b, during the access authentication the HSS/AAA returns to the Trusted Non-3GPP Access or the ePDG the PDN GW identity and the associated APN for each PDN the UE is connected to. For non-3GPP accesses that support UE to establish connectivity to PDNs after attach, the UE performs an attach to the target non-3GPP access indicating that it is a handover, resulting in the UE being connected to one PDN, and the UE establishes connectivity with the remaining PDNs that are being transferred from the 3GPP system using the UE-initiated Connectivity to Additional PDN procedure.

- If the UE hands over between 3GPP access and a non-3GPP access and the UE has more than one PDN connection to a given APN in the source access and multiple PDN connections to a single APN are not supported via the target access, only one PDN connection to the given APN will be established in the target access. In this case, the following applies:

  a) If dynamic PCC is deployed and the PCRF receives a Gateway Control Session Establishment Request from the target BBERF indicating an IP-CAN type different from 3GPP access, the PCRF shall select one of the IP-CAN sessions for this APN and continue with the BBERF relocation procedure for that PDN connection.

  b) When the PDN GW receives a PBU over PMIP-based S2a or S2b or S5/S8, the PDN GW shall select one of the PDN connections for this APN and continue with the handover procedure for that PDN connection. The PDN GW shall terminate the remaining PDN connections for that APN without removing the PDN GW information in HSS. If dynamic PCC is deployed, the PDN GW informs the PCRF about the deactivated PDN connections using the PCEF initiated IP-CAN session termination procedure as described in TS 23.203 [19].

  c) Whenever the PDN GW receives a PBU containing an IPv6 prefix or an IPv4 address associated to one of the PDN connections and the IPv6 prefix or the IPv4 address is valid, the PDN GW shall use the IPv6 prefix or the IPv4 address to select the PDN connection out of the active PDN connections. When the information is not included in the PBU, the PDN GW and PCRF shall select the latest PDN connection out of the active PDN connections for the given APN (i.e. the PDN connection that was activated last out of the active PDN connections for the given APN).

  NOTE 1: The UE may disconnect from certain PDN connections while still in the 3GPP access to ensure that there is only one PDN connection per APN when handing over to non-3GPP access.

- If the UE hands over between 3GPP access and a non-3GPP access and the UE has more than one PDN connection to a given APN in the source access and multiple PDN connections to a single APN is supported in the target access the following applies:

  a) All PDN connections to the same APN shall be handed over.

  b) When the PDN GW receives the request to establish a PDN connection to the given APN, the PDN GW shall select one of the PDN connections for this APN and continue with the handover procedure for that PDN connection.

c) When S2c is used and it is bootstrapped before the handover to a foreigner link the home address identifies the PDN connection and the PDN GW shall select the PDN connection accordingly.

NOTE 2: As all PDN connections to a single APN are moved during a handover, the UE initiates the PDN connection re-establishment over the new access network for all of the PDN connections to the given APN. Therefore there is no need for the UE to indicate which of its PDN connections to the given APN is moved with a particular PDN connection establishment request. The UE learns which of its PDN connections is moved as a result of a PDN connection establishment request from the assigned IPv6 prefix/IPv4 address.

NOTE 3: There is no relation between the values of the PDN connection identities used over S2a/S2b and the EPS bearer identities used within 3GPP networks. If GTP is used on S2b, there is no relation between the values of the EPS bearer identities used within 3GPP networks and non-3GPP networks.

- Upon handover from non-3GPP access to 3GPP access, if the MME has changed since the last detach or if there is no valid Subscriber context for the UE in the MME, or if the ME identity has changed, during the access authentication the HSS returns the Subscriber Data to the MME, including the PDN GW identity and the associated APN for each PDN the UE is connected to before the handover. The UE performs an attach to the 3GPP access with and indication for "handover" and then establishes connectivity with the remainder of PDNs that it was connected with over the non-3GPP system before the handover, using UE requested PDN connectivity specified in TS 23.401 [4]. The UE provides an indication of "handover" by providing Request Type indicating "handover" in the PDN connectivity request message as specified in TS 23.401 [4].

- For connectivity based on S2c:

  - Upon handover from 3GPP access to non-3GPP access, and from non-3GPP access to another non-3GPP access, the UE performs DSMIPv6 bootstrapping (if not yet performed) and binding procedures for each PDN connection that is being transferred from the source to the target access.

  - Upon handover from non-3GPP access, the UE de-registers the DSMIPv6 binding for each PDN connection that is being transferred from the source to the target access.

NOTE 4: If some IP traffic had been routed over WLAN as a result of 3GPP RAT mobility (e.g. from E-UTRAN to UTRAN), a UE can use an implementation-dependent hysteresis mechanism (e.g. based on an implementation dependent timer) to prevent the ping-pong such as traffic being handed back to the original RAT (e.g. E-UTRAN) again in a short period of time.

8.2 Handovers between non-3GPP IP access with PMIPv6 on S2a/S2b and 3GPP Access

8.2.1 Handover from Trusted or Untrusted Non-3GPP IP Access with PMIPv6 on S2a/S2b to 3GPP Access

8.2.1.1 General Procedure for GTP based S5/S8 for E-UTRAN Access

The steps involved in the handover from a trusted or untrusted non-3GPP IP access to E-UTRAN connected to EPC are depicted below for both the non-roaming and roaming cases and when PMIPv6 is used on S2a or S2b. It is assumed that while the UE is served by the trusted or untrusted non-3GPP IP access, a PMIPv6 tunnel is established between the non-3GPP access network and the PDN GW in the EPC.

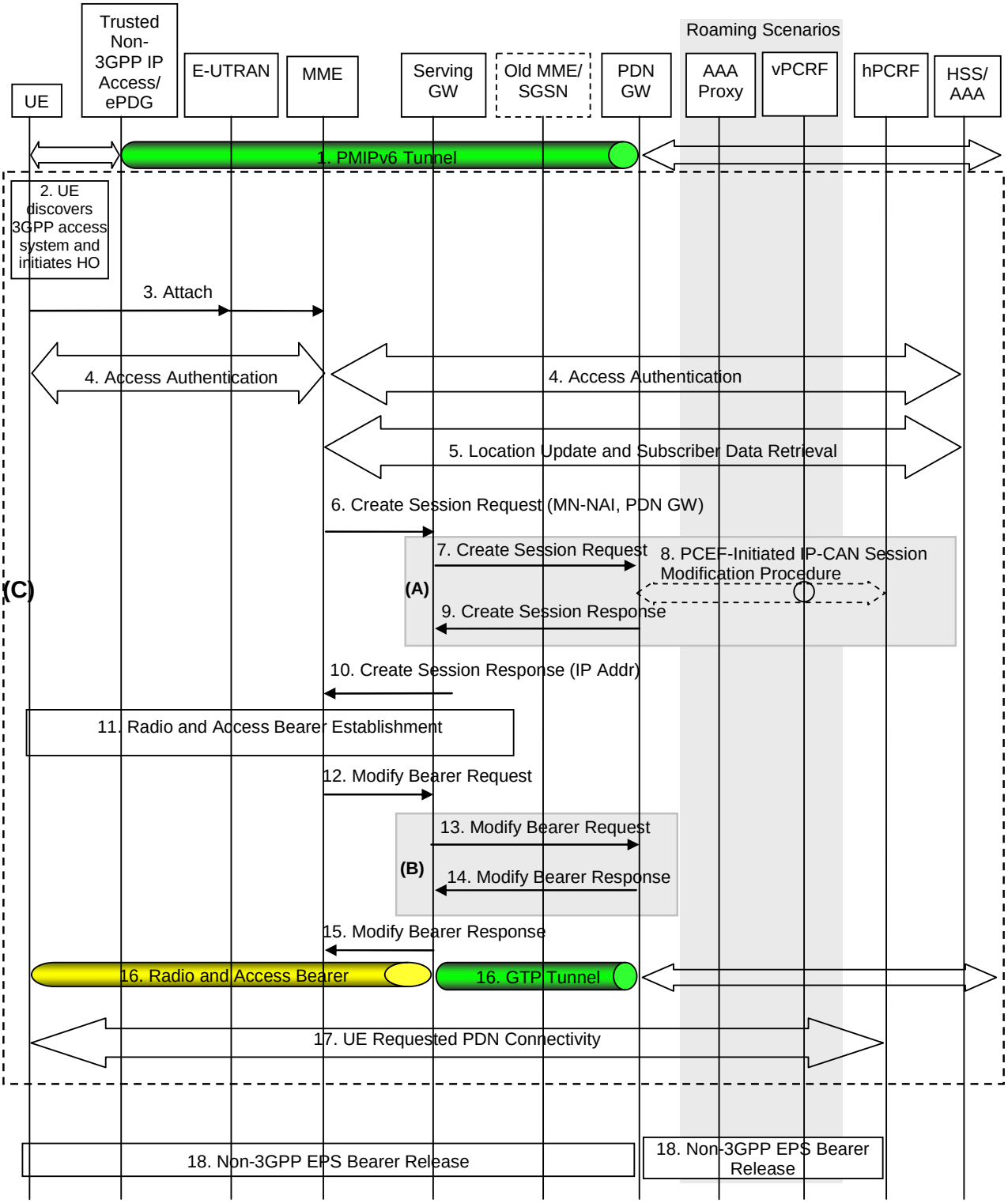


Figure 8.2.1.1-1: Handover from Trusted or Untrusted Non-3GPP IP Access to E-UTRAN with PMIPv6 on S2a or S2b and GTP on S5/S8 interfaces

NOTE 1: All steps outside of (A) and (B) are common for architecture variants with GTP-based S5/S8 and PMIP-based S5/S8. Procedure steps (A) and (B) for PMIP-based S5/S8 are described in clause 8.2.1.2.

NOTE 2: All steps inside of (C) are common for architecture variants with GTP-based S2b and PMIP-based S2b. Procedure for steps outside of (C) for GTP-based S2b are described in clause 8.6.1.1.

In case of connectivity to multiple PDNs the following applies:

- If the UE is connected to both 3GPP access and non-3GPP access before the handover of PDN connections to 3GPP access is triggered, steps 2 to 16 shall be skipped and the UE shall only perform step 17 for each PDN connection that is being transferred from non-3GPP access.

- If the UE is connected only to non-3GPP access before the handover of PDN connections to 3GPP access is triggered, steps 2 to 16 shall be performed. In step 3 the UE should provide the APN corresponding to one of the PDN connections that are being transferred from non-3GPP access. If the APN is not provided, and the subscription context from HSS contains a PDN GW identity corresponding to the default APN, the MME shall use the PDN GW corresponding to the default APN as specified in TS 23.401 [4]. The UE shall then repeat step 17 for each of the remaining PDN connections that are being transferred from non-3GPP access.

- Step 18 shall be repeated for each PDN connection that is being transferred from non-3GPP access.

The steps in 17 can occur in parallel for each PDN. Other impacts related to the handover for multiple PDNs are described in clause 8.1.

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

Both the roaming (Figure 4.2.1-2) and non-roaming (Figure 4.2.1-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the Serving GW in the VPLMN. The vPCRF receives the Acknowledgment from the Serving GW and forwards it to the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

The steps involved in the handover are discussed below.

1) The UE uses a trusted or untrusted non-3GPP access system and is being served by PDN GW (as PMIPv6 LMA).

2) The UE discovers the E-UTRAN access and determines to transfer its current sessions (i.e. handover) from the currently used non-3GPP access system to E-UTRAN. The mechanisms that aid the UE to discover the 3GPP Access system, are specified in clause 4.8 (Network Discovery and Selection).

3) The UE sends an Attach Request to the MME with Request Type indicating "Handover" Attach. The message from the UE is routed by E-UTRAN to the MME as specified in TS 23.401 [4] (E-UTRAN). The UE should include any one of the APNs, corresponding to the PDN connections in the source non-3GPP access. The APN is provided as specified in TS 23.401 [4].

4) The MME may contact the HSS and authenticate the UE as described in TS 23.401 [4].

5) After successful authentication, the MME may perform location update procedure and subscriber data retrieval from the HSS as specified in TS 23.401 [4]. Since theRequest Type is "Handover", the PDN GW identity conveyed to the MME will be stored in PDN subscription context. The MME receives information on the PDNs the UE is connected to over the non-3GPP access in the Subscriber Data obtained from the HSS.

6) The MME selects an APN, a serving GW and PDN GW as described in TS 23.401 [4]. The MME sends a Create Session Request (including IMSI, MME Context ID (SGSN equivalent is TBD), PDN-GW address, Handover Indication, APN) message to the selected Serving GW. Since the Request Type is "Handover", a Handover Indication information is included.

7) The Serving GW sends a Create Session Request (Handover Indication) message to the PDN-GW in the VPLMN or HPLMN as described in TS 23.401 [4]. Since the MME includes Handover Indication information in Create Session Request message, the Serving GW includes this information in Create Session Request message.

   Since Handover Indication is included, the PDN GW should not switch the tunnel from non-3GPP IP access to 3GPP access system at this point.

8) Since Handover Indication is included, the PDN GW may execute a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19] to report e.g. change in IP-CAN type. If the UE had disconnected from the default PDN before handover then the PDN GW executes a PCEF initiated IP CAN Session Establishment procedures as described in TS 23.203 [19].

   Since Handover Indication is included in step 7, the PDN GW defers any modification to the PCC Rules (due to changes received from the PCRF, if there is PCRF interaction) and still applies the existing PCC Rules for charging and policy until step 13.

Depending on the active PCC rules, the establishment of dedicated bearers for the UE may be required. The establishment of dedicated bearers in combination with the default takes place as described in Annex F of TS 23.401 [4].

NOTE 3: Depending upon the support of the piggybacking feature in the network, the dedicated bearer can be created as part of default bearer establishment or immediately afterwards.

NOTE 4: PDN GW address and Serving GW address selection is as described in the clause "GW selection" in TS 23.401 [4].

9) The PDN GW responds with a Create Session Response message to the Serving GW as described in TS 23.401 [4].The Create Session Response contains the IP address or the prefix that was assigned to the UE while it was connected to the non-3GPP IP access. It also contains the Charging Id previously assigned to the PDN connection in the non-3GPP access although the Charging Id still applies to the non-3GPP access.

10) The Serving GW returns a Create Session Response message to the MME as specified in TS 23.401 [4]. This message also includes the IP address of the UE. This message also serves as an indication to the MME that the S5 bearer setup and update has been successful. At this step the PMIPv6 or GTP tunnel(s) over S5 are established.

11) Radio and Access bearers are established at this step in the 3GPP access as specified in TS 23.401 [4].

12) The MME sends a Modify Bearer Request (eNodeB address, eNodeB TEID, Handover Indication) message to the Serving GW.

13) Since the Handover Indication is included in step 12), the Serving GW sends a Modify Bearer Request message to the PDN GW to prompt the PDN GW to tunnel packets from non 3GPP IP access to 3GPP access system and immediately start routing packets to the Serving GW for the default and any dedicated EPS bearers established.

    In this step, the PDN GW applies any modification to the PCC Rules received from the PCRF, if there is PCRF interaction in step 8. The Charging Id previously in use for the PDN connection in the non-3GPP access now only applies to the default bearer in use in E-UTRAN access. If dedicated bearers are created, a new Charging Id is assigned by the PGW for each of them according to TS 23.401 [4].

NOTE 5: Steps 13 and 14 are not performed if the PDNs are reconnected after handoff by the UE in step 17.

14) The PDN GW acknowledges by sending Modify Bearer Response to the Serving GW.

15) The Serving GW acknowledges by sending Modify Bearer Response (EPS Bearer Identity) message to the MME.

16) The UE sends and receives data at this point via the E-UTRAN system.

17) For connectivity to multiple PDNs, the UE establishes connectivity to each PDN that is being transferred from non-3GPP access, besides the PDN connection established in steps 3-15, by executing the UE requested PDN connectivity procedure specified in TS 23.401 [4].

18) The PDN GW shall initiate resource allocation deactivation procedure in the trusted/untrusted non-3GPP IP access as defined in clause 6.12 or clause 7.9.

8.2.1.2 Using PMIP-based S5/S8

When a Trusted or Untrusted Non-3GPP IP Access to 3GPP Access handover occurs, the following steps are performed instead of and in addition to the steps performed in the GTP-based S5/S8 case (see previous clause). In the case of PMIP-based S5/S8, a Create Session Request and Modify Bearer Request is not sent from the Serving GW to the PDN GW. Rather, the serving GW interacts with the hPCRF and PMIP messages are exchanged between the Serving GW and the PDN GW.

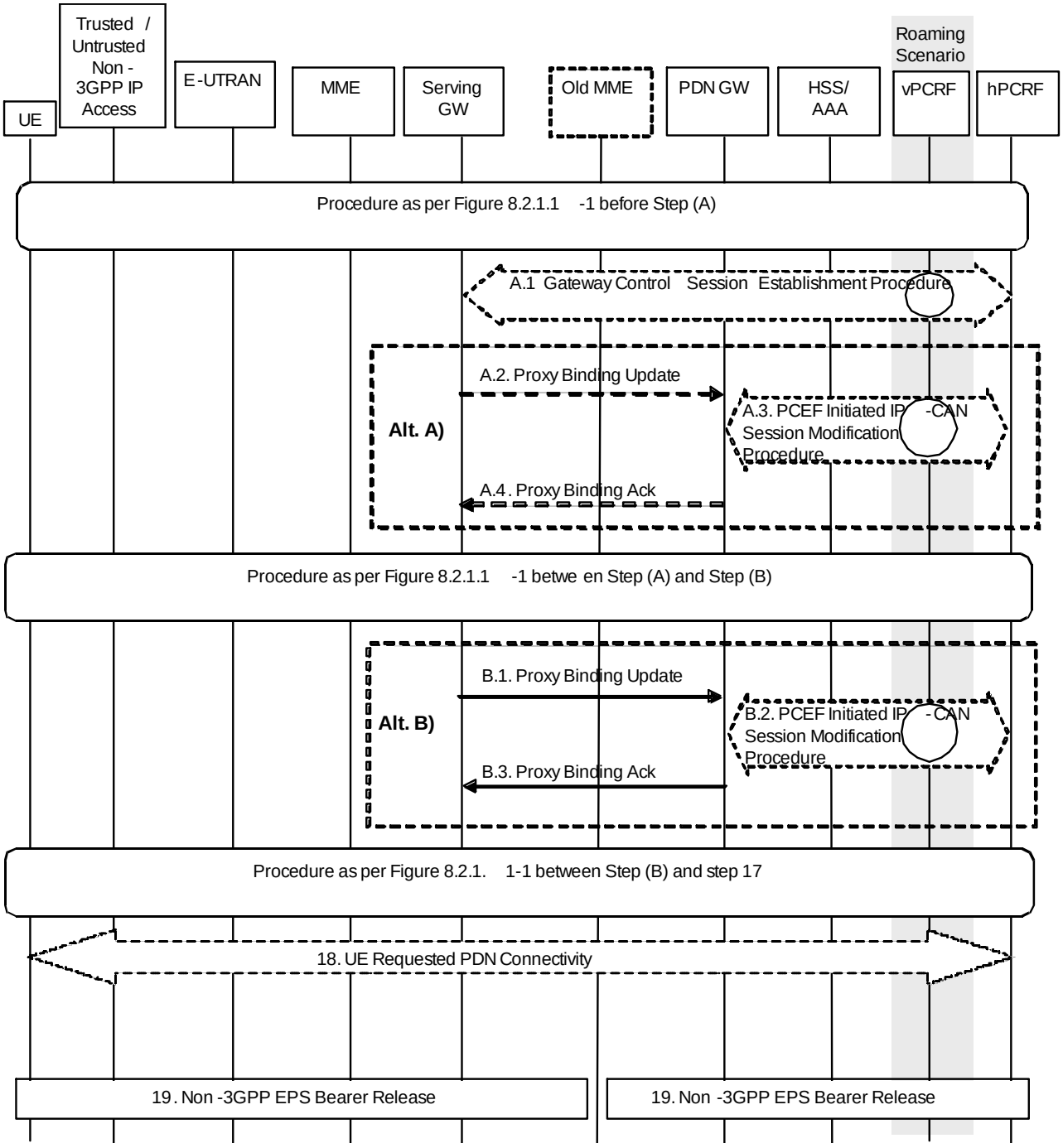


Figure 8.2.1.2-1: Trusted/Untrusted Non-3GPP IP Access to E-UTRAN Handover over PMIP-based S2a and using PMIP-based S5/S8

In case of connectivity to multiple PDNs the following applies:

In case of connectivity to multiple PDNs the following applies:

- If the UE is connected to both 3GPP access and non-3GPP access before the handover of PDN connections to 3GPP access is triggered, steps 2 to 16 of Figure 8.2.1.1-1 shall be skipped and the UE shall only perform step 18 of Figure 8.2.1.2-1 for each PDN connection that is being transferred from non-3GPP access.

- If the UE is connected only to non-3GPP access before the handover of PDN connections to 3GPP access is triggered, steps 2 to 16 of Figure 8.2.1.1-1 shall be performed. In step 3 of Figure 8.2.1.1-1 the UE shall provide the APN corresponding to one of the PDN connections that are being transferred from non-3GPP access. The UE shall then repeat step 18 of Figure 8.2.1.2-1 for each of the remaining PDN connections that are being transferred from non-3GPP access.

- Step 19 of Figure 8.2.1.2-1 shall be repeated for each PDN connection that is being transferred from non-3GPP access.

The steps in 18 of Figure 8.2.1.2-1 can occur in parallel for each PDN. Other impacts related to the handover for multiple PDNs are described in clause 8.1.

This procedure supports the home routed (Figure 4.2.2.1), roaming (Figure 4.2.3-1) and Local breakout (Figure 4.2.3-4) case. The Serving GW establishes a Gateway Control Session with the PCRF in the HPLMN. In the case of the roaming or local breakout scenario, the Serving GW interacts with the hPCRF by way of the vPCRF. The signalling takes place through the vPCRF in the VPLMN. In the case of Local Breakout, the PDN GW in the VPLMN exchanges messages with the vPCRF. The vPCRF then exchanges messages with the hPCRF in the HPLMN.

The optional interaction steps between the gateways and the PCRF in Figure 8.2.1.2-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

The steps shown in (Alt A) and (Alt B) are mutually exclusive in this procedure, i.e. either steps A.2-A.5 are executed or steps B.1-B.3. In order to execute the alternative (Alt B), the IP Address(es) of the UE needs to be available after step A.1. The IP Address(es) of the UE is received in step A.1, if dynamic policy provisioning is deployed. If multiple PDN connections to same APN are supported by the Serving GW, (Alt A) shall be used in this procedure.

In case the IP address(es) of the UE is available after step A1, (Alt B) provides lower jitter for dual radio handovers. In case the IP address(es) of the UE is not available after step A1, (Alt A) shall be used.

A.1) The Serving GW initiates a Gateway Control Session Establishment Procedure with the PCRF as specified in TS 23.203 [19] to obtain the rules required for the Serving GW to perform the bearer binding for all the active sessions the UE may establish as a result of the handover procedure.

If the updated QoS rules require establishment of dedicated bearer for the UE, the establishment of those bearers take place before step B1. The establishment of dedicated bearers in combination with the default takes place as described in Annex F of TS 23.401 [4].

A.2) The Serving GW sends a PMIPv6 Proxy Binding Update (MN NAI, Lifetime, Access Technology Type, Handover Indicator, IP Address Requested, APN, GRE Key for downlink traffic, Additional Parameters) message to the PDN GW. The MN NAI identifies the UE. The Lifetime field must be set to a non-zero value in the case of a registration. Access Technology Type is set to indicate 3GPP access to EPS. The Serving GW includes request for IPv4 Home Address and/or IPv6 Home Network Prefix as specified in step C.2 of clause 5.2. The APN may be necessary to differentiate the intended PDN from the other PDNs supported by the same PDN GW. The Serving GW includes the EPS bearer identity of the default bearer received from the MME if multiple PDN connections to the same APN are supported. The optional Additional Parameters may contain information, for example, protocol configuration options.

A.3) The PDN GW executes a PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19] to obtain the rules required for the PDN GW to function as the PCEF for all the active IP sessions the UE has established with new IP-CAN type.

A.4) The PDN GW responds with a Proxy Binding Ack (MN NAI, Lifetime, UE Address Info, GRE key for uplink traffic, Charging ID, Additional Parameters) message to the Serving GW. The MN NAI is identical to the MN NAI sent in the Proxy Binding Update. The Lifetime indicates the duration the binding will remain valid. The UE address info returns the IP Address assigned to the UE. IP address allocation by the PDN-GW is as specified in clause 4.7.1. If the PDN GW sends the DHCPv4 Address Allocation Procedure Indication in the Proxy Binding Acknowledgement message, the UE IPv4 address assigned by the PDN GW is not provided as part of the default bearer activation procedures to the UE. In this case, the Serving GW does not forward the IPv4 address assigned by the PDN GW to the MME, but sets the PDN Address to 0.0.0.0 in the message to the MME. If the corresponding Proxy Binding Update contains the EPS bearer identity, the PDN GW shall acknowledge if multiple PDN connections to the given APN are supported. The optional Additional Parameter information element may contain other information, including for example Protocol Configuration Options. The Serving GW acts as the MAG (in terms of PMIPv6). Since this step is triggered by the Proxy Binding Update message from the Serving GW in step A.2, it can occur after step A.2 and does not need to wait for step A.3.

The Charging Id provided by the PGW is the Charging Id previously assigned to the PDN connection for the non-3GPP access.

NOTE 1: PDN GW address selection is as described in TS 23.401 [4].

NOTE 2: The Serving GW learns from the PBA whether the PDN GW supports multiple PDN connection to the same APN or not.

Steps between A and B.1 are described in clause 8.2.1.1.

B.1-B.3) Corresponds to steps A.2 - A.4, respectively.

Steps between B.1 and 18 are described in clause 8.2.1.1.

18) For connectivity to multiple PDNs, the UE establishes connectivity to each PDN that is being transferred from non-3GPP access, besides the PDN connection established in the steps above, by executing the UE requested PDN connectivity procedure specified in clause 5.6.1.

19) The PDN GW shall initiate resource allocation deactivation procedure in the trusted/untrusted non-3GPP IP access as defined in clause 6.12 or clause 7.9.

8.2.1.3 General Procedure for GTP-based S5/S8 for UTRAN/GERAN

The steps involved in the handover from a trusted/untrusted non-3GPP IP access to UTRAN/GERAN connected to EPC are depicted below for both the non-roaming and roaming cases and when PMIPv6 is used on S2a or S2b. It is assumed that while the UE is served by the trusted/untrusted non-3GPP IP access, a PMIPv6 tunnel is established between the non-3GPP access network and the PDN GW in the EPC.

NOTE 1: This procedure is applicable to S4-SGSN only.

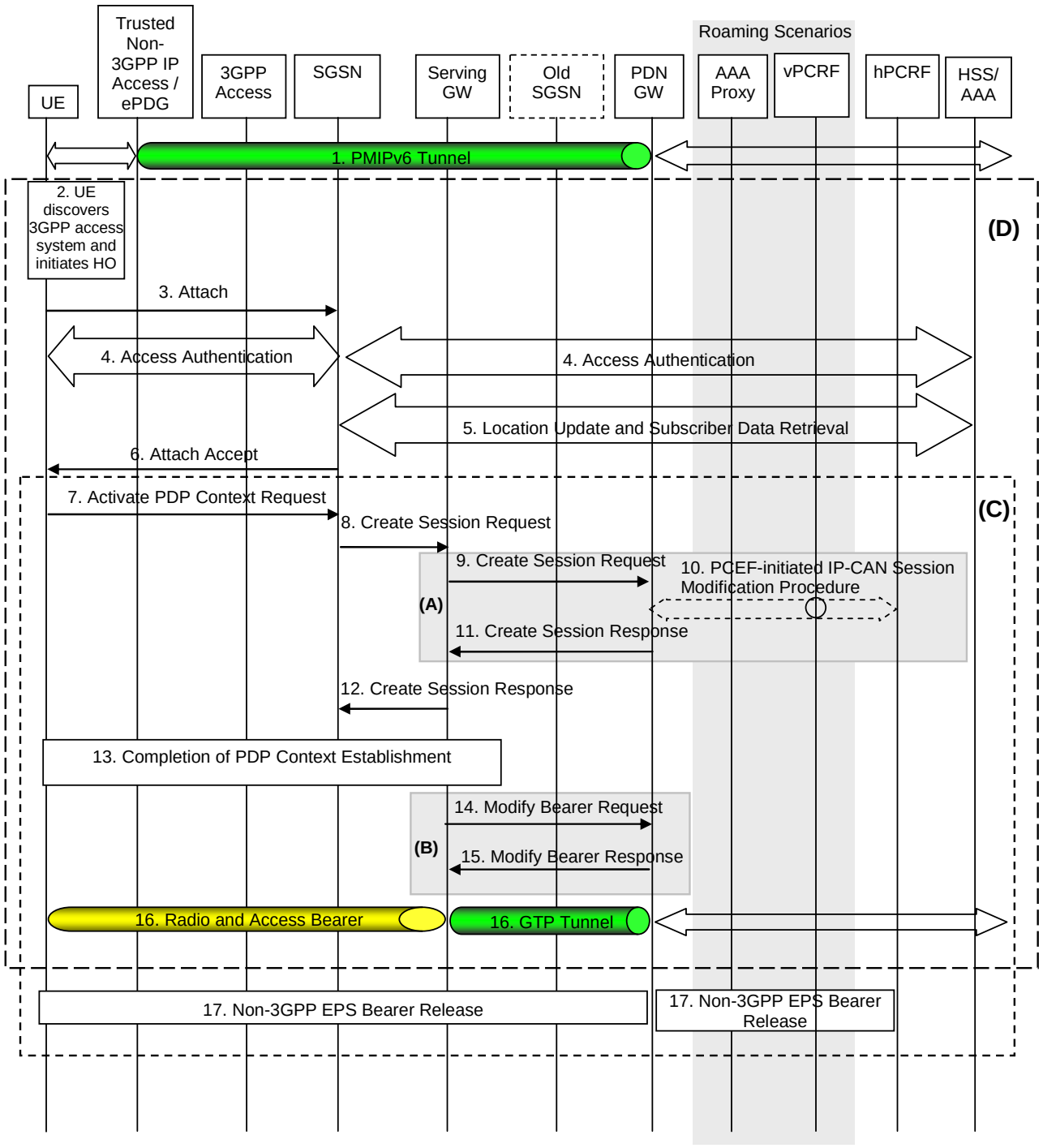


Figure 8.2.1.3-1: Handover from Trusted/untrusted Non-3GPP IP Access to UTRAN/GERAN with PMIP on S2a and GTP based S5/S8

NOTE 2: All steps outside of (A) and (B) are common for architecture variants with GTP based S5/S8 and PMIP based S5/S8. Procedure steps (A) and (B) for PMIP based S5/S8 are described in clause 8.2.1.4.

NOTE 3: All steps in (D) are common for architecture variants with GTP based S2b and PMIP based S2b. Procedures for steps outside of (D) for GTP based S2b are described in clause 8.6.1.2.

In case of connectivity to multiple PDNs the following applies:

- If the UE is connected to both 3GPP access and non-3GPP access before the handover of PDN connections to 3GPP access is triggered, steps 2 to 6 shall be skipped.

- If the UE is connected only to non-3GPP access before the handover of PDN connections to 3GPP access is triggered, steps 2 to 6 shall be performed.

- The steps in (C) shall be repeated for each PDN connection that is being transferred from non-3GPP access.

The steps in (C) can occur in parallel for each PDN.

The steps involved in the handover are described below.

1. The UE uses a trusted/untrusted non-3GPP access system and is being served by PDN GW (as PMIPv6 LMA).

2. The UE discovers the 3GPP Access system (UTRAN or GERAN) and determines to transfer its current sessions (i.e. handover) from the currently used non-3GPP access system to the discovered 3GPP Access system. The mechanisms that aid the UE to discover the 3GPP Access system, are specified in clause 4.8 (Network Discovery and Selection).

3. The UE sends an Attach Request to the SGSN. The message from the UE is routed by 3GPP Access to the SGSN as specified in clause 6.5 of TS 23.060 [21].

4. The SGSN may contact the HSS and authenticate the UE as described in TS 23.060 [21].

5. The SGSN may perform location update procedure and subscriber data retrieval from the HSS as specified in TS 23.060 [21]. PDN GW identity information is part of the subscriber data.

6. The SGSN sends the Attach Accept request to the UE to indicate the completion of the attach procedure as defined in TS 23.060 [21].

7. The UE initiate at this stage this establishment of the primary PDP context as defined in clause 9.2.2 of TS 23.060 [21].

8. The SGSN selects a Serving GW as described in TS 23.060 [21] and sends Create Session Request (Handover indication, and other parameters described in TS 23.060 [21]) message to the selected Serving GW.

9. The Serving GW sends a Create Session Request message to the PDN-GW as described in TS 23.060 [21]. The PDN GW should not switch the tunnel from non-3GPP IP access to 3GPP access system at this point.

10. The PDN GW may execute a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19] to report e.g. change in IP-CAN type.

    Since the PDN GW does not switch the tunnel in step 9, it defers any modification to the PCC Rules (due to changes received from the PCRF, if there is PCRF interaction) and still applies the existing PCC Rules for charging and policy until step 14.

    Depending on the active PCC rules, the establishment of dedicated bearers for the UE may be required.

NOTE 4: PDN GW address and Serving GW address selection is as described in the clause "GW selection" in TS 23.401 [4].

11. The PDN GW responds with a Create Session Response message to the Serving GW as described in TS 23.060 [21].The Create Session Response contains the IP address or the prefix that was assigned to the UE while it was connected to the non-3GPP IP access. It also contains the Charging Id previously assigned to the PDN connection in the non-3GPP access although the Charging Id still applies to the non-3GPP access.

12. The Serving GW returns a Create Session Response message to the SGSN as specified in TS 23.060 [21]. This message also includes the IP address of the UE. This message also serves as an indication to the SGSN that the S5 bearer setup and update has been successful.

13. The rest of the PDP context establishment as specified in TS 23.060 [21] is completed here.

NOTE 5: The S4-SGSN sends a Modify Bearer Request message to the Serving GW including the Handover Indication flag to inform Serving GW when PDP context establishment has been completed.

14. The Serving GW sends a Modify Bearer Request message to the PDN GW in the VPLMN or the HPLMN including the Handover Indication flag that prompts the PDN GW to tunnel packets from non 3GPP IP access to 3GPP access system and immediately start routing packets to the Serving GW for the default and any dedicated EPS bearers established. In case of non-roaming or roaming with home routed traffic this message is sent to the PDN GW in the HPLMN. In case of local breakout traffic the message is sent to the PDN GW in the VPLMN.

In this step, the PDN GW applies any modification to the PCC Rules received from the PCRF, if there is PCRF interaction in step 10. The Charging Id previously in use for the PDN connection in the non-3GPP access now only applies to the default bearer in use in GERAN/UTRAN access. If dedicated bearers are created, a new Charging Id is assigned by the PGW for each of them according to TS 23.401 [4].

15. The PDN GW acknowledges by sending Modify Bearer Response to the Serving GW.

16. The UE sends and receives data at this point via the 3GPP access system.

17. The PDN GW shall initiate resource allocation deactivation procedure in the trusted/untrusted non-3GPP IP access as defined in clause 6.12 or clause 7.9.

8.2.1.4 Using PMIP-based S5/S8

When a Trusted/untrusted Non-3GPP IP Access to UTRAN/GERAN handover occurs, the following steps are performed instead of and in addition to the steps performed in the GTP based S5/S8 case (see previous clause). In the case of PMIP based S5/S8, a Create Session Request and Modify Bearer Request is not sent from the Serving GW to the PDN GW. Rather, the serving GW interacts with the hPCRF and PMIP messages are exchanged between the Serving GW and the PDN GW.

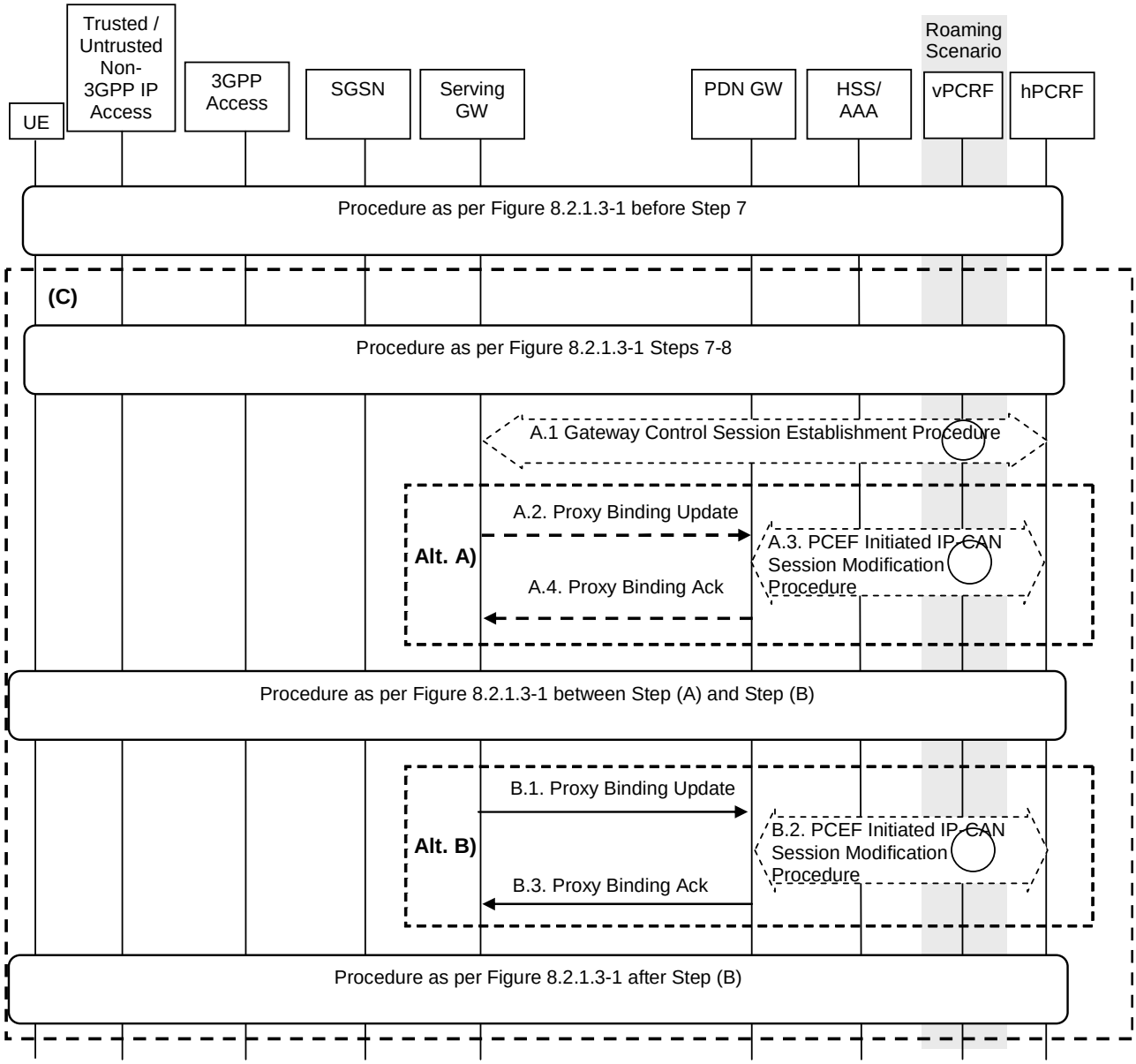


Figure 8.2.1.4-1: Trusted/untrusted Non-3GPP IP Access to GERAN/UTRAN over PMIP-based S2a and using PMIP-based S5/S8

In case of connectivity to multiple PDNs the following applies:

- If the UE is connected to both 3GPP access and non-3GPP access before the handover of PDN connections to 3GPP access is triggered, the procedure as per Figure 8.2.1.3-1 before step 7 shall be skipped.
- If the UE is connected only to non-3GPP access before the handover of PDN connections to 3GPP access is triggered, the procedure as per Figure 8.2.1.3-1 before step 7 shall be performed.
- The steps in (C) shall be repeated for each PDN connection that is being transferred from non-3GPP access.

The steps in (C) can occur in parallel for each PDN.

This procedure supports the home routed (Figure 4.2.2-1), roaming (Figure 4.2.3-1) and Local breakout (Figure 4.2.3-4) case. The Serving GW establishes a Gateway Control Session with the PCRF in the HPLMN. In the case of the roaming or local breakout scenario, the Serving GW interacts with the hPCRF by way of the vPCRF. The signalling takes place through the vPCRF in the VPLMN. In the case of Local Breakout, the PDN GW in the VPLMN exchanges messages with the vPCRF. The vPCRF then exchanges messages with the hPCRF in the HPLMN.

The optional interaction steps between the gateways and the PCRF in Figure 8.2.1.4-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

The steps shown in (Alt A) and (Alt B) are mutually exclusive in this procedure, i.e. either steps A.2-A.5 are executed or steps B.1-B.3. In order to execute the alternative (Alt B), the IP Address(es) of the UE needs to be available after step A.1. The IP Address(es) of the UE is received in step A.1, if dynamic policy provisioning is deployed. If multiple PDN connections to same APN are supported by the Serving GW, (Alt A) shall be used in this procedure.

In case the IP address(es) of the UE is available after step A1, (Alt B) provides lower jitter for dual radio handovers. In case the IP address(es) of the UE is not available after step A1, (Alt A) shall be used.

A.1) The Serving GW initiates a Gateway Control Session Establishment Procedure with the PCRF as specified in TS 23.203 [19] to obtain the rules required for the Serving GW to perform the bearer binding for all the active sessions the UE may establish as a result of the handover procedure.

If the updated PCC rules require establishment of dedicated bearer for the UE, the establishment of those bearers take place before step B.1.

The description of steps A.1 to A.4 and B.1 to B.3 are the same as in clause 8.2.1.2.

8.2.2 3GPP Access to Trusted Non-3GPP IP Access Handover with PMIPv6 on S2a

The steps involved in the handover from 3GPP Access connected to the EPC to trusted non-3GPP IP access are depicted below for the case of non-roaming, roaming with home routed traffic, roaming with local breakout and roaming with anchoring in the Serving Gateway in the VPLMN. It is assumed that while the UE is served by the 3GPP Access, a PMIPv6 or GTP tunnel is established between the S-GW and the PDN GW in the evolved packet core.

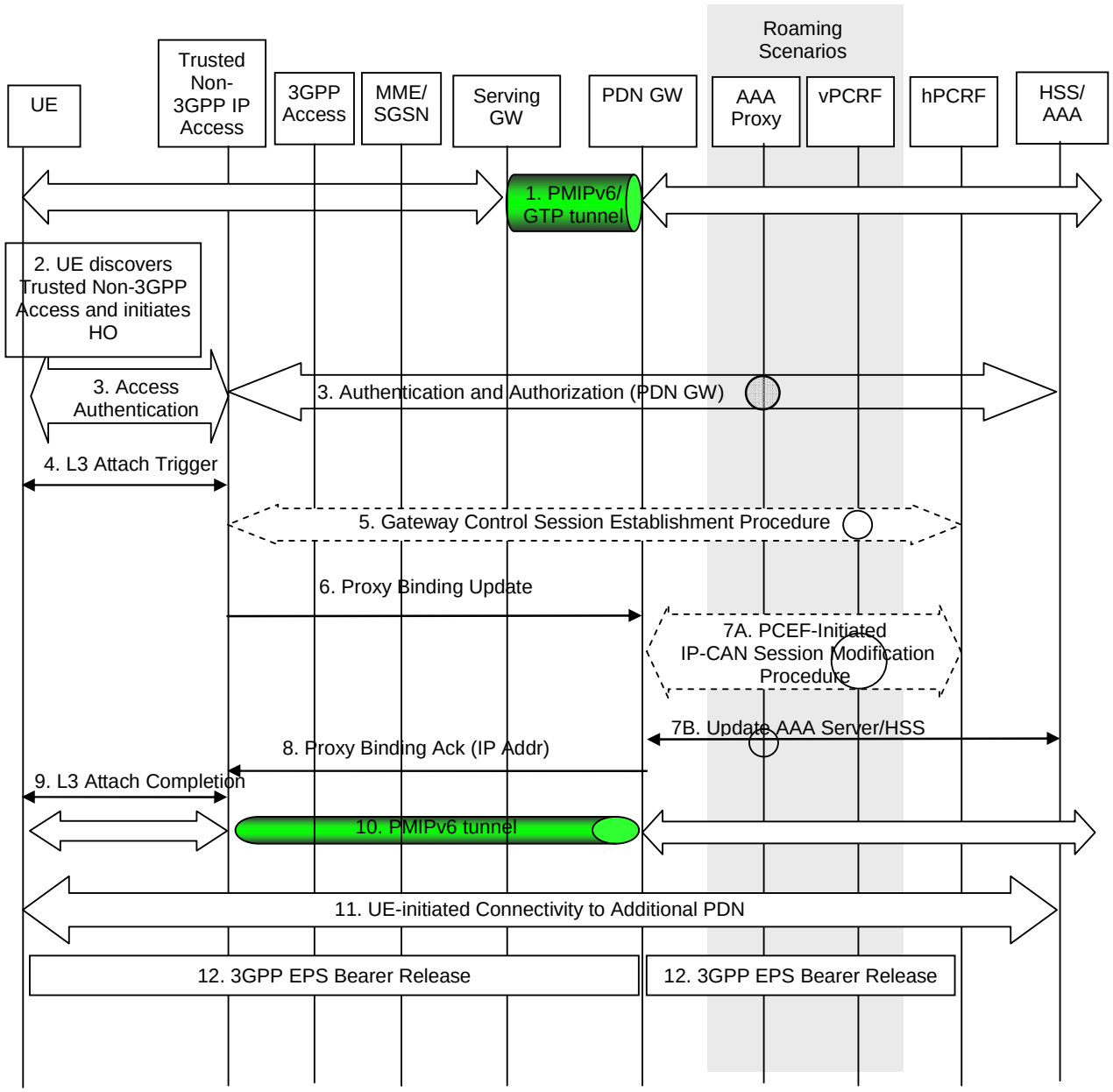


Figure 8.2.2-1: Handover from 3GPP Access to Trusted Non-3GPP IP Access with PMIPv6 on S2a and PMIPv6 or GTP on S5 interface

This procedure supports the home routed (Figure 4.2.2.1), roaming (Figure 4.2.3-1) and Local breakout (Figure 4.2.3-4) case. The PCRF in the HPLMN is informed of the change and any change in the policy that results is signalled to the Serving GW. The signalling takes place through the vPCRF in the VPLMN. In the case of Local Breakout, the PDN GW in the VPLMN exchanges messages with the vPCRF.

The optional interaction steps between the gateways and the PCRF in Figure 8.2.2-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

For connectivity to multiple PDNs the following applies:

- If the UE is connected to both 3GPP access and non-3GPP access before the handover of PDN connections to trusted non-3GPP access is triggered, steps 2 to 10 shall be skipped and the UE shall only perform step 11 for each PDN connection that is being transferred from 3GPP access.

- If the UE is connected only to 3GPP access before the handover of PDN connections to trusted non-3GPP access is triggered, steps 2 to 10 shall be performed. In step 4 the UE shall provide an APN corresponding to one of the PDN connections that are being transferred from 3GPP access. The UE shall then repeat step 11 for each of the remaining PDN connections that are being transferred from 3GPP access.

- Step 12 shall be repeated for each PDN connection that is being transferred from 3GPP access.

Step 11 can occur in parallel for each PDN. Other impacts related to the handover for multiple PDNs are described in clause 8.1.

1) The UE is connected in the 3GPP Access and has a PMIPv6 or GTP tunnel on the S5 interface.

2) The UE discovers the trusted non-3GPP IP access system and determines to transfer its current sessions (i.e. handover) from the currently used 3GPP Access to the discovered trusted non-3GPP IP access system. The mechanisms that aid the UE to discover the trusted non-3GPP IP access system, are specified in clause 4.8 (Network Discovery and Selection).

3) The UE performs access authentication and authorization in the non-3GPP access system. The 3GPP AAA server authenticates and authorizes the UE for access in the trusted non-3GPP system. The 3GPP AAA server queries the HSS and returns the PDN-GW identity or identities to the trusted non-3GPP access system at this step (upon successful authentication and authorization). The 3GPP AAA Server also returns to the trusted non-3GPP access system the MN NAI to be used to identify the UE in Proxy Binding Update and Gateway Control Session Establishment messages (steps 5 and 6).

   PDN GW address selection is as described in clause 4.5.1 of this specification. The PDNs the UE is connected to before handover are obtained from the HSS with the UE subscriber data.

NOTE 1: The MN NAI returned from the 3GPP AAA Server to the trusted non-3GPP access system is a permanent IMSI based MN NAI.

4) After successful authentication and authorization, the L3 attach procedure is triggered. At the latest, in this step, the UE should indicate its capability for the IP address preservation. How this information is signalled from the UE to the access network is outside of the scope of 3GPP.

   If the UE provides an APN, the Trusted non-3GPP Access verifies that it is allowed by subscription. If the UE does not provide an APN, and the subscription context from HSS contains a PDN GW identity and APN pair corresponding to the default APN, the Trusted non-3GPP Access uses the default APN. The case where the APN selected for the handover attach (default APN or the APN provided by the UE) does not have corresponding PDN GW identity information in the subscription context is considered as an error case.

5) The Trusted Non-3GPP IP Access initiates a Gateway Control Session Establishment Procedure with the PCRF as specified in TS 23.203 [19]. If the Trusted Non-3GPP IP Access supports UE/NW bearer control mode, the PCRF provides all the QoS rules required for the Trusted Non-3GPP IP Access to perform the bearer binding.

   If the updated rules require network-initiated dynamic resource allocation for the UE, the resource allocation takes place before step 6.

   If the Handover Indicator in the Proxy Binding Update (to be sent in step 6) is set to indicate either initial attach or that the handover state is unknown, the Trusted non-3GPP IP Access indicates in the Gateway Control Session Establishment message that linking with the Gx session shall be deferred until step 7, as specified in TS 23.203 [19]. In this case, when performing the leg linking, the PCRF verifies that the IP-CAN type reported over Gxa and Gx are the same.

6) The entity in the Trusted non-3GPP IP Access acting as a MAG sends a Proxy Binding Update (MN-NAI, Lifetime, Access Technology Type, Handover Indicator, APN, GRE key for downlink traffic) message to the PDN GW in order to establish the new registration. The MN NAI identifies the UE for whom the message is being sent. The Lifetime field must be set to a nonzero value in the case of a registration. Access Technology Type is set to a value matching the characteristics of the non-3GPP access. The APN may be necessary to differentiate the intended PDN from the other PDNs supported by the same PDN GW. The MAG creates and includes a PDN connection identity if the MAG supports multiple PDN connections to a single APN.

NOTE 2: When multiple PDN connections to a single APN are supported, the MN-ID, the APN and the PDN connection identity indentify the PDN connection within the Trusted Non-3GPP access network.

NOTE 3: When the PDN GW receives the Proxy Binding Update and the the PS bearers corresponding to the PDN connection being handed over are suspended, then the PDN GW considers the bearers of the PDN connection being handed over as resumed and performs the handover.

7A) The PDN GW executes a PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19]. The Event Report indicates the change in Access Type.

If the PDN GW decided to allocate a new IP address/prefix instead of preserving the old IP address/prefix, as described in clause 4.1.3.2.3, the PDN GW executes an IP-CAN session Establishment Procedure with the PCRF instead of a PCEF-Initiated IP-CAN Session Modification Procedure.

7B) The PDN GW informs the 3GPP AAA Server of its PDN GW identity and the APN corresponding to the UE's PDN Connection and obtains authorization information from the 3GPP AAA Server. The message includes information that identifies the PLMN in which the PDN GW is located. The 3GPP AAA Server may update the information registered in the HSS as described in clause 12.

8) The PDN GW responds with a PMIP Binding Acknowledgement (MN NAI, Lifetime, UE Address Info, Additional Parameters, GRE key for uplink traffic, Charging ID) message to the Trusted Non-3GPP IP Access. The MN NAI is identical to the MN NAI sent in the Proxy Binding Update. The Lifetime indicates the duration the binding will remain valid. If the corresponding Proxy Binding Update contains a PDN connection identity, the PDN GW shall acknowledge if the PDN GW supports multiple PDN connections to a single APN. The UE address info returns the IP Address assigned to the UE. The optional Additional Parameter information element may contain other information. Since this step is triggered by the Proxy Binding Update message from the Trusted non-3GPP IP Access in step 6 and the result of the optional step 7, it can occur after step 7. If step 7 is not taken, this step can occur after step 6. The Charging Id provided is the Charging Id previously assigned to the PDN connection if the source access is a PMIP-based access or to the Default Bearer if the source access is GTP-based.

NOTE 4: The MAG learns from the PBA whether the PDN GW supports multiple PDN connection to the same APN or not.

9) L3 attach procedure is completed at this point. The IP address(es) assigned to the UE by the PDN-GW is conveyed to the UE.

10) The PMIPv6 tunnel is set up between the Trusted Non-3GPP IP Access and the PDN GW. The UE can send/receive IP packets at this point.

11) For connectivity to multiple PDNs, the UE establishes connectivity to all the PDNs that are being transferred from 3GPP access besides the PDN connection that was established in the steps 3-10, as described in clause 6.8.1.

12) The PDN GW shall initiate the PDN GW Initiated PDN Disconnection procedure in 3GPP access as defined in clause 5.6.2.2 or the PDN GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [4], clause 5.4.4.1.

8.2.3 3GPP Access to Untrusted Non-3GPP IP Access Handover with PMIPv6 on S2b

This clause shows a call flow for a handover when a UE moves from a 3GPP Access to an untrusted non-3GPP access network. PMIPv6/GTP is assumed to be used on the S5/S8 interface and PMIPv6 is used on the S2b interface.

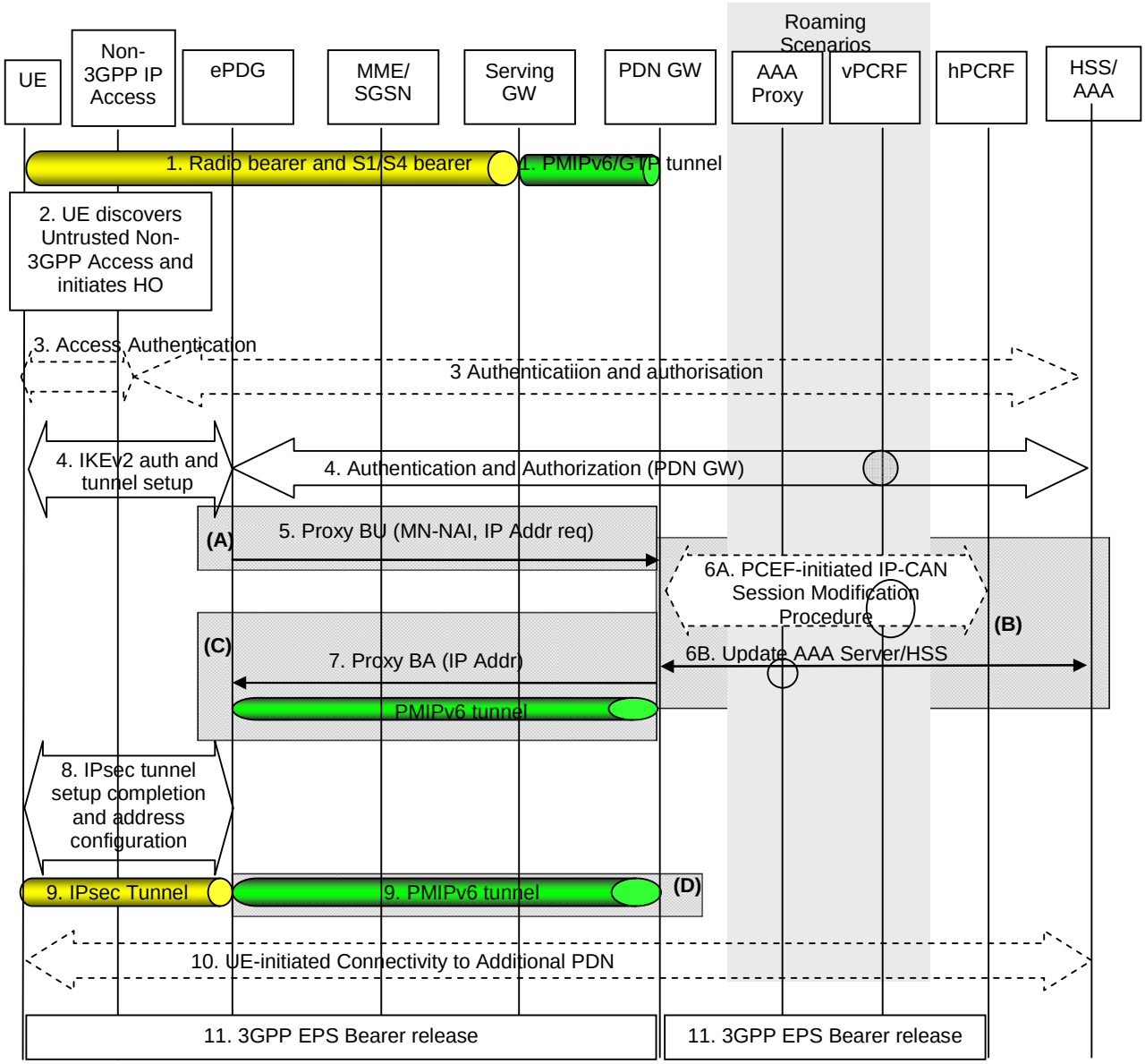


Figure 8.2.3-1: Handover from 3GPP Access to Untrusted Non-3GPP IP Access with PMIPv6 on S2b

NOTE 1: For GTP based S2b, procedure steps (A) to (D) are defined in clause 8.6.2.1.

Both the roaming (Figure 4.2.1-2) and non-roaming (Figure 4.2.1-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the Serving GW in the VPLMN. The vPCRF receives the Acknowledgment from the Serving GW and forwards it to the hPCRF. In the non-roaming case, the vPCRF is not involved.

For connectivity to multiple PDNs the following applies:

- If the UE is connected to both 3GPP access and non-3GPP access before the handover of PDN connections to untrusted non-3GPP access is triggered, steps 2 to 9 shall be skipped and the UE shall only perform step 10 for each PDN connection that is being transferred from 3GPP access.

- If the UE is connected only to 3GPP access before the handover of PDN connections to untrusted non-3GPP access is triggered, steps 2 to 9 shall be performed. In step 3 the UE shall provide an APN corresponding to one of the PDN connections that are being transferred from 3GPP access. The UE shall then repeat step 10 for each of the remaining PDN connections that are being transferred from 3GPP access.

- Step 11 shall be repeated for each PDN connection that is being transferred from 3GPP access.

Step 10 can occur in parallel for each PDN. Other impacts related to the handover for multiple PDNs are described in clause 8.1.

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured in the gateway.

1) The UE is initially attached to the 3GPP Access network.

2) The UE moves and attaches to an untrusted non-3GPP IP access network.

3) Access authentication procedure between UE and the 3GPP EPC may be performed as defined by TS 33.402 [45]. When the 3GPP AAA server has WLAN Location Information about the UE, it provides it over SWm to the ePDG together with the Age of this information. The WLAN Location information is provided to the ePDG when the 3GPP AAA server considers that location information coming from the WLAN AN used by the UE is trustable.

4) The IKEv2 tunnel establishment procedure is started by the UE. The ePDG IP address to which the UE needs to form IPsec tunnel with is discovered as specified in clause 4.5.4. After the UE is authenticated, UE is also authorized for access to the APN. The procedure is as described in TS 33.402 [45]. As part of access authentication the PDN GW identity is sent to the ePDG by the 3GPP AAA server. If the UE supports IP address preservation during handover from 3GPP Access to the untrusted non-3GPP IP access, the UE shall include its address (IPv4 address or IPv6 prefix /address or both) allocated when it's attached to 3GPP Access into the CFG_Request sent to the ePDG during IKEv2 message exchange.

5) The ePDG sends the Proxy Binding Update (MN-NAI, Lifetime, Access Technology Type, Handover Indicator, GRE key for downlink traffic, UE Address Info, Additional Parameter) message to the PDN GW. Access Technology Type is set to a value matching the characteristics of the non-3GPP access. The UE Address Info shall be set according to the CFG_Request in step 3. The ePDG shall not change the requested address(es) in the CFG_Request sent by the UE, and encode such address(es) in PBU and send to the PDN GW. If the UE included the address in step 3, the ePDG sets the handover indicator to indicate Handoff between two different interfaces of the UE. The APN is used by the PDN GW to determine which PDN to establish connectivity for, in the case that the PDN GW supports multiple PDN connectivity. The ePDG creates and includes a PDN connection identity if the ePDG supports multiple PDN connections to a single APN.

NOTE 2: When multiple PDN connections to a single APN are supported, the MN-ID, the APN and the PDN connection identity indentify the PDN connection within the Untrusted Non-3GPP access network.

6A) If PCC is supported, the PDN GW requires configuration for enforcing policy, the PDN GW executes a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19].

6B) The PDN GW informs the 3GPP AAA Server of its PDN GW identity and the APN corresponding to the UE's PDN Connection and obtains authorization information from the 3GPP AAA Server. The message includes information that identifies the PLMN in which the PDN GW is located. The 3GPP AAA Server may update the information registered in the HSS as described in clause 12.

7) The PDN GW processes the Proxy Binding Update message from the ePDG, updates the binding cache entry for the UE and responds with a Proxy Binding Acknowledgement (MN_NAI, Lifetime, GRE key for uplink traffic, UE Address Info, Charging ID, Additional Parameters) message. In the Proxy Binding Ack, the PDN GW replies with the same IP address and/or prefix that was assigned to the UE earlier. If the corresponding Proxy Binding Update contains a PDN connection identity, the PDN GW shall acknowledge if the PDN GW supports multiple PDN connections to a single APN. At this point a PMIPv6 tunnel exists between PDN GW and ePDG. Since this step is triggered by the Proxy Binding Update message from the ePDG in step 4, it can occur after step 4 and does not need to wait for step 5. The Charging Id provided is the Charging Id previously assigned to the PDN connection if the source access is a PMIP-based access or to the Default Bearer if the source access is GTP-based.

NOTE 3: The ePDG learns from the PBA whether the PDN GW supports multiple PDN connection to the same APN or not.

NOTE 4: When the PDN GW receives the Proxy Binding Update and the the PS bearers corresponding to the PDN connection being handed over are suspended, then the PDN GW considers the bearers of the PDN connection being handed over as resumed and performs the handover.

8) The ePDG and the UE continue the IKEv2 exchange and IP address configuration.

9) At the end of the handover procedure there is a default bearer for the UE that consists of an IPsec tunnel between the UE and the ePDG and a PMIPv6 tunnel between the ePDG and the PDN GW.

10) For connectivity to multiple PDNs, the UE establishes connectivity to each PDN that is being transferred from 3GPP access, besides the PDN connection that was established in the steps 3-8, by executing the UE-initiated Connectivity to Additional PDN procedure specified in clause 7.6.1.

11) The PDN GW shall initiate the PDN GW Initiated PDN Disconnection procedure in 3GPP access as defined in clause 5.6.2.2 or the PDN GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [4], clause 5.4.4.1.

8.2.4 Void

8.2.5 Void

8.2.6 Non-3GPP IP Access to 3GPP Access Handover with PMIPv6 on S2a/b for Chained PMIP-based S8

The steps involved in the handover from a trusted or non-trusted non-3GPP IP access to a 3GPP access connected to EPC are depicted below for roaming cases with chained S2a/b and PMIP-based S8. It is assumed that while the UE is served by the non-3GPP IP access, a PMIPv6 tunnel is established between the non-3GPP access network and the Serving GW and another one between the Serving GW and the PDN GW.

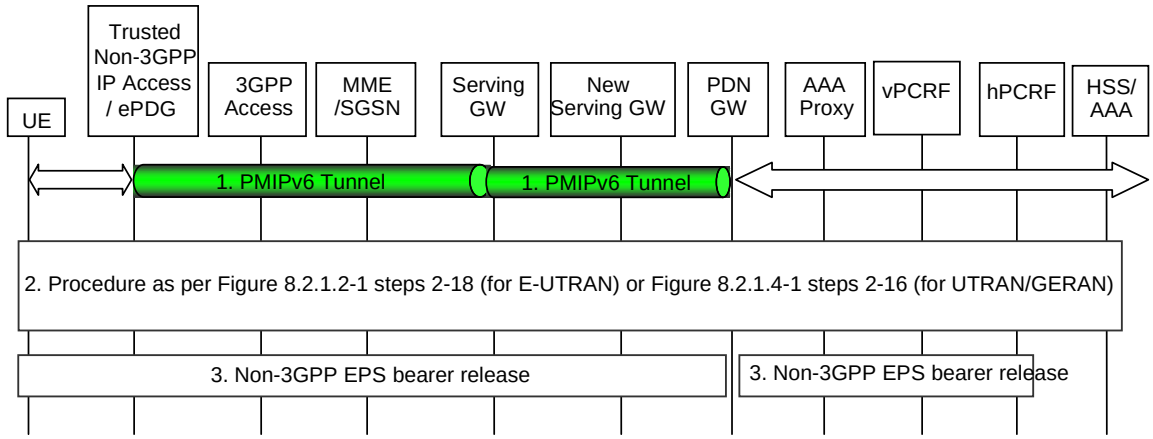


Figure 8.2.6-1: Handover from Trusted or Untrusted Non-3GPP IP Access to 3GPP Access with chained S2a/b and PMIP-based S8

In case of handover to E-UTRAN, the following applies for connectivity to multiple PDNs:

- If the UE is connected to both 3GPP access and non-3GPP access before the handover of PDN connections to 3GPP access is triggered, the procedure as per Figure 8.2.1.2-1 before step 18 shall be skipped and the UE shall only perform step 18 of Figure 8.2.1.2-1 for each PDN connection that is being transferred from non-3GPP access.

- If the UE is connected only to non-3GPP access before the handover of PDN connections to 3GPP access is triggered, the procedure as per Figure 8.2.1.2-1 before step 18 shall be performed. In step 3 of Figure 8.2.1.2-1 the UE shall provide an APN corresponding to one of the PDN connections that are being transferred from non-3GPP access. The UE shall then repeat step 18 of Figure 8.2.1.2-1 for each of the remaining PDN connections that are being transferred from 3GPP access.

In case of handover to UTRAN/GERAN, the following applies for connectivity to multiple PDNs:

- If the UE is connected to both 3GPP access and non-3GPP access before the handover of PDN connections to 3GPP access is triggered, steps 2 to 6 of Figure 8.2.1.4-1 shall be skipped.

- If the UE is connected only to non-3GPP access before the handover of PDN connections to 3GPP access is triggered, steps 2 to 6 of Figure 8.2.1.4-1 shall be performed.

- The UE shall repeat steps 7 to 16 of Figure 8.2.1.4-1 for each PDN connection that is being transferred from non-3GPP access.

For connectivity to multiple PDNs step 3 of Figure 8.2.6-1 shall be repeated for each PDN connection that is being transferred from non-3GPP access.

NOTE: The procedure applies both for the case where a new Serving GW is selected during attach on 3GPP access or for the case where the Serving GW is not changed.

1) The UE uses a trusted or untrusted non-3GPP access system. PDN connectivity is achieved through concatenated PMIPv6 tunnels between the trusted non-3GPP access or ePDG and the Serving GW, and between the Serving GW and the PDN GW.

2) The handover procedure from trusted or untrusted non-3GPP IP access with PMIPv6 on S2a/S2b to 3GPP access with PMIP-based S5/S8 is performed as described in steps 2-18 of clause 8.2.1.2 (for E-UTRAN) and steps 2-16 of clause 8.2.1.4 (for UTRAN/GERAN).

3) In case a new Serving GW has been selected during the attach on 3GPP access, the PDN GW triggers the bearer release in the non-3GPP access as defined in clause 6.12.3. Otherwise, the Serving GW triggers resource release in the non-3GPP access as defined in steps 2-5 of clause 6.12.3.

8.2.7 3GPP Access to Non-3GPP IP Access Handover with PMIPv6 on S2a/b for Chained PMIP-based S8

The steps involved in the handover from a 3GPP access to a trusted or non-trusted non-3GPP IP access connected to EPC are depicted below for roaming cases with chained S2a/b and PMIP-based S8.

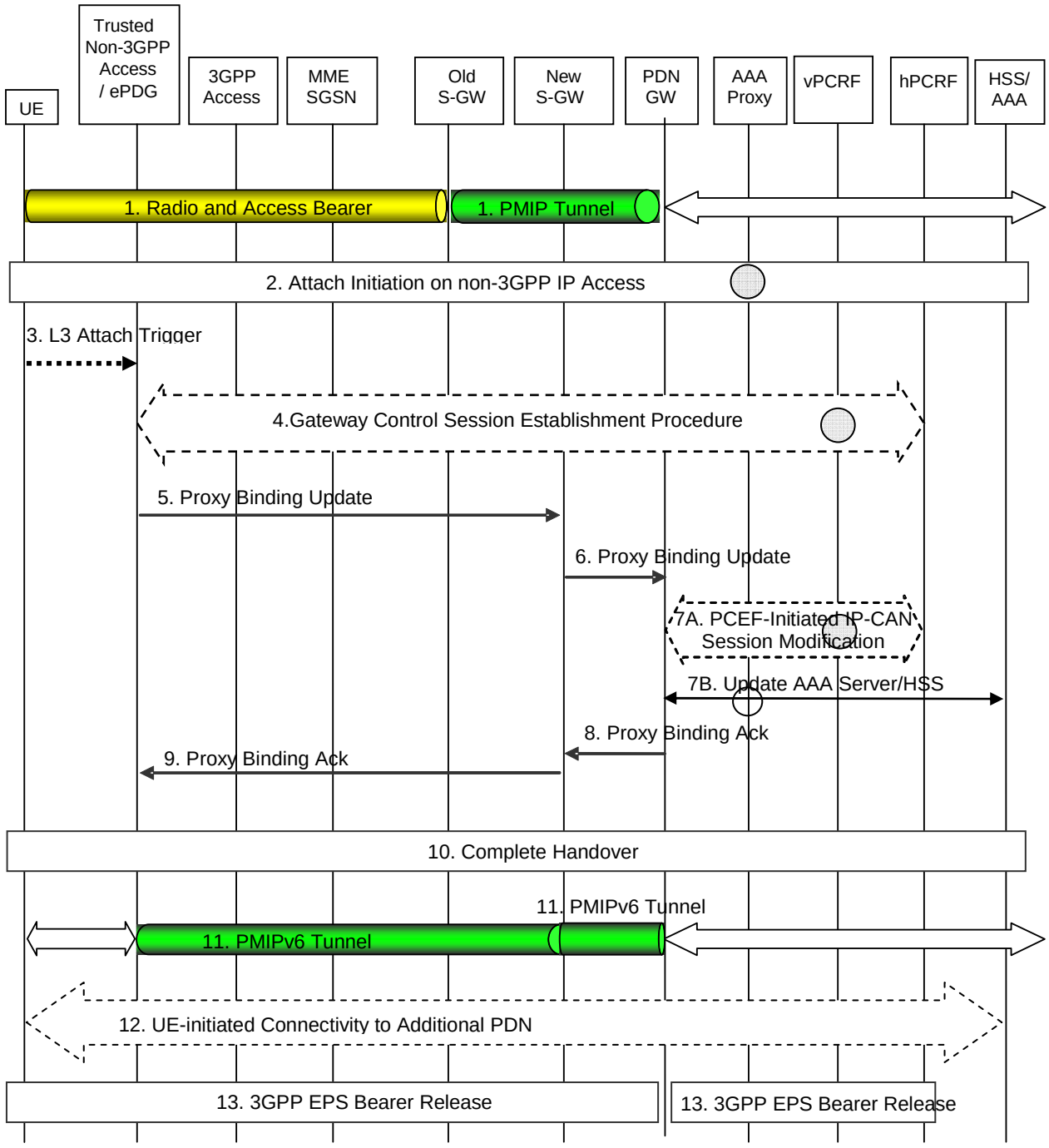


Figure 8.2.7-1: Handover from 3GPP IP Access to Trusted or Untrusted Non-3GPP Access with chained S2a/b and PMIP-based S8

For connectivity to multiple PDNs the following applies:

- If the UE is connected to both 3GPP access and non-3GPP access before the handover of PDN connections to non-3GPP access is triggered, steps 2 to 11 shall be skipped and the UE shall only perform step 12 for each PDN connection that is being transferred from 3GPP access.

- If the UE is connected only to 3GPP access before the handover of PDN connections to non-3GPP access is triggered, steps 2 to 11 shall be performed. In step 3 the UE shall provide an APN corresponding to one of the PDN connections that are being transferred from 3GPP access. The UE shall then repeat step 12 for each of the remaining PDN connections that are being transferred from 3GPP access.

- Step 13 shall be repeated for each PDN connection that is being transferred from 3GPP access.

Step 12 can occur in parallel for each PDN. Other impacts related to the handover for multiple PDNs are described in clause 8.1.

Steps 3 and 4 do not apply in case of handover from a 3GPP access to an untrusted non-3GPP access.

The optional interaction steps between the gateways and the PCRF in Figure 8.2.7-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

NOTE 1: The procedure applies both for the case where a new Serving GW is selected during attach on 3GPP access, or for the case where the Serving GW is not changed.

1) The UE is connected to the PDN via a 3GPP Access and has a PMIPv6 tunnel on the S8 interface.

2) The attach initiation on the trusted or untrusted non-3GPP access is performed as described in steps 2-3 of clause 8.2.2 (for trusted non-3GPP access) and steps 2-3 of clause 8.2.3 (for untrusted non-3GPP access). As part of the authentication procedure, the 3GPP AAA proxy obtains the PDN-GW identity from the HSS/AAA as described in clause 4.5.1, and performs Serving GW selection as described in clause 4.5.3. Both PDN GW identity and Serving GW information is provided to the MAG function of the trusted non-3GPP access or ePDG. If PCC is deployed, the MAG function of the Trusted Non-3GPP IP access is notified to interact with the PCRF when it is the PMIP-based chained case.

3) After successful authentication and authorization, the L3 attach procedure in the trusted non-3GPP access is triggered as described in step 4 of clause 8.2.2.

4) The trusted non-3GPP access initiates a Gateway Control Session Establishment Procedure with the PCRF as described in step 5 of clause 8.2.2.

5) The MAG function of Trusted Non-3GPP IP Access or ePDG sends a Proxy Binding Update (MN-NAI, Lifetime, Access Technology Type, Handover Indicator, APN, GRE key for downlink traffic, PDN GW address, Additional Parameters) message to the Serving GW in the VPLMN. The MN NAI identifies the UE. The Lifetime field must be set to a nonzero value, indicating registration. Access Technology Type is set to a value matching the characteristics of the non-3GPP access. Handover Indicator is set to indicate handoff between two different interfaces of the UE. The MAG creates and includes a PDN connection identity if the MAG supports multiple PDN connections to a single APN. The Additional Parameters may include Protocol Configuration Options and other information.

NOTE 2: When multiple PDN connections to a single APN are supported, the MN-ID, the APN and the PDN connection identity indentify the PDN connection within the Trusted Non-3GPP access network.

6) The Serving GW sends a corresponding Proxy Binding Update (MN-NAI, Lifetime, Access Technology Type, Handover Indicator, APN, GRE key for downlink traffic, Additional Parameters) message (as in step 3) to the PDN GW. If the MAG included the PDN connection identity in the Proxy Binding Update of the previous step and the Serving GW supports multiple PDN connections to a single APN then the Serving GW forwards the PDN connection identity to the PDN GW.

NOTE 3: In this Release of the specification, the Serving GW uses the right protocol to connect with the PDN GW based on the pre-configured information on itself in case the selected Serving GW supporting both PMIP and GTP.

7A) The PDN GW initiates the PCEF-Initiated IP-CAN Session Modification Procedure with the hPCRF to update the rules in the PDN GW, as specified in TS 23.203 [19].

7B) The PDN GW informs the 3GPP AAA Server of its PDN GW identity and the APN corresponding to the UE's PDN Connection and obtains authorization information from the 3GPP AAA Server. The message includes information that identifies the PLMN in which the PDN GW is located. The 3GPP AAA Server may update the information registered in the HSS as described in clause 12.

8) The PDN GW processes the proxy binding update and creates a binding cache entry for the PMIPv6 tunnel towards the Serving GW. The PDN GW responds with a Proxy Binding Acknowledgement (MN-NAI, Lifetime, UE Address Info, GRE key for uplink traffic, Additional Parameters) message to the Serving GW. The MN-NAI is identical to the MN-NAI sent in the Proxy Binding Update. The Lifetime indicates the duration the binding will remain valid. The UE Address Info includes one or more IP addresses. If the corresponding Proxy Binding Update contains a PDN connection identity, the PDN GW shall acknowledge if the PDN GW supports multiple PDN connections to a single APN. The Additional Parameters may include Protocol Configuration Options and

other information. The Additional Parameters may include Protocol Configuration Options and other information.

NOTE 4: The Serving GW learns from the PBA whether the PDN GW supports multiple PDN connection to the same APN or not.

NOTE 5: When the PDN GW receives the Proxy Binding Update and the the PS bearers corresponding to the PDN connection being handed over are suspended, then the PDN GW considers the bearers of the PDN connection being handed over as resumed and performs the handover.

9) The Serving GW processes the proxy binding acknowledgement and creates a binding cache entry for the PMIPv6 tunnel towards the MAG function in the trusted non-3GPP access or ePDG. At this point, the Serving GW also establishes the internal forwarding state for the concatenation of the PMIPv6 tunnels. The Serving GW then sends a corresponding Proxy Binding Acknowledgement (MN NAI, Lifetime, UE Address Info, GRE key for uplink traffic, Charging ID, Additional Parameters) message (as in step 8) to the MAG function of Trusted Non-3GPP IP Access or ePDG.

10) The handover attach procedure is completed as described in step 9 of clause 8.2.2 (for trusted non-3GPP access) and steps 7-8 of clause 8.2.3 (for untrusted non-3GPP access).

11) The UE is connected to the PDN via the non-3GPP access system. PDN connectivity is achieved through concatenated PMIPv6 tunnels between the trusted non-3GPP access or ePDG and the Serving GW, and between the Serving GW and the PDN GW.

12) For connectivity to multiple PDNs, the UE establishes connectivity to each PDN that is being transferred from 3GPP access, besides the PDN connection established in steps 2-11, by executing the UE-initiated Connectivity to Additional PDN procedure specified in clause 6.8.1.2, that applies to both trusted and untrusted non-3GPP accesses.

13) In case a new Serving GW has been selected during the attach on the non-3GPP access, the PDN GW triggers the bearer release in the 3GPP access using the PDN GW initiated Bearer Deactivation procedure. Otherwise, the Serving GW triggers the bearer release in the 3GPP Access using the Serving GW initiated Bearer Deactivation procedure. The 3GPP access resources associated with the PDN address are released if existing.

8.2.8 Void

8.2.9 Void

8.3 Handover from 3GPP access to Trusted Non-3GPP IP Access with MIPv4 FACoA on S2a

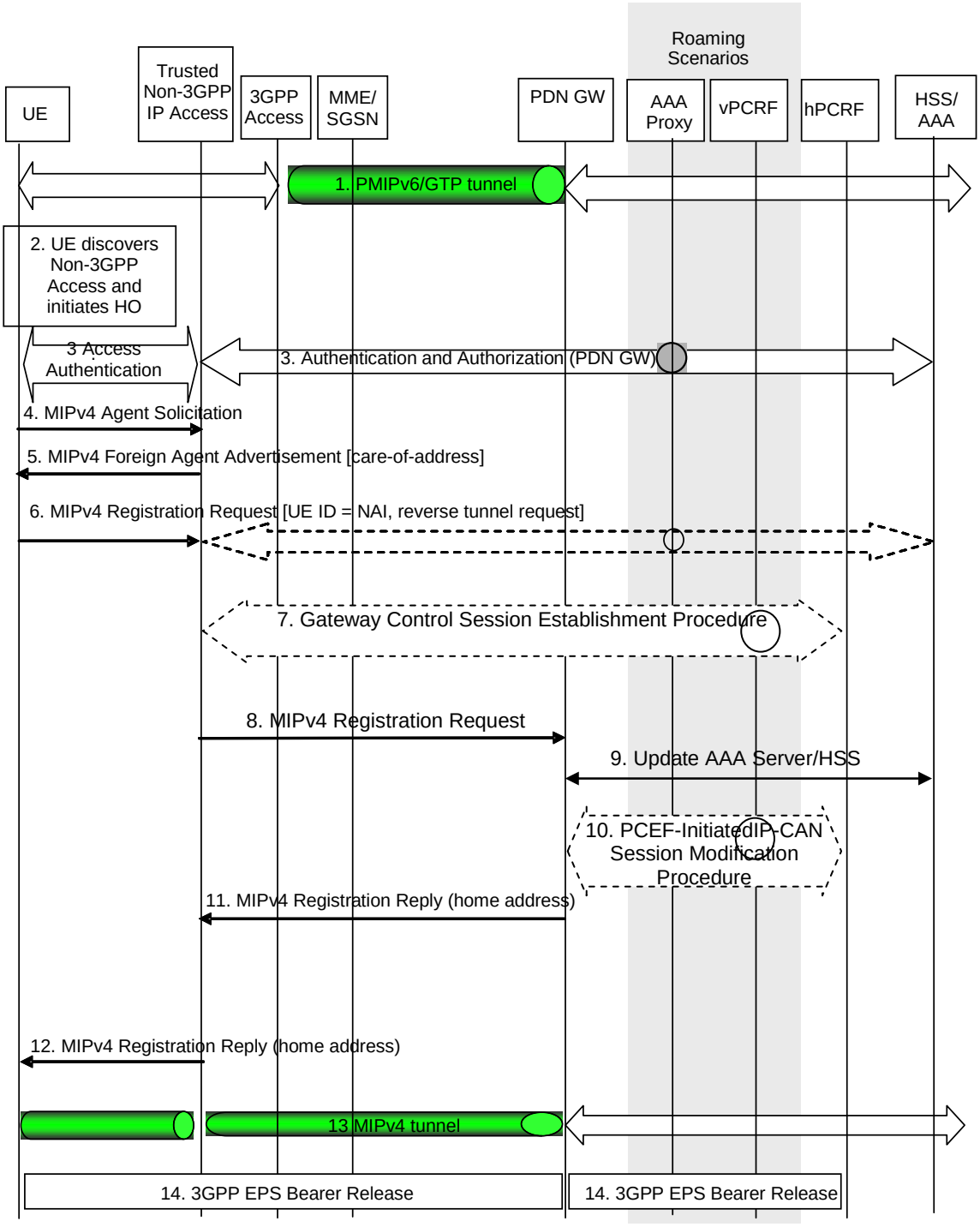


Figure 8.3-1: 3GPP IP Access to Non-3GPP IP access Handover over MIPv4-based S2a

In case of connectivity to multiple PDNs the following applies:

- If the UE is connected to both 3GPP access and trusted non-3GPP access before the handover of PDN connections to trusted non-3GPP access is triggered, steps 2 to 5 shall be skipped.

- If the UE is connected only to 3GPP access before the handover of PDN connections to trusted non-3GPP access is triggered, steps 2 to 5 shall be performed.

- Steps 6 to 14 shall be repeated for each PDN connection that is being transferred from 3GPP access.

Step 6 to step 14 can occur in parallel for each PDN. Other impacts related to the handover for multiple PDNs are described in clause 8.1.

The steps involved in the handover from 3GPP Access connected to the EPC to trusted non-3GPP IP access are depicted below for the case of non-roaming, roaming with home routed traffic, roaming with local breakout and roaming with anchoring in the Serving Gateway in the VPLMN. It is assumed that while the UE is served by the 3GPP Access, a PMIPv6 or GTP tunnel is established between the S-GW and the PDN GW in the evolved packet core.

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

Both the roaming (Figure 4.2.1-2) and non-roaming (Figure 4.2.1-1) scenarios are depicted in the figure. In the roaming case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the Serving GW in the VPLMN. The vPCRF receives the Acknowledgment from the Serving GW and forwards it to the hPCRF. In the non-roaming case, the vPCRF is not involved at all.

The event that triggers Authentication and Authorization in step 3 or step 6 between the Trusted Non-3GPP IP Access and the 3GPP AAA Server, or whether this step occurs at all, depends on the specific access technology.

1) The UE is connected in the 3GPP Access and has a PMIPv6 or GTP tunnel on the S5 interface.

2) The UE discovers the trusted non-3GPP IP access system and determines to transfer its current sessions (i.e. handover) from the currently used 3GPP Access to the discovered trusted non-3GPP IP access system. The mechanisms that aid the UE to discover the trusted non-3GPP IP access system, are specified in clause 4.8 (Network Discovery and Selection).

3) The UE performs access authentication and authorization in the non-3GPP access system as defined by TS 33.402 [45]. The 3GPP AAA server authenticates and authorizes the UE for access in the trusted non-3GPP system. As part of the authentication and authorization procedure, the 3GPP AAA server obtains the PDN-GW identity from the HSS and it returns the same PDN-GW identity to the trusted non-3GPP access system at this step (upon successful authentication and authorization).

4) The UE may send an Agent Solicitation (AS) RFC 5944 [12] message. Specification of this message is out of the scope of 3GPP.

5) The FA in the Trusted Non-3GPP IP Access sends a Foreign Agent Advertisement (FAA) (RFC 5944 [12]) message to the UE. The FAA message includes the Care-of Address (CoA) of the Foreign Agent function in the FA. Specification of this message is out of the scope of 3GPP.

6) The UE sends a Registration Request (RRQ) (MN-NAI, lifetime) message as defined in RFC 5944 [12] to the FA as specified in RFC 5944 [12]. Reverse Tunnelling shall be requested. This ensures that all traffic will go through the PDN GW. The RRQ message shall include the NAI-Extension RFC 2794 [34]. The UE may not indicate a specific Home Agent address in the RRQ message, in which case the FA uses the PDN GW address as received in step 3. The UE then receives the IP address of the PDN Gateway in step 11 as part of the RRP message. The UE should then include the PDN Gateway address in the Home Agent address field of subsequent RRQ messages.

7) The Trusted non-3GPP access initiates the Gateway Control Session Establishment Procedure with the PCRF. The Trusted non-3GPP access provides the information to the PCRF to correctly associate it with the IP-CAN session and also to convey subscription related parameters to the PCRF. If the Trusted Non-3GPP access supports UE/NW bearer control mode, the PCRF provides all the QoS rules required for the Trusted Non-3GPP access to perform the bearer binding.

8) The FA processes the message according to RFC 5944 [12] and forwards a corresponding RRQ (MN-NAI, lifetime) message to the PDN GW.

9) The PDN GW informs the 3GPP AAA Server of its PDN GW identity and the APN corresponding to the UE's PDN Connection and obtains authentication and authorization information from the 3GPP AAA Server. The message includes information that identifies the PLMN in which the PDN GW is located. The 3GPP AAA Server may update the information registered in the HSS as described in clause 12.

10) The PDN GW allocates an IP address for the UE. The PDN GW initiates the IP CAN Session Modification Procedure with the PCRF, as specified in TS 23.203 [19]. The PDN GW provides information to the PCRF that the IP-CAN type has changed and the PCRF responds to the PDN GW with PCC rules and event triggers.

NOTE: When the PDN GW receives the RRQ and the the PS bearers corresponding to the PDN connection being handed over are suspended, then the PDN GW considers the bearers of the PDN connection being handed over as resumed and performs the handover.

11) The PDN GW sends a Registration Reply (RRP) (MN-NAI, Home Address, Home Agent Address) message as defined in RFC 5944 [12] to the FA.

12) The FA processes the RRP (MN-NAI, Home Address) according to RFC 5944 [12] and sends a corresponding RRP message to the UE.

13) IP connectivity from the UE to the PDN GW is now setup. A MIP tunnel is established between the FA in the Trusted Non-3GPP IP Access and the PDN GW.

14) The PDN GW shall initiate the PDN GW Initiated PDN Disconnection procedure in 3GPP access as defined in clause 5.6.2.2 or the PDN GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [4], clause 5.4.4.1.

8.3b Handover from Trusted Non-3GPP IP Access with MIPv4 FACoA on S2a to 3GPP access

In this scenario, the session starts in a trusted non-3GPP access system using MIPv4 FA CoA and subsequently, the session hands over to a 3GPP access system. The steps involved are shown in the figure below.

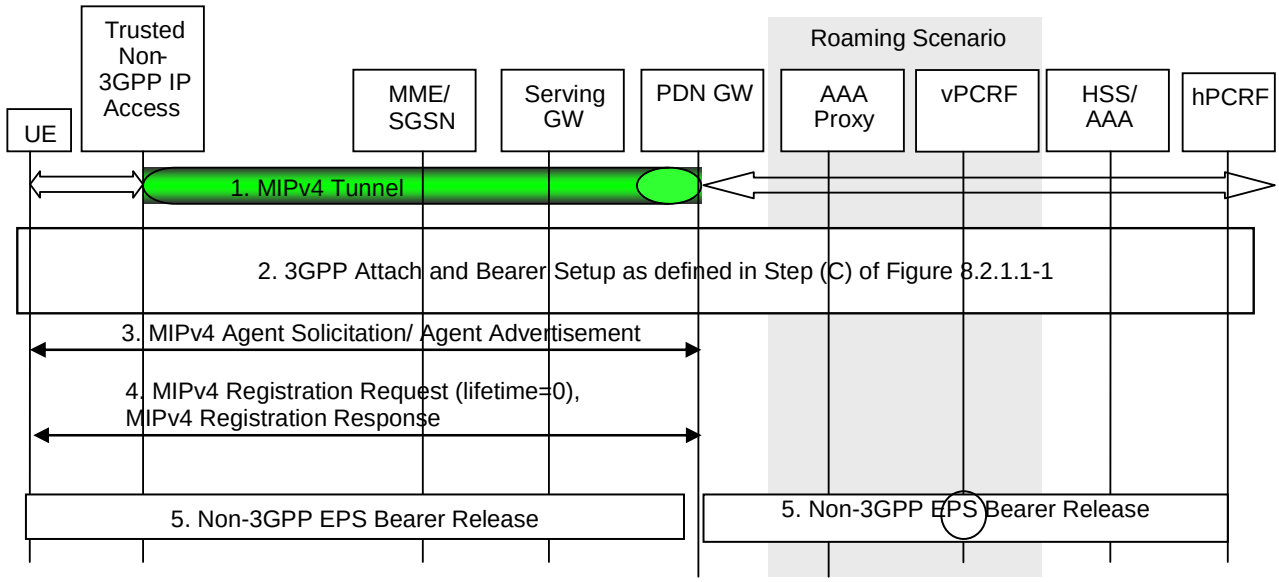


Figure 8.3b-1: Handover from Trusted Non-3GPP IP Access with MIPv4 FACoA on S2a to 3GPP Access

For connectivity to multiple PDNs the following applies:

- If UE is connected to both 3GPP access and non-3GPP access before the handover of PDN connections to 3GPP access is triggered, steps 2 to 16 of Figure 8.2.1.1-1 shall be skipped and the UE shall only perform step 17 of Figure 8.2.1.1-1 for each PDN connection that is being transferred from non-3GPP access.

- If UE is connected only to non-3GPP access before the handover of PDN connections to 3GPP access is triggered, steps 2 to 16 of Figure 8.2.1.1-1 shall be performed. In step 3 of Figure 8.2.1.1-1 the UE shall provide the APN corresponding to one of the PDN connections that are being transferred from non-3GPP access. The UE shall then repeat step 17 of Figure 8.2.1.1-1 for each of the remaining PDN connections that are being transferred from non-3GPP access.

- Steps 4 and 5 of Figure 8.3b-1 shall be repeated for each PDN connection that is being transferred from non-3GPP access.

Other impacts related to the handover for multiple PDNs are described in clause 8.1.

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

1) The UE uses a trusted non-3GPP access system. It has a MIPv4 session with the PDN GW with a FA in the trusted non-3GPP access using FACoA.

2) The UE discovers and attaches to the 3GPP access as defined in Step (C) of Figure 8.2.1.1-1, except that the IP CAN session modification and the path switch are triggered as explained below.

3) The UE may send an Agent Solicitation RFC 5944 [12] message. The HA functionality in the PDN GW sends an Agent Advertisement (AA) RFC 5944 [12] message to the UE.

4) The UE determines that it is back home through inspection of the H bit and advertised prefix within the agent advertisement (AA) received in the previous step. The UE sends a Registration Request message with the destination address set to the HA's address and with a Lifetime field set to 0 to indicate deregistration. Once the deregistration request is accepted, the UE receives an Registration Response message from the HA.

5) The PDN GW shall initiate resource allocation deactivation procedure in the trusted/untrusted non-3GPP IP access as defined in clause 6.12.

8.4 Handovers with DSMIPv6 on S2c

8.4.1 Trusted or Untrusted Non-3GPP IP Access with DSMIPv6 over S2c to 3GPP Access Handover

In this scenario, the session starts in a trusted or untrusted non-3GPP access system using DSMIPv6 and subsequently, the session hands over to a 3GPP access system.

The steps involved in the handover from a trusted/untrusted non-3GPP IP access to 3GPP Access connected to EPC are depicted below when DSMIPv6 is used on S2c over non-3GPP system.

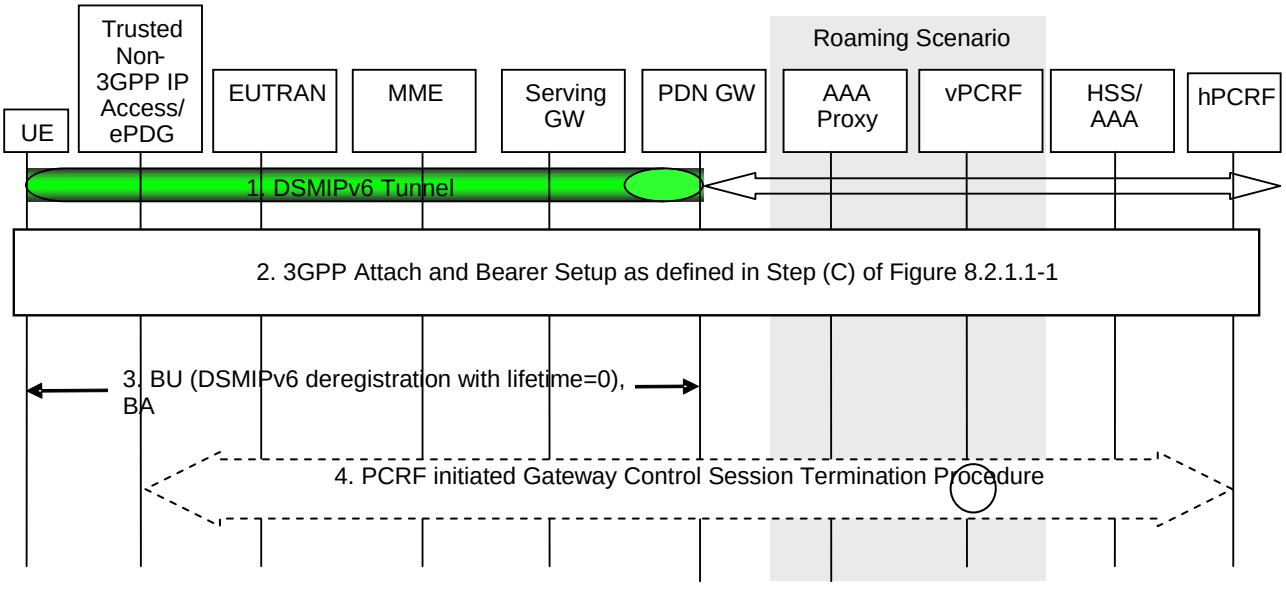


Figure 8.4.1-1: Trusted Non-3GPP S2c (DSMIPv6) to 3GPP with S5 handover

For connectivity to multiple PDNs the following applies:

- If UE is connected to both 3GPP access and non-3GPP access before the handover of PDN connections to 3GPP access is triggered, steps 2 to 16 of Figure 8.2.1.1-1 shall be skipped and the UE shall only perform step 17 of Figure 8.2.1.1-1 for each PDN connection that is being transferred from non-3GPP access.

- If UE is connected only to non-3GPP access before the handover of PDN connections to 3GPP access is triggered, steps 2 to 16 of Figure 8.2.1.1-1 shall be performed. In step 3 of Figure 8.2.1.1-1 the UE shall provide the APN corresponding to one of the PDN connections that are being transferred from non-3GPP access. The UE shall then repeat step 17 of Figure 8.2.1.1-1 for each of the remaining PDN connections that are being transferred from non-3GPP access.

- Step 3 of Figure 8.4.1-1 shall be repeated for each PDN connection that is being transferred from non-3GPP access.

Other impacts related to the handover for multiple PDNs are described in clause 8.1.

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateway.

1) The UE uses a trusted or untrusted non-3GPP access system. It has a DSMIPv6 session with the PDN GW.

2) The UE discovers and attaches to the 3GPP access as defined in Step (C) of Figure 8.2.1.1-1, except that the IP-CAN session modification and the path switch are triggered as explained below.

3) The UE sends a BU (lifetime) to the PDN GW to de-register its DSMIPv6 binding, as defined in RFC 5555 [10] that was created while the UE was in non-3GPP access system. The UE shall inform the PDN GW that the whole home prefix shall be moved. The PDN GW responds with a BA message as defined in RFC 5555 [10].

   Any time after step 2, prior to receiving the de-registration Binding Update from the UE (i.e. BU with lifetime = 0), which is received in (step 3), the PDN GW may de-register the DSMIPv6 binding. In this case the PDN GW shall send a Binding Revocation Indication message to the UE.

   Following the de-registration of the DSMIPv6 binding due to reception of de-registration Binding update or due to triggering Binding Revocation, the PDN GW triggers PCEF initiated IP-CAN session modification, instead of doing it as part of the step 2, and performs path switch to forward downlink packets to the UE without any tunnelling (as the UE is on the home link).

4) This step occurs only if all PDN connections have handed over to the 3GPP access. The PCRF initiates "PCRF-initiated Gateway Control Session Termination" procedure to release the resources in the non-3GPP access. This procedure is triggered by the PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF, occurring as a result of step 2.

According to RFC 4877 [22] the security associations between the UE and the PDN GW(s) should not be immediately deleted. As the security associations were created dynamically using IKEv2 they will be automatically deleted when they expire. The IP address used by the UE as home address is not released by the UE and the PDN GW as a result of the deletion of such security associations if the UE remains connected to the PDN GW. This applies also to the scenario where the UE performed the initial attach over a 3GPP access and was given a IP address, bootstrapped the DSMIPv6 over the 3GPP access, performed an handover to the non-3GPP access using S2c, and is now performing an handover towards 3GPP access and therefore returning to the Home Link.

8.4.2 3GPP Access to Trusted Non-3GPP IP Access Handover with DSMIPv6 over S2c

In this scenario, the session starts in 3GPP access (e.g. E-UTRAN) using PMIPv6 or GTP over S5 or no S5 is used (co-located Serving GW and PDN GW). The session hands over to the trusted non-3GPP access system that does not use PMIPv6 where the UE will receive a different prefix than the one it was using in 3GPP access system. The UE subsequently initiates DSMIPv6 with the same PDN GW to maintain the IP session.

Support of PCC for Trusted non-3GPP accesses is optional. The PCC interactions shown in Figure 8.4.2-1 are omitted if the Trusted non-3GPP access does not support PCC. If PCC is not supported, policy rules may be configured by other means.

In the non-roaming case, none of the optional entities in Figure 8.4.2-1 are involved.

The optional entities are involved in other cases.

- In the roaming cases, however, the 3GPP AAA Proxy mediates all interaction between the 3GPP AAA Server in the PLMN and entities in the VPLMN and non-3GPP access.
- Similarly, interaction between hPCRF in the HPLMN and entities in the VPLMN and non-3GPP access occurs by way of the vPCRF in the VPLMN. In both these cases, messages are relayed by the optional entities towards and from the HPLMN.

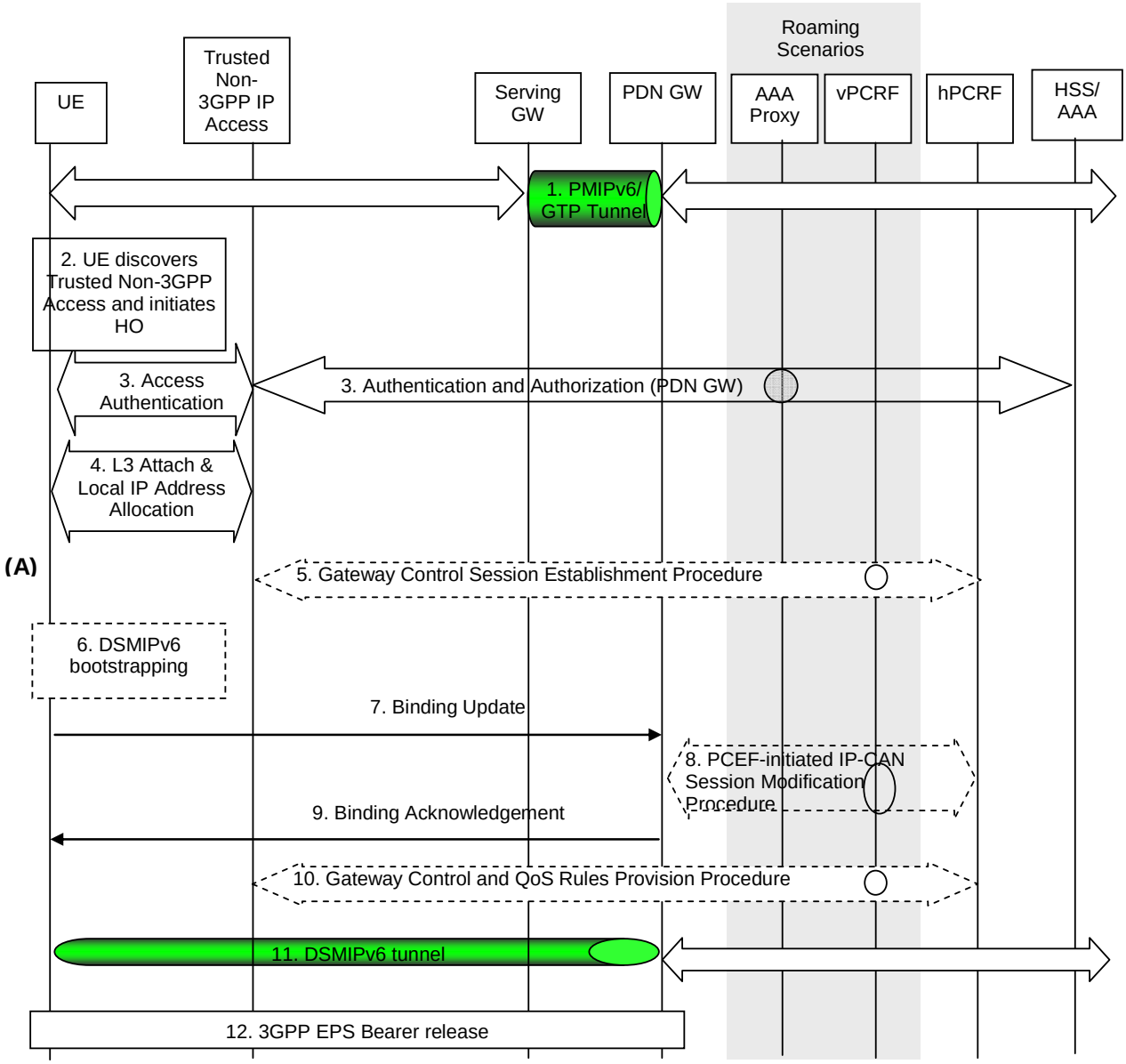


Figure 8.4.2-1: 3GPP S5 to Trusted Non-3GPP S2c (DSMIPv6) Handover

In case of connectivity to multiple PDNs the following applies:

- If the UE is connected to both 3GPP access and non-3GPP access before the handover of PDN connections to trusted non-3GPP access is triggered, steps 2 to 5 shall be skipped.
- If the UE is connected only to 3GPP access before the handover of PDN connections to trusted non-3GPP access is triggered, steps 2 to 5 shall be performed.
- Steps 7 to 12 shall be repeated for each PDN connection that is being transferred from 3GPP access. If not performed in 3GPP access prior to the handover, Step 6 shall also be repeated for each PDN connection that is being transferred from 3GPP access.

Other impacts related to the handover for multiple PDNs are described in clause 8.1

1) The UE uses a 3GPP access system. It has an IP address that is supported over S5 interface, this IP address will be used as a HoA over the S2c reference point.

2) At this point the UE decides to initiate non-3GPP access procedure. The decision is based on any number of reasons e.g. local policies of the UE.

3) The UE shall perform access authentication and authorization in the non-3GPP access system as defined by TS 33.402 [45] unless the conditions in TS 33.402 [45] are met that allow to skip this procedure. In the roaming case signalling may be routed via a 3GPP AAA Proxy in the VPLMN. As part of the AAA exchange for network access authentication, the 3GPP AAA Server and/or the 3GPP AAA Proxy may return to the non-3GPP access system a set of home/visited operator's policies to be enforced on the usage of local IP address, or IPv6 prefix, allocated by the access system upon successful authentication.

4) The L3 connection is established between the UE and the Trusted Non-3GPP Access system. As a result of this procedure, an IPv4 address or an IPv6 address/prefix is also assigned to the UE by the access system (i.e. a Local IP address that will be used as a Care-of Address for DSMIPv6 over the S2c reference point).

5) The Trusted non-3GPP IP Access initiates a Gateway Control Session Establishment Procedure with the PCRF as specified in TS 23.203 [19].

   Based e.g. on the UE identity and user profile, operator's policies and the IP-CAN type, the PCRF decides on the QoS policy rules and completes the GW control session establishment towards the access gateway (5b)

   In the roaming case, PCC signalling is sent via a vPCRF server in the VPLMN

6) If bootstrapping was not performed prior to the handover defined here, the UE may discover PDN GW address using MIPv6 bootstrapping procedures defined in clause 4.5.2. If the PDN GW discovered by the UE upon MIPv6 bootstrapping is different from the PDN GW that was in use on the 3GPP access, a PDN GW reallocation as per steps 2-3 in clause 6.10 is performed. The target PDN GW that is communicated to the UE as part of the reallocation procedure must be exactly the PDN GW that was serving the UE while on the 3GPP access.

7) The UE sends a DSMIPv6 BU message to the PDN GW to register its CoA, the CoA is the local IP address allocated in step 4. The UE shall inform the PDN GW that the whole home prefix shall be moved.

NOTE: When the PDN GW receives the BU and the the PS bearers corresponding to the PDN connection being handed over are suspended, then the PDN GW considers the bearers of the PDN connection being handed over as resumed and performs the handover.

8) If PCC is supported, the PDN GW executes a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19].

   In the roaming case, PCC signalling is sent via a vPCRF server in the VPLMN.

9) The PDN GW sends the MIP Binding Ack to the UE. Since this step is triggered by the Binding Update message from the UE in step 7, it can occur after step 7 and does not need to wait for step 8.

   The PDN GW may send message 9 before the procedure in step message 8 is complete.

10) The PCRF initiates the Gateway Control and QoS Rules Provision Procedure specified in TS 23.203 [19] by sending a message with the information of mobility protocol tunnelling encapsulation header to the Trusted non-3GPP IP Access. In case the QoS rules have changed, the updated QoS rules shall also be included in this message.

11) The UE continues with IP service using the same IP address in step 1.

12) The PDN GW shall initiate the PDN GW Initiated PDN Disconnection procedure in 3GPP access as defined in clause 5.6.2.2 or the PDN GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [4], clause 5.4.4.1.

8.4.3 3GPP Access to Untrusted Non-3GPP IP Access Handover with DSMIPv6 over S2c

In this scenario, the session starts in 3GPP access (e.g. E-UTRAN) using either GTP or PMIPv6 is used over S5, or no S5 is used (co-located Serving GW and PDN GW).). In the roaming case instead of S5, S8 is used. The session hands

over to an untrusted non-3GPP access system that does not use PMIPv6 where the UE will receive a different prefix from the ePDG than the one it was using in 3GPP access system The UE subsequently initiates DSMIPv6 with the its PDN GW to maintain the IP session.

Support of PCC for Untrusted non-3GPP accesses is optional. The PCC interactions shown in Figure 8.4.3-1 are omitted if the Untrusted non-3GPP access does not support PCC. If PCC is not supported, policy rules may be configured by other means.

In the non-roaming case, none of the optional entities in Figure 8.4.3-1 are involved.

The optional entities are involved in other cases.

- In the roaming cases, however, the 3GPP AAA Proxy mediates all interaction between the 3GPP AAA Server in the PLMN and entities in the VPLMN and non-3GPP access.
- Similarly, interaction between hPCRF in the HPLMN and entities in the VPLMN and non-3GPP access occurs by way of the vPCRF in the VPLMN. In both these cases, messages are relayed by the optional entities towards and from the HPLMN.

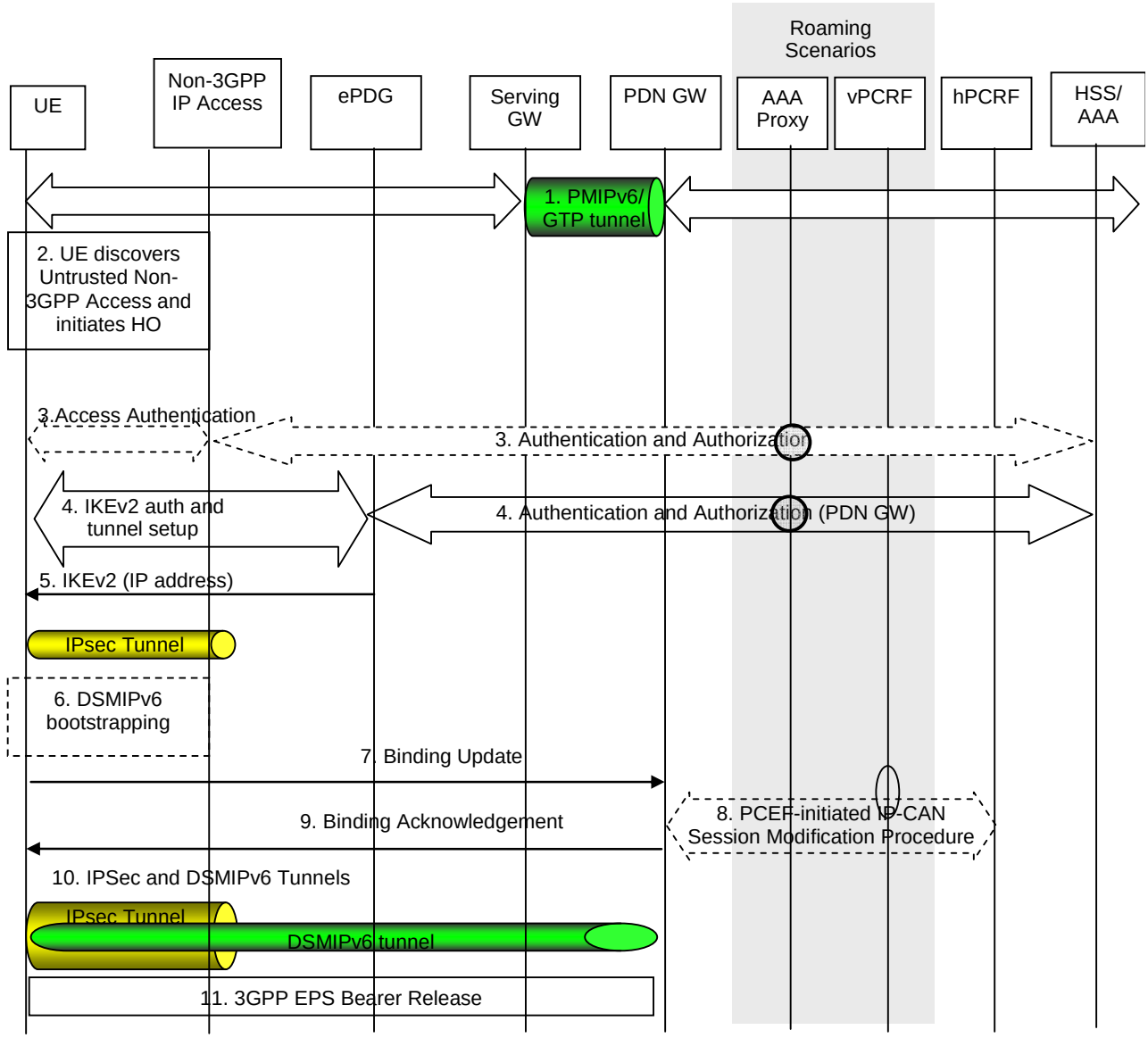


Figure 8.4.3-1: 3GPP Access to Untrusted Non-3GPP IP Access with S2c (DSMIPv6) Handover

In case of connectivity to multiple PDNs the following applies:

- If the UE is connected to both 3GPP access and non-3GPP access before the handover of PDN connections to untrusted non-3GPP access is triggered, steps 2 to 4 shall be skipped.

- If the UE is connected only to 3GPP access before the handover of PDN connections to untrusted non-3GPP access is triggered, steps 2 to 4 shall be performed.

- Steps 6 to 10 shall be repeated for each PDN connection that is being transferred from 3GPP access. If not performed in 3GPP access prior to the handover, Step 5 shall also be repeated for each PDN connection that is being transferred from 3GPP access.

Other impacts related to the handover for multiple PDN GWs are described in clause 8.1

1. The UE uses a 3GPP access system. It has an IP address that is supported over S5 interface, this IP address will be used as a HoA over the S2c reference point.

2. At this point the UE decides to initiate non-3GPP access procedure. The decision is based on any number of reasons e.g. local policies of the UE.

3 Access authentication procedure between UE and the 3GPP EPC may be performed as defined by TS 33.402 [45].

4. The IKEv2 tunnel establishment procedure is started by the UE. The UE may indicate in a notification part of the IKEv2 authentication request that it supports MOBIKE. The ePDG IP address to which the UE needs to form IPsec tunnel is discovered via DNS query as specified in clause 4.5.4. After the UE is authenticated, UE is also authorized for access to the APN. The procedure is as described in TS 33.402 [45].

NOTE 1: It is assumed that the access system is aware that network-based mobility procedures do not need to be initiated.

5. The ePDG sends the final IKEv2 message with the assigned IP address in IKEv2 Configuration payloads. The IKEv2 procedure is completed and the IPSEC tunnel is set-up. In this procedure, the assigned IP address is an IPv4 address or an IPv6 prefix assigned to the UE by the ePDG and the assigned IP address that will be used as a Care-of Address for DSMIPv6 over the S2c reference point.

6. If bootstrapping was not performed prior to the handover defined here, the UE may discover PDN GW address using DSMIPv6 bootstrapping procedures defined in clause 4.5.2. If the PDN GW discovered by the UE upon MIPv6 bootstrapping is different from the PDN GW that was in use on the 3GPP access, a PDN GW reallocation as per steps 2-3 in clause 6.10 is performed. The target PDN GW that is communicated to the UE as part of the reallocation procedure must be exactly the PDN GW that was serving the UE while on the 3GPP access.

7. The UE sends a DSMIPv6 BU message to the PDN GW to register its CoA. The UE shall inform the PDN GW that the whole home prefix shall be moved.

8. If PCC is supported, the PDN GW executes a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19] to obtain the rules required for the PDN GW in the VPLMN or HPLMN to function as the PCEF for all the active sessions the UE has established with the new IP-CAN type as a result of the handover procedure.

NOTE 2: When the PDN GW receives the Proxy Binding Update and the the PS bearers corresponding to the PDN connection being handed over are suspended, then the PDN GW considers the bearers of the PDN connection being handed over as resumed and performs the handover.

9. The PDN GW sends the DSMIPv6 Binding Ack to the UE. Since this step is triggered by the Binding Update message from the UE in step 6, it can occur after step 6 and does not need to wait for step 7.

   The PDN GW may send message 8 before the procedure in step 8 is complete.

10. The UE continues with IP service using the same IP address in step 1.

11. The PDN GW shall initiate the PDN GW Initiated PDN Disconnection procedure in 3GPP access as defined in clause 5.6.2.2 or the PDN GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [4], clause 5.4.4.1.

8.5 Handover with Access Network Discovery and Selection

8.5.1 Handover between 3GPP Access and Trusted / Untrusted Non-3GPP IP Access with access network discovery and selection

The figure below shows the main steps involved in a handover between a 3GPP access and a non-3GPP IP access (also called an inter-system handover) when network discovery and selection information is provided by the network (see clause 4.8). This information is provided in order to control the UE's inter-system handover decisions and in order to reduce the battery consumption for inter-system mobility.

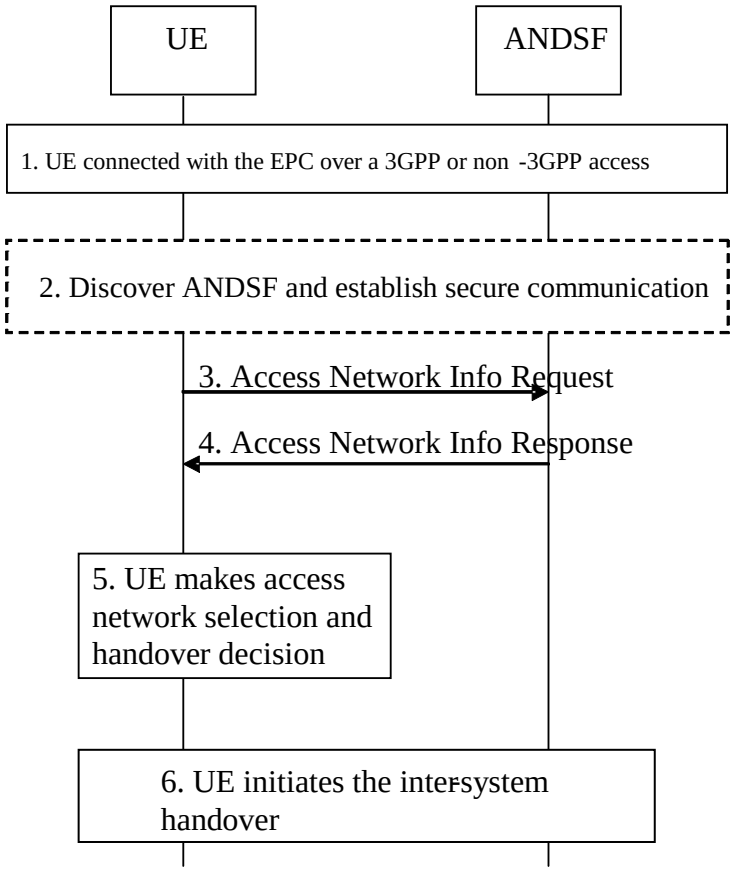


Figure 8.5.1-1: Handover between 3GPP Access and trusted / untrusted non-3GPP IP Access with Access Network Discovery and Selection

1. The UE is connected with a source access network (either a 3GPP access or a trusted / untrusted non-3GPP IP access). Its radio interfaces not connected to any access network may be in power saving or powered down mode.

2. If the inter-system mobility policies (see clause 4.8) in the UE indicate that inter-system mobility is allowed with at least one access technology type, then the UE may decide to discover neighbour access networks with assistance by the network. In this case, the UE discovers the address of ANDSF (if needed) as specified in clause 4.8, establishes secure communication with the ANDSF as specified in TS 33.402 [45] and requests access network info from the ANDSF as specified in the steps below.

3. The UE sends an Access Network Info Request (UE Capabilities, UE Location) message to the H-ANDSF (in the non-roaming and roaming case) and the V-ANDSF (in the roaming case) to retrieve network discovery and selection information. The UE Capabilities indicate the capabilities of the UE pertaining to access network discovery, such as the access technology types that can be supported by the UE. If the UE Location is available in the UE, it should be included in the message to indicate the UE's current location, e.g. for the 3GPP access, Cell ID, TAI, and/or GPS (if available). If the UE Location is not included then other mechanisms may be used by ANDSF to identify the UE's current location.

NOTE 1: In this Release of the specification, no mechanisms are specified for the ANDSF to identify the UE's current location, if this information is not provided by the UE.

4. The ANDSF responds with an Access Network Info Response (Available Access Network Info, Updated Inter-system Mobility Policies) message to the UE. The Available Access Networks Info contains a list of access networks that are available in the vicinity of UE. If the UE included one or more access technology types in the Access Network Info Request, then information about neighbour access network with the requested access technology types is included. The Updated Inter-system Mobility Policies may be included in order to update / install operator defined rules / preferences in the UE. These rules / preferences may indicate a preference value for an available access network and help the UE select an available access network that is more preferable to the current access network.

5. The UE powers up its appropriate radio interface(s) (if needed) and measures the available access networks for which inter-system mobility is allowed, as indicated by the updated / current inter-system mobility policies. The UE selects the most preferable available access network for inter-system mobility based on the inter-system mobility policies and user preferences.

6. If the UE selects a preferable access network for handover, then the UE initiates handover to the selected access network as described in clause 8.

NOTE 2: Steps 2, 3 and 4 in the above procedure may not immediately result in an inter-system handover (steps 5 and 6).

8.6 Handovers between non-3GPP IP access with GTP on S2b and 3GPP Access

8.6.1 Handover from Untrusted Non-3GPP IP Access with GTP on S2b to 3GPP Access

8.6.1.1 General Procedure for GTP based S5/S8 for E-UTRAN Access

The steps involved in the handover from an untrusted non-3GPP IP access to E-UTRAN connected to EPC are depicted below for both the non-roaming and roaming cases and when GTP is used on S2b. It is assumed that while the UE is served by the untrusted non-3GPP IP access, GTP tunnel(s) are established between the ePDG and the PDN GW in the EPC.

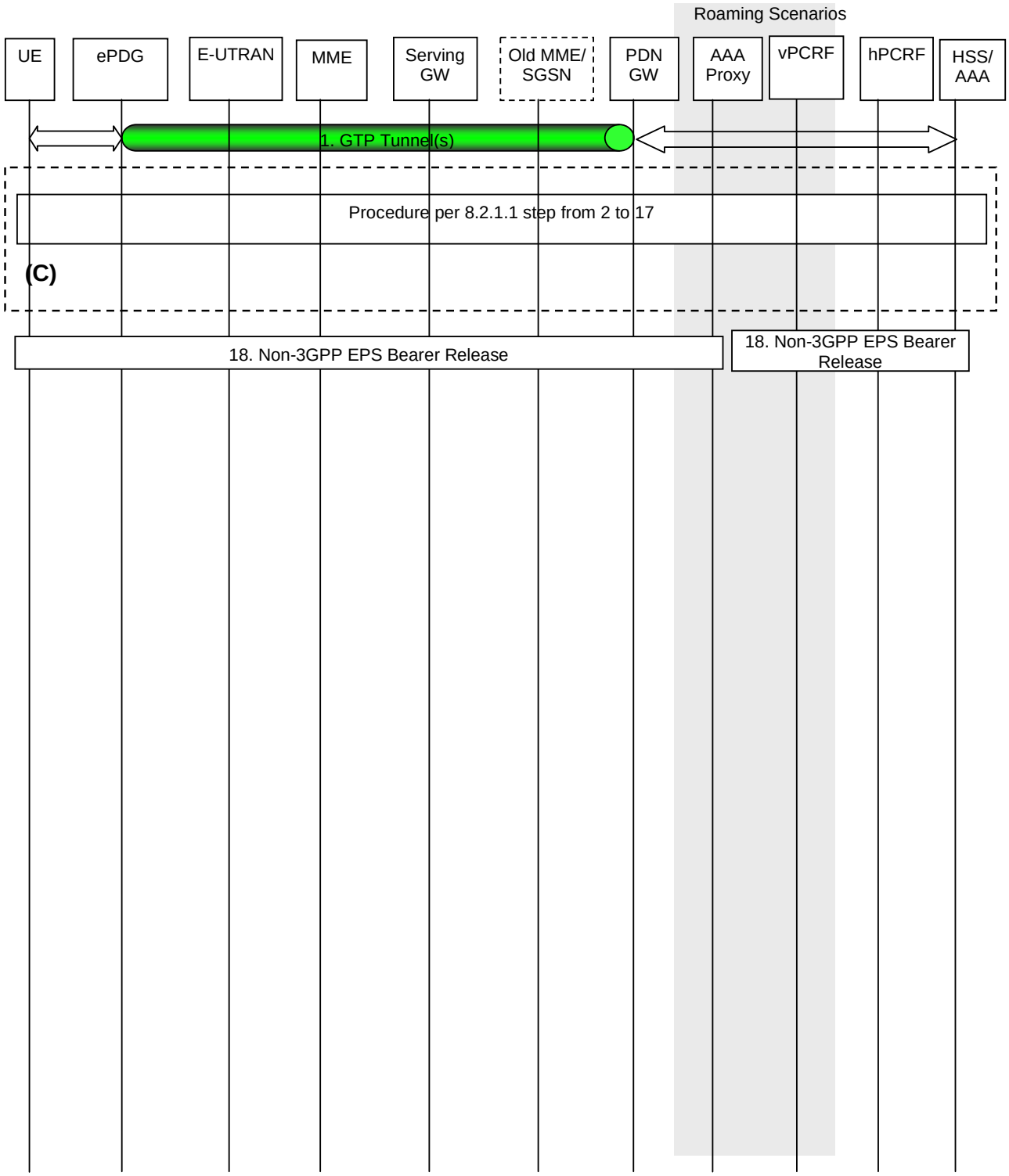


Figure 8.6.1.1-1: Handover from Untrusted Non-3GPP IP Access to E-UTRAN with GTP on S2b and GTP on S5/S8 interfaces

The home routed roaming (Figure 4.2.3-1), LBO (Figure 4.2.3-4) and non-roaming (Figure 4.2.2-1) scenarios are depicted in the figure.

- In the LBO case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the PDN GW in the VPLMN. The vPCRF receives the Acknowledgment from the PDN GW and forwards it to the hPCRF.

- In the non-roaming and home routed roaming case, the vPCRF is not involved.

In case of connectivity to multiple PDNs the same behaviour as described in clause 8.2.1.1 also applies to this procedure.

1) The UE uses an untrusted non-3GPP access system and is being served by PDN GW.

2 to 17) as for steps 2 to 17 of clause 8.2.1.1.

On step 9, the Charging Id provided by the PGW to the default and dedicated bearers in 3GPP access is the Charging Id previously assigned to the corresponding default and the dedicated bearers (i.e. bearer with the same QCI and ARP) of the PDN connection in the non-3GPP access on the S2b interface, although the Charging Id still applies to the non-3GPP access.

NOTE 1: Depending upon the support of the piggybacking feature in the network, the dedicated bearer can be created as part of default bearer establishment or immediately afterwards.

On step 13, the Charging Id previously in use for the default and dedicated bearers in the non-3GPP access on the S2b interface now applies to the corresponding default and dedicated bearers in 3GPP access (i.e. bearer with the same QCI and ARP as in non-3GPP access).

NOTE 2: Two GTP sessions may exist in the PDN GW for the same UE and APN over the S2b and S5/S8 interfaces during a transient period.

18) The PDN GW shall initiate resource allocation deactivation procedure in the untrusted non-3GPP IP access as defined in clause 7.9.2

8.6.1.2 General Procedure for GTP-based S5/S8 for UTRAN/GERAN

The steps involved in the handover from an untrusted non-3GPP IP access to UTRAN/GERAN connected to EPC are depicted below for both the non-roaming and roaming cases and when GTP is used on S2b. It is assumed that while the UE is served by the untrusted non-3GPP IP access, GTP tunnel(s) are established between the non-3GPP access network and the PDN GW in the EPC.

NOTE 1: This procedure is applicable to S4-SGSN only.

The home routed roaming (Figure 4.2.3-1), LBO (Figure 4.2.3-4) and non-roaming (Figure 4.2.2-1) scenarios are depicted in the figure.

- In the LBO case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the PDN GW in the VPLMN. The vPCRF receives the Acknowledgment from the PDN GW and forwards it to the hPCRF.

- In the non-roaming and home routed roaming case, the vPCRF is not involved.

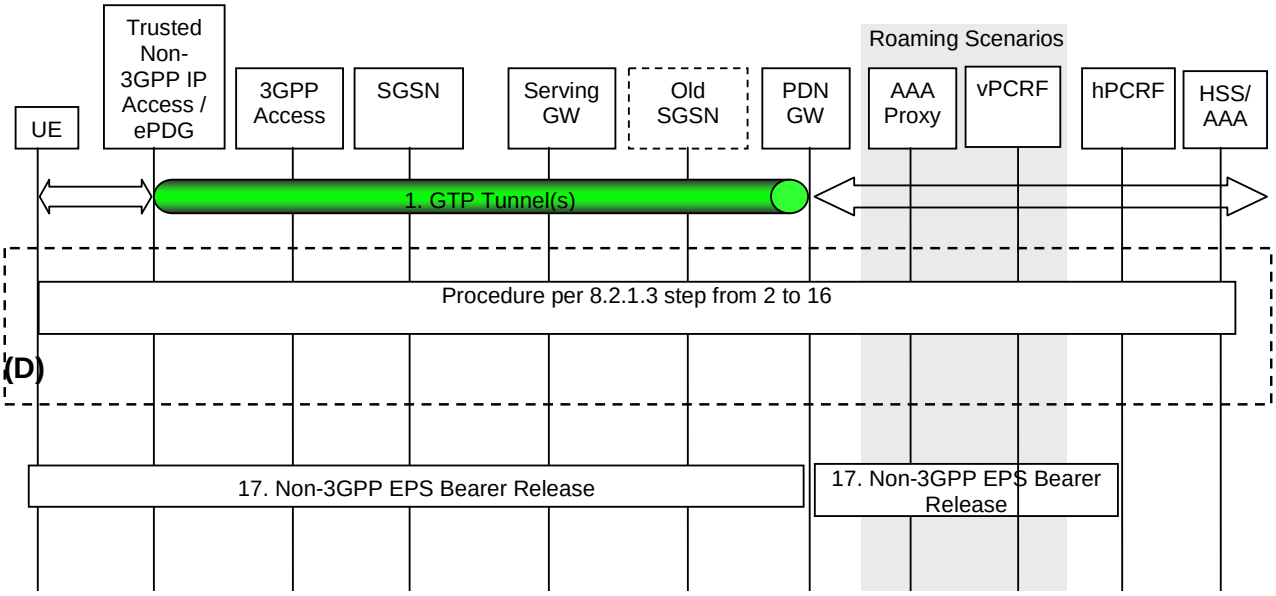


Figure 8.6.1.2-1: Handover from Untrusted Non-3GPP IP Access to UTRAN/GERAN with GTP on S2b and GTP on S5/S8 interfaces

In case of connectivity to multiple PDNs the same behaviour as described in clause 8.2.1.3 also applies to this procedure.

1) The UE uses an untrusted non-3GPP access system and is being served by PDN GW.

2) to 16) As for steps 2 to 16 of clause 8.2.1.3.

On step 11, the Charging Id provided by the PGW to the default and dedicated bearers in 3GPP access is the Charging Id previously assigned to the corresponding default and the dedicated bearers (i.e. bearer with the same QCI and ARP) of the PDN connection in the non-3GPP access on the S2b interface, although the Charging Id still applies to the non-3GPP access.

NOTE 2: For UTRAN/GERAN access, the dedicated bearer establishment does not take place along with the default bearer establishment (i.e. sending of Create Session Response message).

On step 14, the Charging Id previously in use for the default and dedicated bearers in the non-3GPP access on the S2b interface now applies to the corresponding default and dedicated bearers in 3GPP access (i.e. bearer with the same value of QCI, ARP).

NOTE 3: Two GTP sessions may exist in the PDN GW for the same UE and APN over the S2b and S5/S8 interfaces during a transient period.

17) The PDN GW shall initiate resource allocation deactivation procedure in the untrusted non-3GPP IP access as defined in clause 7.9.2.

8.6.2 Handover from 3GPP access to untrusted Non-3GPP IP Access with GTP on S2b

8.6.2.1 3GPP Access to Untrusted Non-3GPP IP Access Handover with GTP on S2b

This clause shows a call flow for a handover when a UE moves from a 3GPP Access to an untrusted non-3GPP access network. GTP is assumed to be used on the S5/S8 interface and GTP is used on the S2b interface.

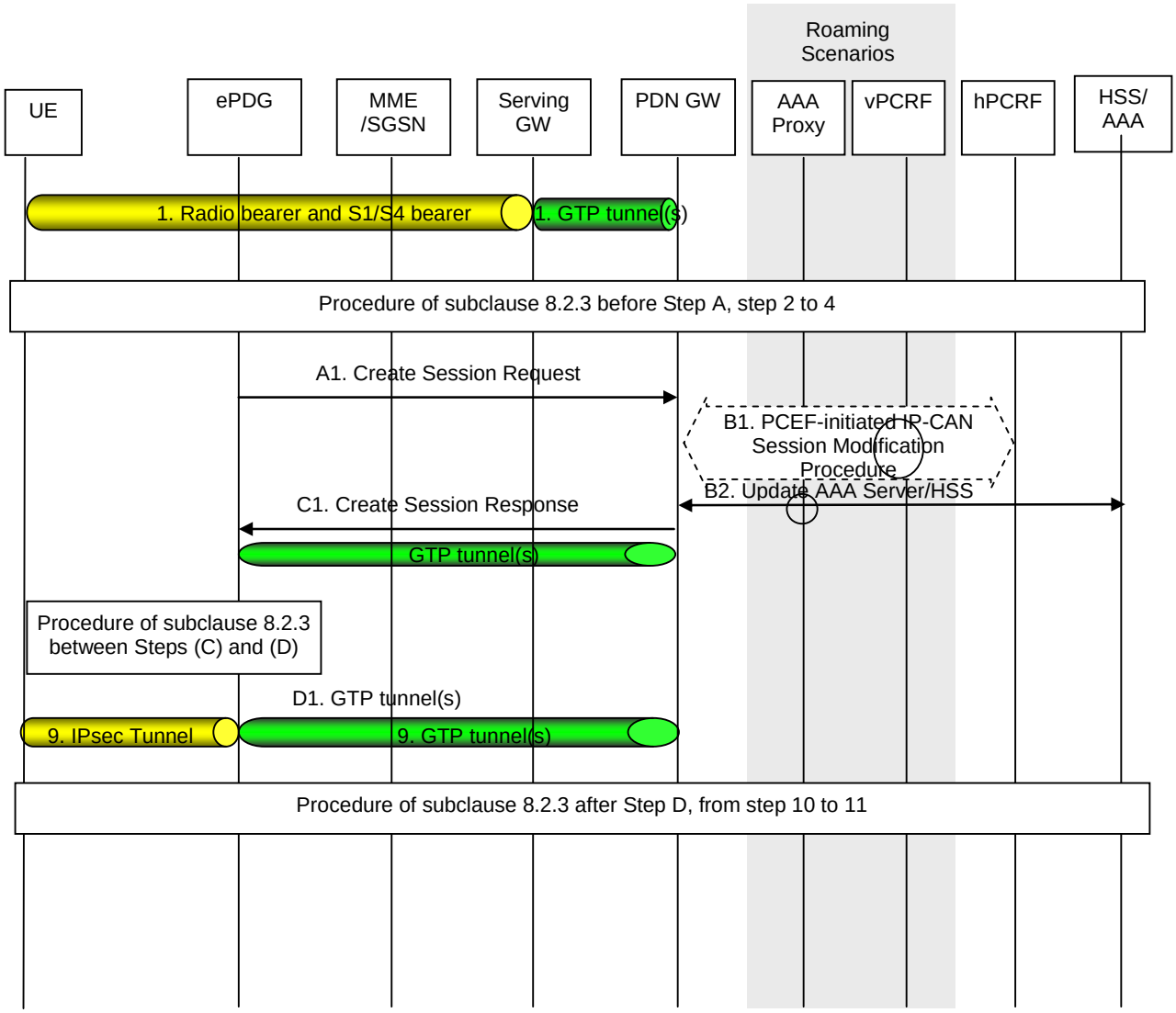


Figure 8.6.2.1-1: Handover from 3GPP Access to Untrusted Non-3GPP IP Access with GTP on S2b

The home routed roaming (Figure 4.2.3-1), LBO (Figure 4.2.3-4) and non-roaming (Figure 4.2.2-1) scenarios are depicted in the figure.

- In the LBO case, the vPCRF acts as an intermediary, sending the QoS Policy Rules Provision from the hPCRF in the HPLMN to the PDN GW in the VPLMN. The vPCRF receives the Acknowledgment from the PDN GW and forwards it to the hPCRF.

- In the non-roaming and home routed roaming case, the vPCRF is not involved.

In case of connectivity to multiple PDNs the same behaviour as described in clause 8.2.3 also applies to this procedure.

The optional interaction steps between the PDN gateway and the PCRF in the procedures only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured in the PDN gateway.

A.1) The ePDG sends a Create Session Request (IMSI, APN, Handover Indication, RAT type, ePDG TEID of the control plane, ePDG Address for the user plane, ePDG TEID of the user plane, EPS Bearer Identity, User Location Information) message to the PDN GW. The RAT type indicates the non-3GPP IP access technology type. If the UE supports IP address preservation and included the address in step 3, the ePDG sets the 'Handover Indication' in the Creation Session Request to allow the PDN GW to re-allocate the same IP address or prefix that was assigned to the UE while it was connected to the 3GPP IP access and to initiate a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF.

The User Location Information shall include UE local IP address and optionally UDP source port number (if NAT is detected). It may also include WLAN Location Information (and its Age) the ePDG may have received from the 3GPP AAA server about the UE.

NOTE 1: The UE local IP address is the source address on the outer header of the IPsec tunnel to the ePDG.

NOTE 2: In a non-3GPP to 3GPP access handover, the 'Handover Indication' leads the PDN GW to delay switching the DL user plane traffic from non-3GPP to 3GPP until a subsequent Modify Bearer Request is received. In a 3GPP to non-3GPP handover scenario with GTP based S2b, the 'Handover Indication' should not delay the switching of DL user plane traffic from 3GPP to non-3GPP access.

NOTE 3: When the PDN GW receives the Create Session Request and the the PS bearers corresponding to the PDN connection being handed over are suspended, then the PDN GW considers the bearers of the PDN connection being handed over as resumed and performs the handover.

B.1) Step B.1 is the same as Step B of clause 8.2.3 with the following addition:

- If requested by the PCRF, the PDN GW forwards to the PCRF in the IP-CAN Session Establishment procedure following information extracted from User Location Information it may have received from the ePDG:

  - The UE local IP address.

  - WLAN location information in conjunction with the Age of this information.

B.2) The PDN GW informs the 3GPP AAA Server of its PDN GW identity and the APN corresponding to the UE's PDN Connection and obtains authorization information from the 3GPP AAA Server. The message includes information that identifies the PLMN in which the PDN GW is located. The 3GPP AAA Server may update the information registered in the HSS as described in clause 12.

C.1) The PDN GW responds with a Create Session Response (PDN GW Address for the user plane, PDN GW TEID of the user plane, PDN GW TEID of the control plane, PDN Type, PDN Address, EPS Bearer Identity, EPS Bearer QoS, APN-AMBR, Charging ID, Cause) message to the ePDG. The Create Session Response contains the IP address and/or the prefix that was assigned to the UE while it was connected to the 3GPP IP access. The Charging Id provided by the PGW is the Charging Id previously assigned to the default bearer of the PDN connection in the 3GPP access.

Depending upon the active PCC rules, the PDN GW may create dedicated bearers on S2b interface. And in that case, it applies the Charging ID previously in use for the corresponding dedicated bearer(s) while the UE was connected to the 3GPP IP access (i.e. bearer with the same QCI and ARP as in 3GPP access).

D.1) At the end of the handover procedure, the PDN connectivity service is provided by IPsec connectivity between the UE and the ePDG concatenated with S2b bearer(s) between the ePDG and the PDN GW.

9 Handovers with Optimizations Between E-UTRAN Access and CDMA2000 Access

9.1 Architecture and Reference Points

9.1.1 Architecture for Optimized Handovers between E-UTRAN Access and cdma2000 HRPD Access

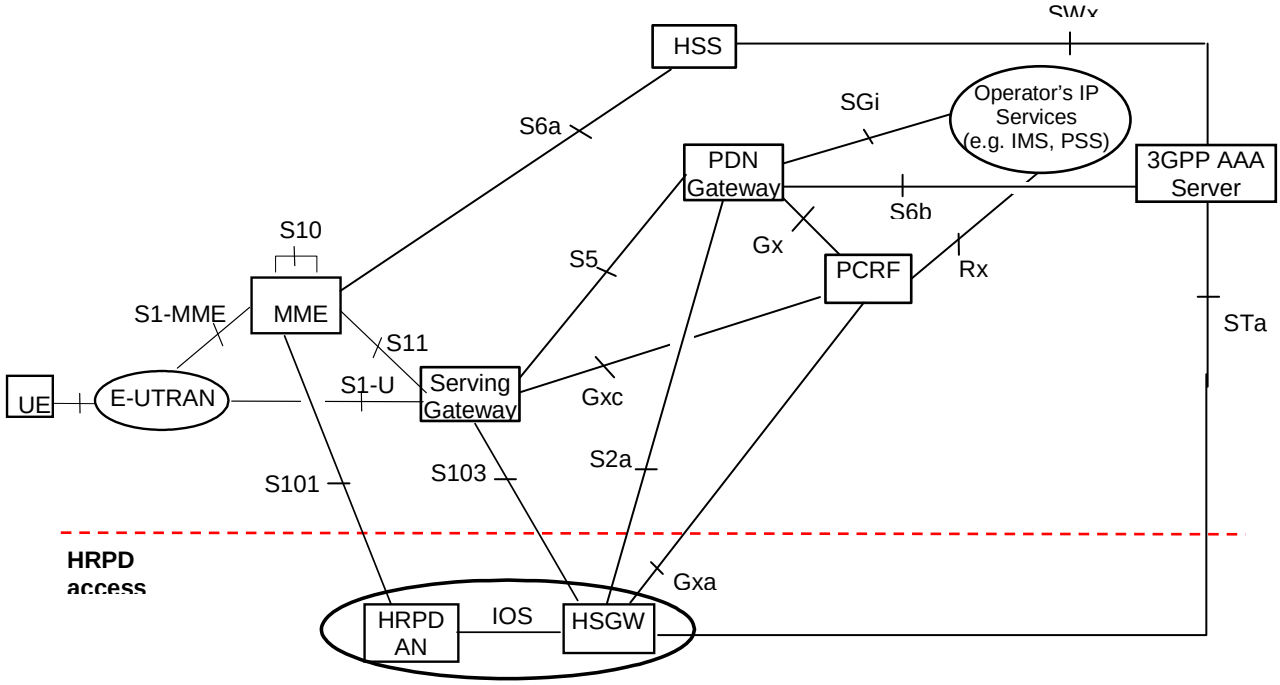


Figure 9.1.1-1: Architecture for optimised handovers between E-UTRAN access and cdma2000 HRPD access (non-roaming case)

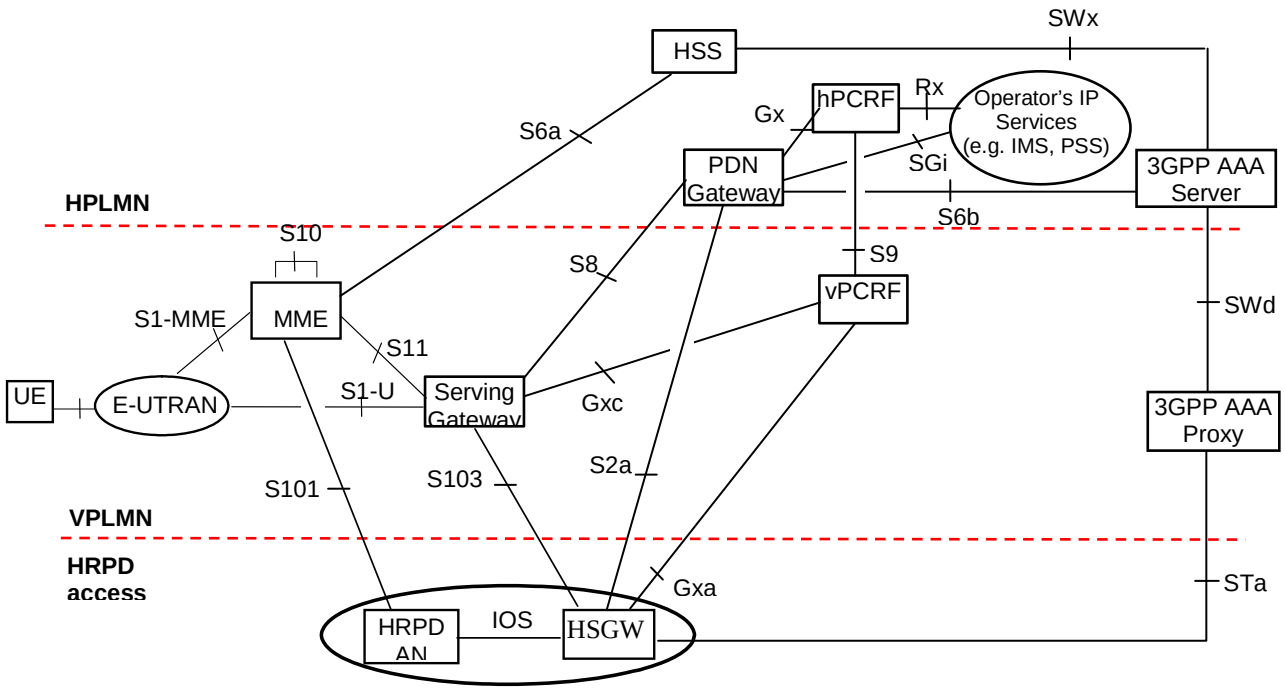


Figure 9.1.1-2: Architecture for optimised handovers between E-UTRAN access and cdma2000 HRPD access (roaming case; Home routed)

NOTE 1: Optimized handover supported by this architecture is intended for the scenario where the operator owns both the E-UTRAN access and the HRPD access, or where there is a suitable inter-operator agreement in place.

NOTE 2: Gxc is used only in the case of PMIP variant of S5 or S8.

NOTE 3: For further specification of the functions and interfaces of the HRPD Serving GW (HS-GW) refer to 3GPP2 X.S0057 [51]. The HRPD in this specification refers to the evolved HRPD as defined in 3GPP2 X.S0057 [51].

Depicted in Figure 9.1.1-1 is an access specific architecture providing support for optimised E-UTRAN-HRPD handovers. in the non-roaming case. Depicted in figure 9.1.1-2 is an access specific architecture providing support for optimised E-UTRAN-HRPD handovers in the roaming case with Home routed traffic.

9.1.2 Reference Points

9.1.2.1 Reference Point List

S101: It enables interactions between EPS and HRPD access to allow for pre-registration and handover signalling with the target system.

S103: This User Plane interface is used to forward DL data to minimize packet losses in mobility from E-UTRAN to HRPD.

9.1.2.2 Requirements for the S101 Reference Point

The S101 interface supports procedures for Pre-Registration, Session Maintenance and Active handovers between E-UTRAN and HRPD networks. This is based on tunnelling over S101 signalling of one technology while the UE is in the other technology. The HRPD air interface messages tunnelled over S101 in E-UTRAN to HRPD mobility are defined in 3GPP2 C.S0087-0 [49].

The S101 reference point shall support the following requirements:

- HRPD and E-UTRAN/EPS messages shall be transported as opaque containers without modifications by the MME or HRPD AN.

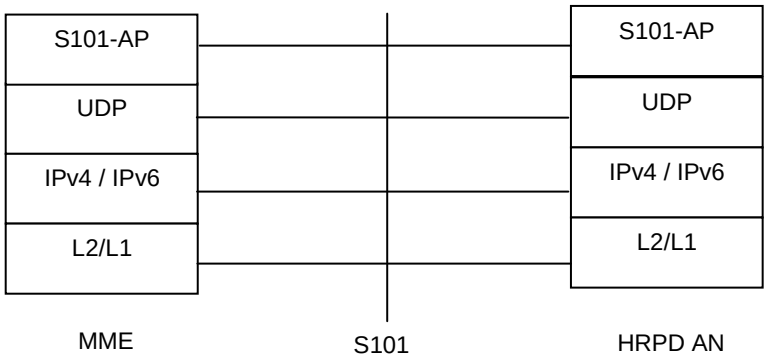
- Messages may carry separate information IEs to indicate status, message types (e.g. handover command) forwarding addresses etc. as required by signalling procedures.

- Provide identifiers (i.e. S101 Session ID) to distinguish messages belonging to different UEs in order to allow responses originating from the target system to an UE to be appropriately forwarded to the UE by the source system.

- Reliable transport for S101 messages should be provided at the application layer and will not require transport layer reliability mechanism.

9.1.2.3 S101 Protocol Stack

The figure below shows the protocol stack for the S101 interface.



Legend:
- S101 Application Protocol (S101-AP): It is the Application Layer Protocol between the MME and HRPD AN
- User Datagram Protocol (UDP): This protocol transfers messages. UDP is defined in RFC 768 [71].
- S101 Application Protocol (S101-AP) provides application layer reliability for its messages, if required.

Figure 9.1.2.3-1: Protocol Stack for the S101 Reference Point

9.1.2.4 S101 Session Identifier

All S101 messages contain a S101 Session ID which serves to identify the UE context at the MME and the HRPD AN. The S101 Session ID uniquely and globally identifies the UE.

9.1.2.5 Requirements for the S103 Reference Point

The S103 interface between the Serving GW and HS-GW supports the forwarding of DL data during mobility from E-UTRAN to HRPD. Signalling procedures on the S101 interface are used to set up tunnels on the S103 interface.

The S103 reference point shall support the following requirements:

- The S103 interface shall support the ability to tunnel traffic on a per-UE, per-PDN basis

- The S103 interface shall support Generic Routing Encapsulation (GRE) RFC 2784 [23] including the Key Field extension RFC 2890 [24]. The Key field value of each GRE packet header uniquely identifies the PDN connectivity that the GRE packet payload is associated with.

9.1.2.6 S103 Protocol Stack

The figure below shows the protocol stack for the S103 interface.

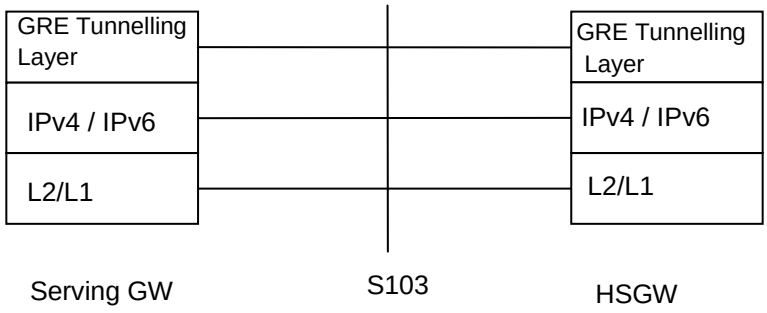


Figure 9.1.2.6-1: Protocol Stack for the S103 Reference Point

Legend:

- On the S103 interface, the tunnelling layer implements GRE encapsulation with the Key Field extension RFC 2784 [23], RFC 2890 [24].

9.2 Overview of Handover Procedures

9.2.1 General

The S101 reference point, and E-UTRAN and HRPD access is used for transparent transfer of pre-registration and handover signalling between the UE and the target access system

The purpose of the procedures is to minimise the total service interruption time experienced at the UE, by allowing the UE to attach and perform service activation (in the case of E-UTRAN) or to perform a session configuration or traffic allocation request (in the case of HRPD) in the target access system before leaving the source access system.

In case where the UE is connected to the E-UTRAN and conditions are such that a handover to HRPD may be required, the source system provides the UE with sufficient information to perform pre-registration with the target HRPD access and core network, over the S101 tunnelling interface. If conditions subsequently warrant that a handover should occur, the handover signalling will also be performed over the S101 tunnelling interface. Once the UE is ready to connect to the target system, it switches to the HRPD access. Alternatively, the E-UTRAN may redirect the UE to HRPD using RRC Connection Release with Redirection Information set as specified in clause 5.3.8 of TS 36.331 [52]. If pre-registration has not been performed successfully, upon receiving the redirection message, the UE acquires the HRPD channel and performs the non-optimized handover according to clause 8.2.2 from step 3 onwards. If pre-registration is successful, upon receiving the redirection message, the UE follows the RRC Connection Release with Redirection procedure to reselect the HRPD cell according to TS 36.331 [52] and then performs the idle-mode optimized handover procedure as specified in clause 9.4 from step 3 onwards.

In case where the UE is connected to the HRPD and conditions are such that a handover to E-UTRAN may be required, the source system provides the UE with sufficient information to perform pre-registration with the target EPS. The pre-registration may be performed over the S101 tunnelling interface. If conditions subsequently warrant that a handover should occur, the handover signalling may also be performed over the S101 tunnelling interface. Once the UE is ready to connect to the target system, it switches to the E-UTRAN access.

9.2.2 Support for HO of IMS Emergency Sessions

In order to support handover from E-UTRAN to HRPD of limited service state UEs, the following additional clarifications apply:

- When a limited service state UE without a UICC or with an unauthenticated IMSI, initiates emergency attach procedures for handover or initial attach to HRPD access to setup emergency sessions, the UE provides its IMEI during the attach procedure. The IMSI, if available, is also provided to the HRPD access by the UE during the attach procedure. If IMSI is not available or IMSI is not authenticated, an IMEI based NAI is used on the S2a interface in this case. Also, authentication with HSS is either skipped or if performed and fails, the HRPD attach procedure is continued.

- In the above scenario, for UEs that supports both E-UTRAN and HRPD access and handover is supported in the network between these accesses, the HRPD access selects a statically configured PDN GW for the UE. This statically configured PDN GW is the same as the statically-configured PDN GW selected for the UE in E-UTRAN access.

- For optimized handover between E-UTRAN and HRPD for Emergency attached UEs in E-UTRAN without an UICC or with an unauthenticated IMSI, IMEI shall be used as the S101 Session ID to identify the UE within the MME and HRPD access nodes. If the IMSI is unauthenticated, the IMSI is provided on the S101 tunnel to the HRPD access with an indication that it is unauthenticated.

NOTE: For optimized handover from E-UTRAN to HRPD the source access system does not release bearers, the management of bearers in HRPD target network is out of the scope of this specification (for example whether HRPD releases non-emergency bearers or not, when the UE is not authorized for service in HRPD).

The procedures for both optimized and non-optimized handovers specified in the other sections in this specification support, without modifications, handover of emergency sessions from E-UTRAN to HRPD access for normal mode UE's, i.e. UEs with IMSI that authenticated successfully.

In this Release of the specification, handover of IMS Emergency Sessions from HRPD access to E-UTRAN access is not supported.

9.3 Optimized Active Handover: E-UTRAN Access to cdma2000 HRPD Access

9.3.0 Introduction

This clause describes the Optimised Handover from E-UTRAN Access to cdma2000 HRPD Access in two phases, pre-registration and the actual handover. In pre-registration phase the UE registers to the cdma2000 HRPD Access, while the UE remains to be connected to the E-UTRAN. The pre-registration may take place well in advance of the need to make the actual handover. In the handover phase, the connection is handed over to cdma2000 HRPD Access, and the UE leaves E-UTRAN.

9.3.1 Pre-registration Phase

Figure 9.3.1-1 illustrates a high-level call flow for the optimised E-UTRAN to HRPD handover procedure, Pre-registration phase.

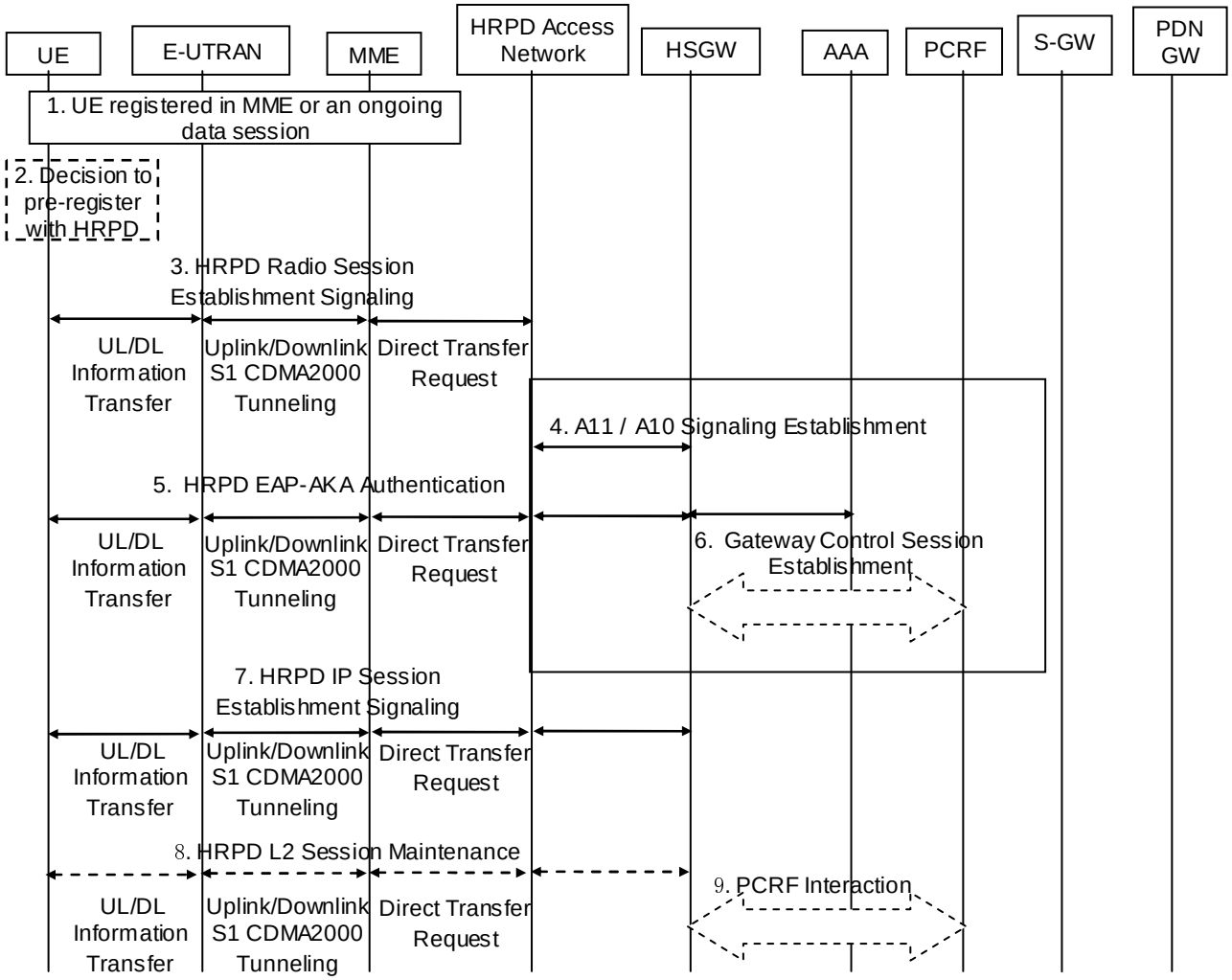


Figure 9.3.1-1: HRPD registration via LTE/SAE tunnel

1. The UE is registered with E-UTRAN/MME. It may have an ongoing data session established over EPS/E-UTRAN access.

2. Based on a Radio Layer trigger (e.g., an indication from the E-UTRAN when the UE is in connected state or an indication over the broadcast channel), the UE decides to initiate a pre-registration procedure with potential target HRPD access. The pre-registration procedure allows the UE to establish and maintain a dormant session in the target HRPD access, while attached to the E-UTRAN/MME.

3. Registration to the HRPD is achieved by exchanging a series of HRPD messages between the UE and the HRPD Access Network. The HRPD signalling that is tunnelled transparently over the E-UTRAN and EPC creates an HRPD session context between the UE and the HRPD Access Network. The procedures described below are used in steps 3, 5, 8 and 9.

   The UE generates an UL Information Transfer message (UL HRPD message). The UL HRPD message is transferred from the UE to the eNodeB as a parameter in the UL Information Transfer.

   The eNodeB sends Uplink S1 CDMA2000 Tunnelling message (UL HRPD message, Sector ID) to the MME. The SectorID is statically configured in the eNodeB.

   The MME selects an HRPD access node address. In order to be able to distinguish S101 signalling transactions belonging to different UEs, an S101 Session ID is used to identify signalling related to that UE on S101. The MME sends a Direct Transfer Request message (S101 Session ID, SectorID, UL HRPD message) to the HRPD access node. The MME determines the correct HRPD access node entity and address from the SectorID.

NOTE 1: There is an unambiguous mapping from the SectorID to the HRPD access node address.

The HRPD Access Network sends signalling in the DL direction to the MME using Direct Transfer Request message (S101 Session ID, DL HRPD message). The S101 Session ID is used to associate the signalling to a particular UE.

The MME sends the information on to the eNodeB using the Downlink S1 CDMA2000 Tunnelling message (DL HRPD message).

The eNodeB uses the DL information transfer message (DL HRPD message) to transport the signalling the UE.

If UE is handing over emergency sessions to HRPD access, the UE informs the HRPD access that it is an emergency handover. In case the UE is in limited service state and does not have an IMSI or its IMSI is unauthenticated, IMEI is used as a Session ID. If the IMSI is unauthenticated, the IMSI is also provided on the S101 tunnel to the HRPD access with an indication that it is unauthenticated.

4. The HRPD Access Network creates a signalling relationship with the HS-GW for the UE with interactions in HRPD network A10 / A11 interfaces.

   If the HRPD Access Node is not configured to support emergency handovers, then it shall reject any handover request that indicates Emergency Handover.

5. The UE, HS-GW, and 3GPP AAA exchange EAP-AKA' signalling to authenticate the UE on the HRPD system. The HS-GW receives the APN(s) and PDN GW identity(es) information from AAA during authentication.

   If the UE is performing an Emergency handover to HRPD access for emergency service and the HRPD access supports Emergency handover, the HPRD access skips the authentication procedure or the HRPD access accepts that the authentication may fail and continues the handover procedure. A statically configured PDN GW is selected by the HRPD access for the UE for unauthenticated UEs.

6. The HS-GW initiates a Gateway Control Session Establishment Procedure with the PCRF as specified in TS 23.203 [19]. If the HS-GW supports UE/NW bearer control mode, the PCRF provides the rules required for the HS-GW to perform the bearer binding for all the active sessions the UE may establish as a result of the handover procedure. For each PDN connection, if the UE has acquired an IPv6 prefix via the 3GPP access, the PCRF returns the IPv6 prefix of UE to the HSGW and the HSGW includes it in the TFT sent to the UE.

7. The UE and HS-GW exchange signalling to establish context to support the bearer traffic environment in use over the E-UTRAN.

8. At any time prior to the Handover Phase, if session maintenance activity is required, the UE or HRPD access network shall perform session maintenance signalling by tunnelling the HRPD session maintenance messages over the S101. If QoS parameters require updating, then this step includes the PCRF interaction. The MME uses the S101 Session ID to identify the UE context over the S101 interface.

NOTE 2: Between Step 7 and Step 8 the UE may enter ECM-IDLE state. To execute the session maintenance procedures at Step 8 it is necessary for the UE to enter ECM-CONNECTED state.

9 PCRF interactions due to session maintenance can be initiated by the PCRF or the HS-GW. The PCRF initiates the Gateway Control and QoS Rules Provision Procedure specified in TS 23.203 [19]. The HS-GW initiates the Gateway Control and QoS Policy Rules Request Procedure as specified in TS 23.203 [19].

9.3.2 Handover Phase

Figure 9.3.2-1 illustrates a high-level call flow for the optimised E-UTRAN to HRPD handover procedure, Handover phase. The prerequisite of the handover phase is the successfully performed Pre-registration phase as it is specified in clause 9.3.1.

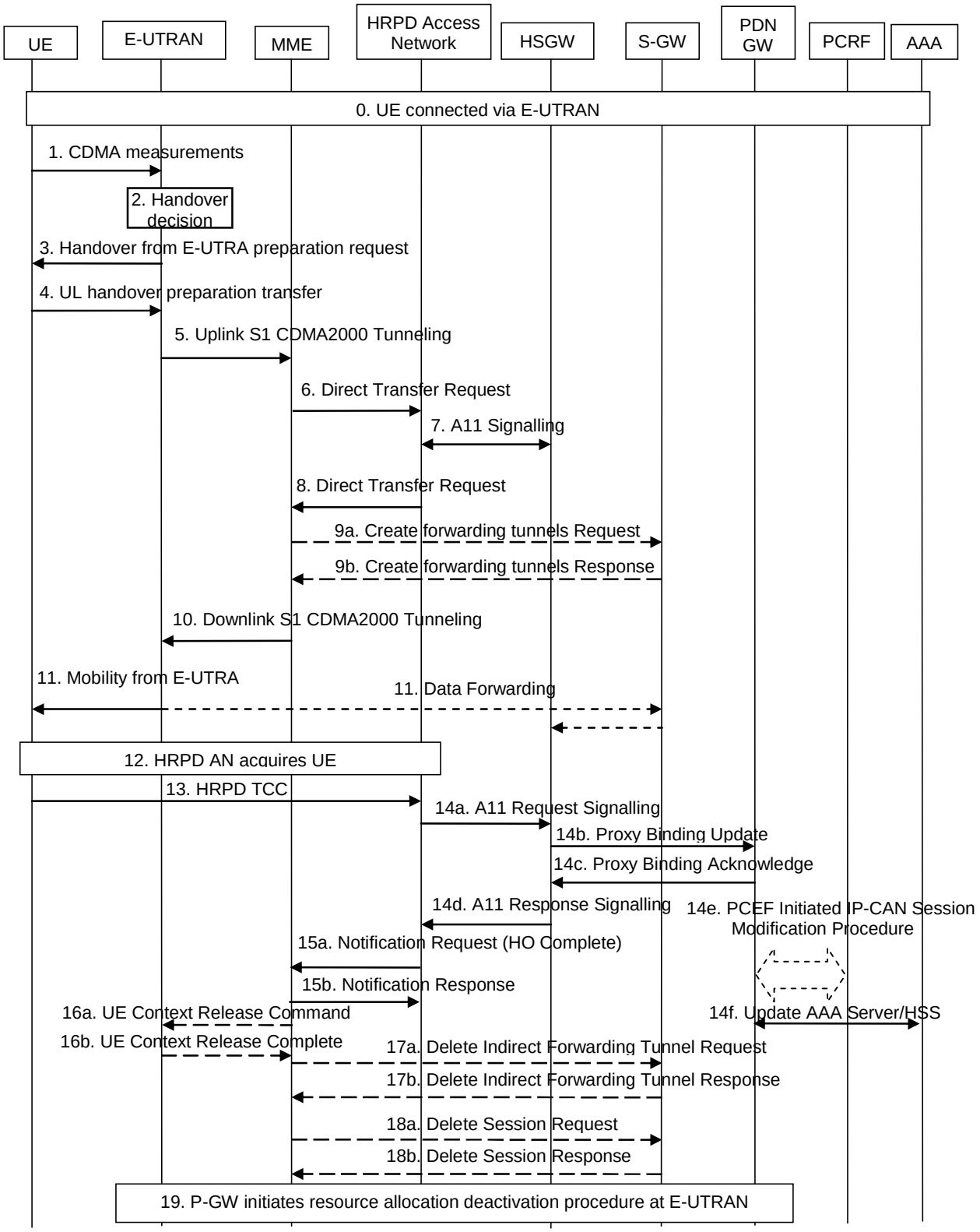


Figure 9.3.2-1: E-UTRAN to HRPD handover

0. Ongoing session established over EPS/E-UTRAN access.

1. The eNodeB receives measurement reports from the UE.

2. The eNodeB makes the handover decision.

3. The handover decision is signalled to the UE with Handover from E-UTRA preparation request message.

4. UE sends an UL handover preparation transfer message (HRPD message starting HO access) to the eNodeB. The HRPD message starting HO access will be carried transparently to the HRPD access node, and its purpose is to request information for accessing an HRPD traffic channel. The message indicates to the eNodeB that the UE is responding to the Handover from E-UTRA preparation request message, and is requesting information for accessing an HRPD traffic channel.

5. The eNodeB sends the Uplink S1 CDMA2000 Tunnelling message (HRPD message starting HO access, and SectorID, CDMA2000 HO Required Indication) to the MME. The SectorID is statically configured in the eNodeB. The eNodeB will also include CDMA2000 HO Required Indication IE to Uplink S1 CDMA2000 Tunnelling message, which indicates to the MME that the handover preparation has started.

6. When receiving Uplink S1 CDMA2000 Tunnelling message with CDMA2000 HO Required Indication the MME determines an HRPD access node address based on the SectorID. An S101 Session ID is used to identify signalling related to that UE on S101. The MME sends a Direct Transfer Request message (S101 Session ID, SectorID, PDN GW Identity(es), GRE key(s) for uplink traffic, APN(s), HRPD message starting HO access) to the HRPD access node.

   When GTP based S5/S8 is used in the EPS, the MME creates the uplink GRE keys from the uplink TEIDs of the default bearers using a standardized algorithm. In this way only one GRE key per PDN connection is created. The PDN GW shall be able to identify any PDN connection based on the GRE key created from the uplink TEID of the default bearer of that PDN connection.

NOTE: When a PDN GW that supports both GTP and PMIP based interfaces allocates a TEID for a GTP tunnel, it also allocates and memorizes a corresponding GRE key if the tunnel is created for a default bearer. Later the PDN GW is able to identify the PDN connection based on the corresponding GRE key, i.e. the PDN GW also assigns the corresponding GRE key to that particular PDN connection and it cannot use that GRE key for any other PDN connection.

7. The HRPD access network allocates the requested radio access resources, and requests a forwarding address from HS-GW. The information sent in the request from the HRPD access network to HS-GW includes APN(s), PDN GW Identity(es) and GRE key(s) for uplink traffic. The response includes the HS-GW Address and GRE key(s) for forwarded traffic on S103. There is one GRE key for each PDN connection for which traffic is to be forwarded.

8. The HRPD access network sends the Direct Transfer Request message (S101 Session ID, HRPD message with HO access information, HS-GW Address and GRE key(s) for forwarded traffic, CDMA2000 HO Status) to the MME. The HS-GW Address and GRE key(s) for forwarded traffic are sent if data forwarding applies. If the HRPD access network did not allocate the resources as requested, this will be indicated to the MME and eNodeB with the CDMA2000 HO Status IE, and the embedded HRPD message indicates the failure to the UE.

9a. If Direct Transfer Request message included HS-GW Address and GRE key(s) for forwarded traffic, the MME determines which of the S1-U bearers should be forwarded to the HRPD and configures resources for indirect data forwarding by sending Create Forwarding Tunnel Request (HS-GW address, GRE key(s) for forwarded traffic, EPS bearer ID(s) subject to forwarding) to the Serving GW.

   The MME shall select the same Serving GW which is used as the anchor point for the UE to perform the data forwarding.

9b. The Serving GW confirms data forwarding resources for S103 and allocates forwarding address for S1 in Create Forwarding Tunnel Response (cause, S-GW address, S1-U uplink TEID(s)). The S1-U uplink TEIDs are provided one per S1-U bearers subject to forwarding.

10. The MME sends the Downlink S1 CDMA2000 Tunnelling message (HRPD message with HO access information, S-GW address, S1-U uplink TEID(s), CDMA2000 HO Status) to the E-UTRAN. If the CDMA2000 HO Status indicates that handover preparation failed, the Downlink S1 CDMA2000 Tunnelling message will be sent with appropriate cause, and the embedded HRPD message that indicates the failure to the UE. The message from the MME provides the eNodeB also with the data forwarding S1-U uplink TEIDs allocated at the Serving GW if data forwarding applies.

11. The E-UTRAN forwards the HRPD message with HO access information to the UE in Mobility from E-UTRA message. This is perceived by the UE as a Handover Command message. If handover preparation failed, DL Information transfer message will be sent instead, with the embedded HRPD message that indicates the failure to the UE.

    If data forwarding applies, the E-UTRAN starts forwarding received downlink data to the S-GW on a per-S1-U bearer forwarding tunnel, which then forwards these packets on a per-PDN per-UE S103 tunnel to the HS-GW. The forwarding starts at the same moment as the Mobility from E-UTRA message is sent to the UE.

12. The UE retunes to the HRPD radio access network and performs traffic channel acquisition.

13. The UE sends an HRPD Traffic Channel Complete (TCC) message to the HRPD access network.

14a-f The E-UTRAN triggers switching the flow in the EPC with the following sequence:

    14a. The HRPD access network sends A11 request signalling to HS-GW to start setting up the U-Plane connection between the HRPD access network and HS-GW.

    14b. The HS-GW sends Proxy Binding Update to PDN GW. The HS-GW sends the all zero IPv4 Home Address (0.0.0.0) or all zero IPv6 Home Prefix (0::/0) in the PBU message. In order to support session continuity, the P-GW performs the Binding Cache entry existence test based on the NAI and assigns the same IPv4 Home Address and/or IPv6 Home Prefix to the UE and acknowledge in the PBA message.

    14c. The PDN GW switches the flow from Serving GW to HS-GW, and sends Proxy Binding Acknowledge to HS-GW, including the Charging ID for the PDN connection.

    14d. The HS-GW responses with A11 response signalling to the HRPD access network.

    14e. The PDN GW executes a PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19] to obtain the rules required for the PDN GW to function as the PCEF for all the active IP sessions the UE has established with new IP-CAN type. Otherwise, information configured with the P-GW may be used to determine policy. Since Steps 14c and 14e are both triggered by the Proxy Binding Update in Step 14b, Steps 14c and 14e may occur in parallel.

    14f. The PDN GW informs the 3GPP AAA Server of its PDN GW identity and the APN corresponding to the UE's PDN Connection and obtains authorization information from the 3GPP AAA Server. The message includes information that identifies the PLMN in which the PDN GW is located. The 3GPP AAA Server may update the information registered in the HSS as described in clause 12.

    For a multiple PDN connection, steps 14b-14c and 14e-14f are performed for each PDN connection.

    Multiple PDN connections to the same APN can be supported using PDN connection identities in the same way as it is specified for S2a procedures.

15a. The HRPD access network sends a Notification Request (HO Complete, S101 session ID) message to the MME (including the S101 session ID to identify the UE context).

15b. The MME responds by sending a Notification Response (S101 session ID) to the HRPD access network.

    If data forwarding was not applied in step 9, the MME shall skip step 17, and shall perform steps 16 and 18.

    If data forwarding was applied in step 9, a timer in MME is started to supervise when the EPS bearer resources in the Serving GW and the temporary resources used for indirect data forwarding in the Serving GW shall be released. The uses of the timer is defined in TS 23.401 [4]. The MME shall perform steps 16, 17 and 18 upon the timer expiry.

    If the EPS bearer resources release is triggered by a Delete Bearer Request message (from step 19) received before the timer expiry, the MME shall stop the timer and skip steps 16, 17 and 18.

16a. The MME releases the UE context in the source E-UTRAN by sending a UE Context Release Command message to the eNodeB.

16b. The source eNodeB releases its bearer resources related to the UE and responds with a UE Context Release Complete message.

17a. The MME sends a Delete Indirect Data Forwarding Tunnel Request message to the Serving GW.

17b. The Serving GW releases the temporary resources used for indirect data forwarding which were allocated at step 9. The Serving GW acknowledges with Delete Indirect Data Forwarding Tunnel Response message.

18a. The MME releases the EPS bearer resources in the Serving GW by sending a Delete Session Request message to the Serving GW. The MME shall indicate to the Serving GW that the Serving GW shall not initiate a delete procedure towards the PDN GW.

18b. The Serving GW acknowledges resource removal with Delete Session Response (Cause) message.

19. At any time after step 14c, the PDN GW shall initiate the PDN GW Initiated PDN Disconnection procedure at E-UTRAN as defined in clause 5.6.2.2 or the PDN GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [4], clause 5.4.4.1. If data forwarding was applied, the forwarding tunnel established in step 9 shall be also released in this step.

9.4 Optimized Idle-mode Mobility: E-UTRAN Access to cdma2000 HRPD Access

This procedure is used in the case the UE has a dormant HRPD session in the target HRPD network, either through the pre-registration procedure or previous HRPD attachment.

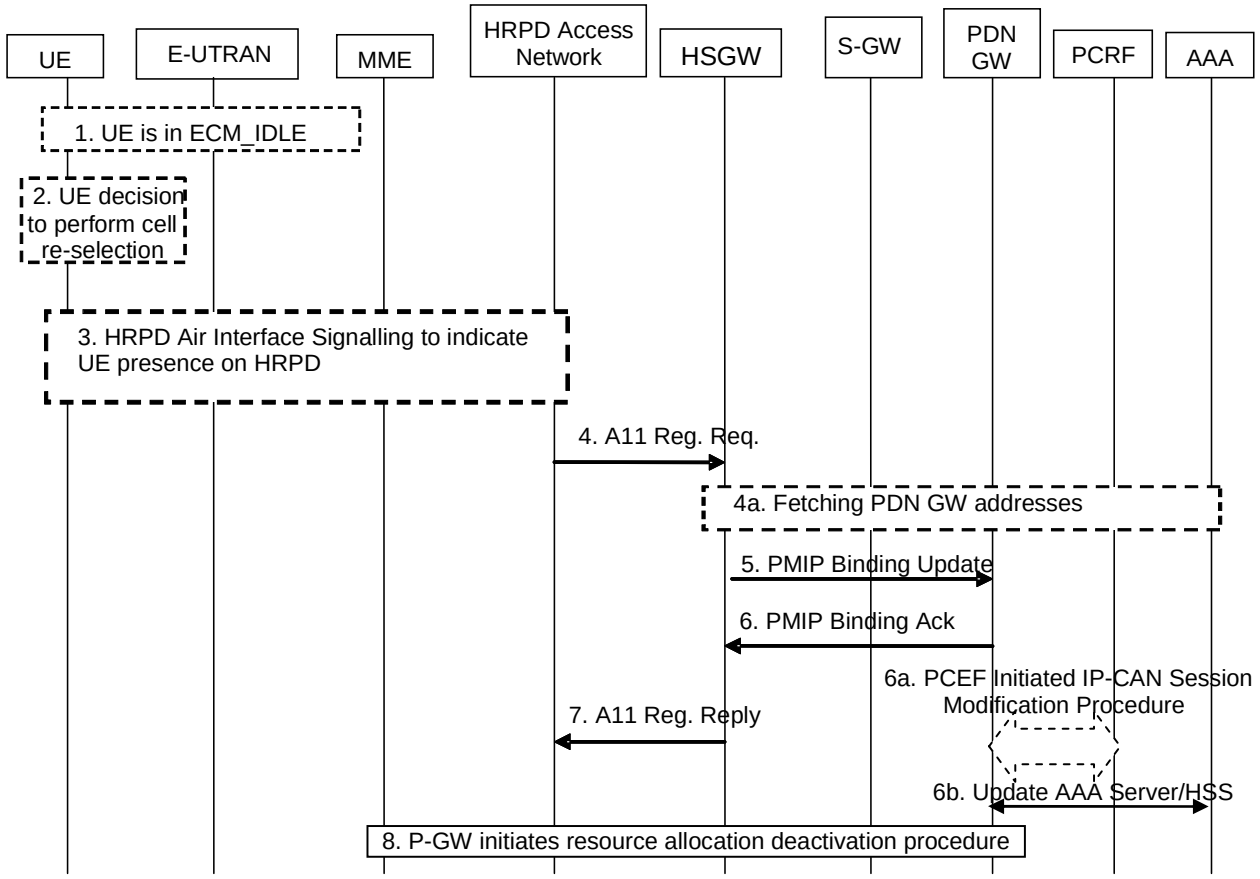


Figure 9.4-1: E-UTRAN to HRPD mobility in idle-mode

1. The UE is attached to E-UTRAN network and stay in ECM_IDLE state. The UE has a dormant HRPD session in the target HRPD network, either through the pre-registration procedure or previous HRPD attachment

2. The UE is in idle mode. Based on some trigger, the idle UE decides to perform cell re-selection to the HRPD system. Note, the cell re-selection decision can be made at any time when the UE is attached in the E-UTRAN network (including as soon as the UE has completed pre-registration).

3. The UE follows 3GPP2 procedures in [49] to inform the HRPD access network the UE has performed an inter-technology idle mode mobility event and is now tuned to HRPD.

4. The HRPD access indicates to the HSGW that the UE has moved to HRPD.

4a. The HS-GW fetches the PDN GW identity for all the active PDN connections from the 3GPP AAA Server.

5~6. The HS-GW exchanges a PMIP BU/BA with the PDN GW. The UE address information in PMIP BA returns the IP Address assigned to the UE. In this message, the Charging ID is also carried for charging correlation purposes. At this point the user plane is switched in the PDN GW towards the HRPD access network via the HS-GW. Multiple PDN connections to the same APN can be supported using PDN connection identities in the same way as it is specified for S2a procedures.

6a. The PDN GW executes a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19] to obtain any new QoS policy and charging rules for all the active sessions as a result of the handover procedure. Since steps 6 and 6a are both triggered by the Proxy Binding Update in step 5, steps 6 and 6a may occur in parallel.

6b. The PDN GW informs the 3GPP AAA Server of its PDN GW identity and the APN corresponding to the UE's PDN Connection and obtains authorization information from the 3GPP AAA Server. The message includes information that identifies the PLMN in which the PDN GW is located. The 3GPP AAA Server may update the information registered in the HSS as described in clause 12.

For multiple PDN connections, steps 5-6 and 6a-6b are performed for each PDN connection.

7. The HS-GW acknowledges the HRPD access network.

8. At any time after step 6, the P-GW shall initiate the PDN GW Initiated PDN Disconnection procedure as defined in clause 5.6.2.2, so that any resources are released in the EPS serving nodes that were serving the UE in E-UTRAN access before the idle-mode mobility to HRPD took place.

9.5 Void

9.5.1 Void

9.5.2 Void

9.6 Void

9.7 S101 Tunnel Redirection Procedure

S101 Tunnel Redirection Procedure is used when the UE performs TAU with MME change while the UE has already triggered a pre-registration procedure from LTE to the HRPD as described in clause 9.3.1 and the S101 session exists between the MME and the HRPD Access Network.

The detail procedure for the idle case is depicted as figure 9.7-1.

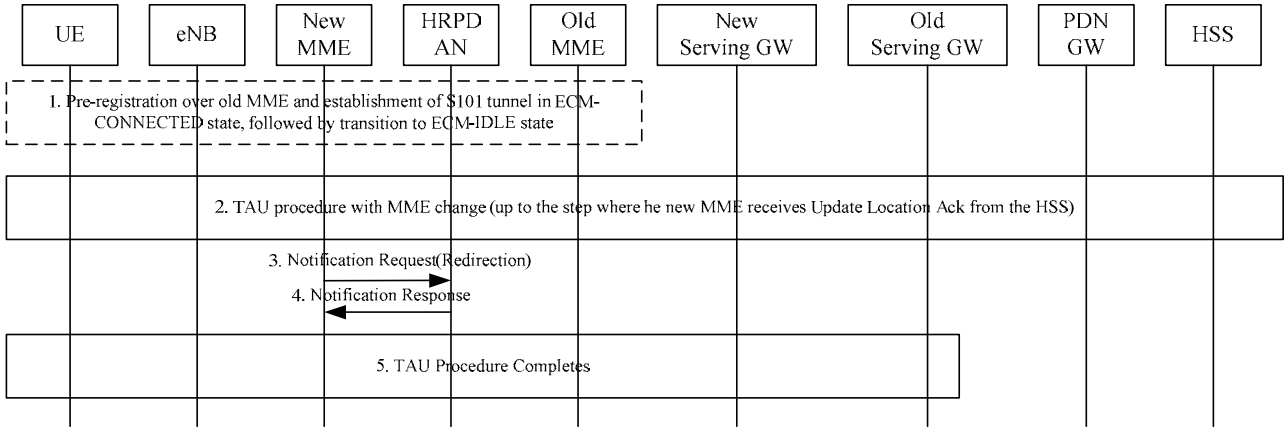


Figure 9.7-1: S101 tunnel redirection during TAU with MME change

1. UE performs pre-registration over the old MME while in ECM-CONNECTED state, followed by transition to ECM-IDLE state. The S101 tunnel exists between the old MME and the HRPD Access Network.
2. TAU procedure with MME change is executed as described in TS 23.401 [4], figure 5.3.3.1-1, up to the step where the new MME receives Update Location Ack from the HSS. The HRPD Access Network IP address is transferred to the new MME via the Context Response message.
3. The new MME sends Notification Request (Redirection, S101 Session ID) message to the HRPD Access Network. After receiving this message, the HRPD Access Network associates the S101 tunnel for this specific UE with the new MME. Then the HRPD Access Network releases any context associated with the old MME.
4. In response to the Notification Request message, the HRPD Access Network sends a Notification Response (S101 Session ID) message to the target MME.
5. The TAU procedure is completed.

The detailed procedure for the active case is depicted as figure 9.7-2.

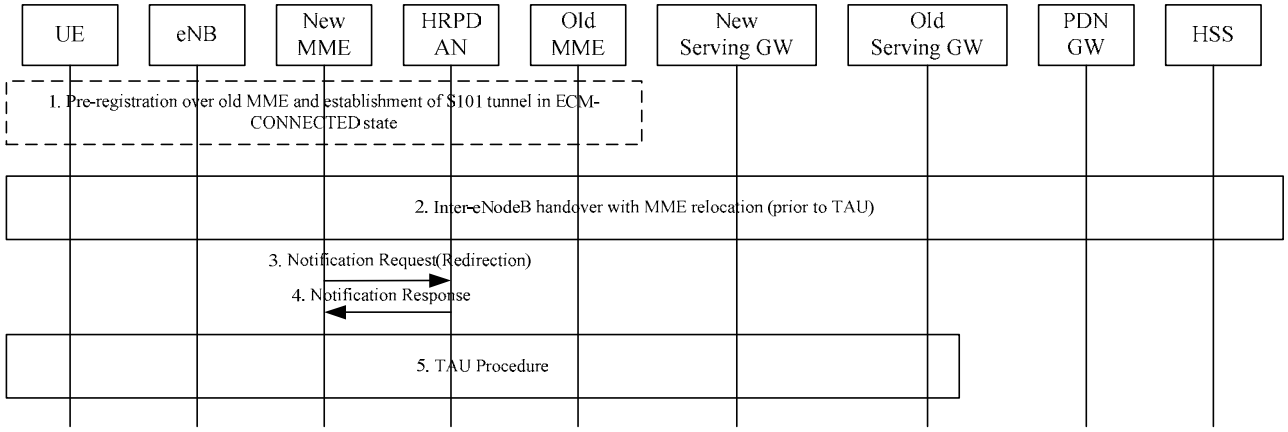


Figure 9.7-2: S101 tunnel redirection during inter-eNodeB handover with MME relocation

1. UE performs pre-registration over the old MME while in ECM-CONNECTED state. The S101 tunnel exists between the old MME and the HRPD Access Network.
2. Inter-eNodeB handover with MME relocation procedure is executed as described in TS 23.401 [4], figure 5.5.1.2.2-1, steps up to TAU. The HRPD Access Network IP address is transferred to the new MME via the Forward Relocation Request message.
3. The new MME sends Notification Request (Redirection, S101 Session ID) message to the HRPD Access Network. After receiving this message, the HRPD Access Network associates the S101 tunnel with the new MME. Then the HRPD Access Network releases any context associated with the old MME.

4. In response to the Notification Request message, the HRPD Access Network sends a Notification Response (S101 Session ID) message to the target MME.

5. The TAU procedure occurs.

10 Handovers with Optimizations Between 3GPP Accesses and Mobile WiMAX

10.1 Optimizations for network-controlled dual radio handover

10.1.1 General Principles

The solution for network-controlled dual radio handover between 3GPP accesses (GERAN, UTRAN, E-UTRAN) and Mobile WiMAX is based on the concepts of clause 4.1.2 In addition, the following principles apply when the ANDSF functionality is supported by the network and by the UE:

1) The EPS shall support mechanisms for delivery of inter-system mobility policies and access network discovery information over the S14 interface, as described in clause 4.8.

2) The inter-system mobility policies shall contain operator-defined rules and preferences that help the UE:

   (i) determine when mobility between mobile WiMAX and 3GPP accesses is restricted or allowed; and

   (ii) determine when a 3GPP or mobile WiMAX access is more preferable than the currently used radio access.

3) The access network discovery information shall contain information about mobile WiMAX access networks that are available in the vicinity of the UE, if the UE's location is known and if such information is available in the network and allowed by the operator.

4) If a UE discovers a neighbour mobile WiMAX access and determines (based on the inter-system mobility policies and user preferences) that:

   (i) the discovered mobile WiMAX access is more preferable to the currently used 3GPP access; and

   (ii) mobility from 3GPP access to mobile WiMAX access is allowed, then the UE shall attempt to handover to the discovered mobile WiMAX access;

   according to the S2a/S2c procedures described in clause 8.

5) If a UE discovers one or more neighbour 3GPP accesses and determines (based on the inter-system mobility policies and user preferences) that:

   (i) 3GPP access is more preferable to mobile WiMAX access; and

   (ii) mobility from mobile WiMAX access to 3GPP access is allowed, then the UE shall select a neighbour 3GPP access (e.g. based on 3GPP access selection rules) and shall attempt to handover to the selected 3GPP access;

   according to procedures described in clause 8.

11 Handover Optimizations Applicable to All Non-3GPP Accesses

<This clause describes handover optimization procedures that are generic and applicable to all non-3GPP accesses.>

12 Interactions Between HSS and AAA Server

12.0 General

The interaction between the 3GPP AAA Server and the HSS is not explicitly presented in several figures of this specification. Though these entities are depicted as "AAA/HSS" in these figures, these functions are distinct and interact over the SWx reference point.

12.1 Location Management Procedures

The location management procedures between HSS and 3GPP AAA Server is described in this clause.

Non-3GPP access location management procedures define the process in which the 3GPP AAA Server interacts with the HSS for the following purposes:

- To register the current 3GPP AAA Server address in the HSS for a given 3GPP user. This procedure is invoked by the 3GPP AAA Server after a new subscriber has been authenticated by the 3GPP AAA Server (either at attach and handover). As part of the response, the HSS returns the subscriber's user profile data (QoS profile, user capabilities, etc.) to the 3GPP AAA Server.

- To register the current PDN GW identity and its association with the UE and APN in the HSS for a given user. This information is provided by the AAA Server to the HSS at attachment to a particular PDN via non-3GPP access.

- To acquire the PDN GW identity for each of the already allocated PDN Gateway(s) with the corresponding PDN information from the HSS over the SWx reference point for a given UE. This is for the case when the UE has already been assigned PDN Gateway(s) due to a previous attach in a 3GPP access (when the UE is handed over from a 3GPP access to a non-3GPP access).

- To de-register the currently registered 3GPP AAA Server-address in the HSS for a given user and purge any related non-3GPP user status data in the HSS. The 3GPP AAA Server de-registers its address and purges user status data when e.g. the UE has disappeared from non-3GPP access coverage, when another EPC core network entity (e.g. charging system) has initiated a disconnection, when a re-authentication failure in the 3GPP AAA Server occurs, etc. If a UE has changed to a 3GPP access RAT, the 3GPP AAA Server initiated De-Registration procedure should not affect any currently selected PDN GW identity and APN associated with the UE's PDN Connection stored in the HSS and in use in the 3GPP access.

- HSS-initiated de-registration procedure to purge the UE from the 3GPP AAA server. This happens when the user's subscription has been cancelled or other operator-determined reasons. As a result, the 3GPP AAA server should deactivate any UE tunnel in the PDN GW and/or detach the UE from the access network.

The previous procedures are described in more detail in the following clauses. These procedures between the 3GPP AAA Server and the HSS are common to all non-3GPP accesses, whether trusted or non-trusted, and are independent of the mobility protocol used.

12.1.1 UE Registration Notification

After a UE has successfully been authenticated and authorised by the 3GPP AAA Server to make use of a given non-3GPP access (over SWa/STa), ePDG (over SWm) or PDN GW (over S6b for S2c), the 3GPP AAA Server registers its address to the HSS, unless already done. In turn, the HSS should store the address of the registered 3GPP AAA server for the given user and mark the user as registered in the 3GPP AAA Server. In the response, the HSS returns user profile data.

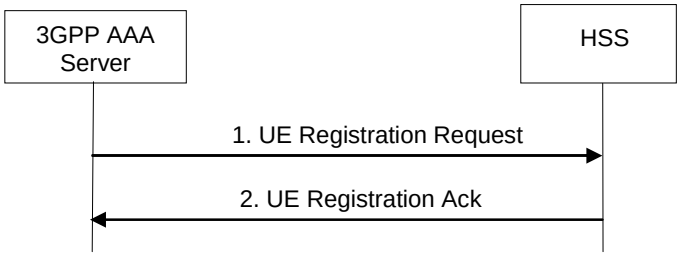


Figure 12.1.1-1: UE Registration Notification

1. Once the UE has been successfully authenticated by the 3GPP AAA server, the 3GPP AAA Server sends a UE Registration Request (User Identity, Mobile Equipment Identity, 3GPP AAA Server address) to the HSS.

2. The HSS checks that the user is known and that the stored 3GPP AAA Server address is the same one stored for the user and that it is the same 3GPP AAA Server that previously requested authentication vectors for this same user. If this is successful, the HSS marks the 3GPP AAA Server as the registered 3GPP AAA Server for user. The HSS responds with a UE Registration Ack (User Identity, Subscription Data). The subscription data includes information to be used by the PDN GW selection function or an already selected PDN GW identity and APN if present.

12.1.2 AAA-initiated UE De-registration Notification

The 3GPP AAA Server requests the HSS to De-Register the currently registered UE. In doing so, the 3GPP AAA Server is notifying the HSS that the UE no longer has any context in the 3GPP AAA Server. The HSS should in turn delete the registered 3GPP AAA Server address.

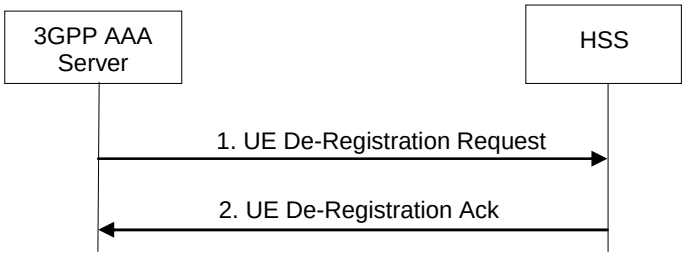


Figure 12.1.2-1: AAA-initiated UE De-registration Notification

1. The 3GPP AAA Server sends a UE De-Registration Request (User Identity, Cause) to the HSS. The "Cause" field may take values such as Authentication-Failure, UE-Detached, Charging-System-Request, etc.

2. The HSS marks the UE as not-registered, removes the 3GPP AAA Server address previously stored for the UE and responds with a UE De-Registration Ack.

12.1.3 HSS-initiated UE De-registration Notification

The HSS requests the 3GPP AAA Server to de-register a UE, for instance, when a subscription is withdrawn or other operator determined reasons. The 3GPP AAA Server should purge user data, set the user to not-registered and detach the UE and/or deactivate any network resources allocated to the user.

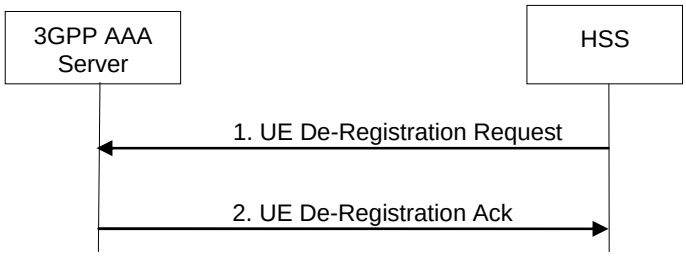


Figure 12.1.3-1: HSS-initiated UE De-registration Notification

1. The HSS server sends a UE De-Registration Request (User Identity, Cause) to the 3GPP AAA Server. The "Cause" field may take values such as Subscription Withdrawn, Administrative-Reason, etc.

2. The 3GPP AAA Server marks the user as not-registered and purges any user data. It responds with a UE De-Registration Ack. In addition, the 3GPP AAA Server should initiate detach of the UE or de-activation of any network resources.

12.1.4 PDN GW Identity Notification from AAA Server

The 3GPP AAA Server updates the HSS with the PDN GW identity of the selected PDN GW and the APN associated with the UE's PDN Connection. This procedure only occurs when the 3GPP AAA Server has in turn successfully received the PDN GW identity and APN from the PDN GW the UE is attached to. The 3GPP AAA server should subsequently always update the HSS with the PDN GW identity in the above-mentioned manner. This procedure is used for PDN GW registration.

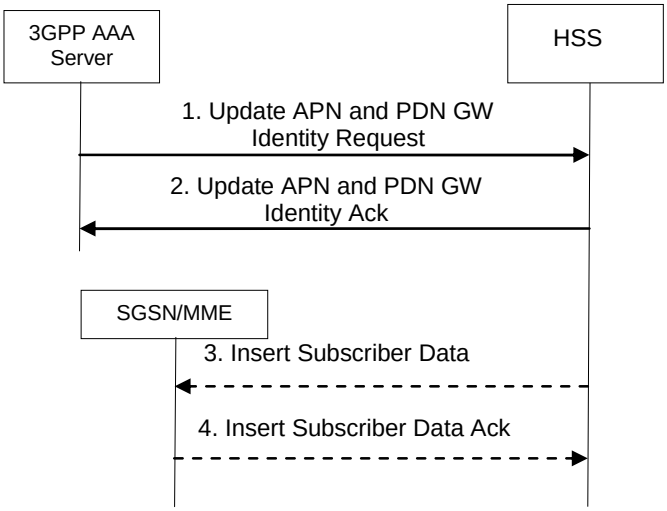


Figure 12.1.4-1: PDN GW Address Notification

1. The 3GPP AAA Server sends a Update PDN GW Identity Request (PDN GW Identity, APN, User Identity) to the HSS.

   The PDN GW identity is either the IP address (e.g. if the PDN GW has a single IP address for all the mobility protocols it supports or if it only supports one mobility protocol) or the FQDN (e.g. if the PDN GW has multiple IP addresses for the mobility protocols it supports).

2. The HSS checks that the user is known and that the stored 3GPP AAA Server name is the currently registered 3GPP AAA server for this same user. If this is successful, the HSS returns a Update PDN GW Identity Acknowledgement.

3. Steps 3-4 are only performed if the PDN GW identity information was successfully modified in the HSS and an SGSN or MME is registered in the HSS for the same UE. In this case the HSS sends an Insert Subscriber Data message to the SGSN or MME to update the change in the SGSN or MME. If both an SGSN and an MME is registered in the HSS, and Insert Subscriber Data message is sent to each of them.

4. The SGSN or MME acknowledges by sending an Insert Subscriber Data Ack message.

12.1.5 PDN GW Identity Notification from MME/SGSN

In case of initial attach, or UE requested PDN connectivity, in the 3GPP access, the SGSN/MME updates the HSS with the PDN GW identity of the selected PDN GW and the APN associated with the UE's PDN connection. If a 3GPP AAA Server is registered in the HSS for the same UE, the HSS provides the updated APN and PDN GW identity information to the 3GPP AAA Server. If NBM is used for establishing connectivity in the non-3GPP access, the 3GPP AAA Server notifies the changes to the non-3GPP access network. This procedure is used for PDN GW registration.

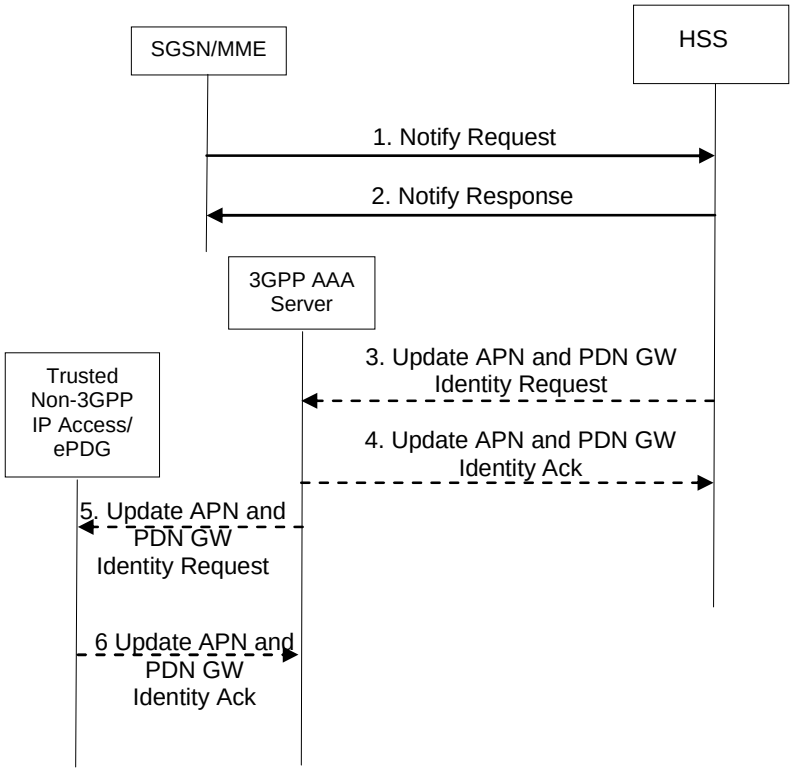


Figure 12.1.5-1: PDN GW address notification from SGSN/MME

1. The SGSN/MME sends a Notify Request (PDN GW Identity, APN, User Identity) to the HSS.

2. The HSS checks that the user is known and that the stored SGSN/MME is the currently registered SGSN/MME for this same user. If this is successful, the HSS returns a Notify Response.

3. Steps 3-4 are only performed if the PDN GW identity information was successfully modified in the HSS and a 3GPP AAA Server is registered in the HSS for the same UE. In this case the HSS sends Update APN and PDN GW Identity Request message to the 3GPP AAA Server.

4. The 3GPP AAA Server acknowledges by sending a Update APN and PDN GW Identity Ack message.

5. If NBM is used for establishing connectivity in the non-3GPP IP access, the 3GPP AAA Server updates the ePDG/trusted non-3GPP IP access network with the new APN and PGW Identity data by sending Update APN and PDN GW Identity message.

6. The ePDG/trusted non-3GPP IP access network acknowledges by sending Update APN and PDN GW Identity Ack message.

12.2 Subscriber Profile Management Procedures

The subscriber profile management procedures between HSS and 3GPP AAA Server is described in this clause.

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 of user profile data in the HSS.

The 3GPP AAA Server may also request the user profile data from the HSS. This procedure is invoked when for some reason the subscription profile of a subscriber is lost or needs to be updated.

12.2.1 HSS-initiated User Profile Update Procedure

The HSS may send a User Profile Update request to the 3GPP AAA Server whenever the subscriber profile in the HSS is modified since it was previously sent to the 3GPP AAA Server. The User Profile Update procedure is depicted in the following figure.

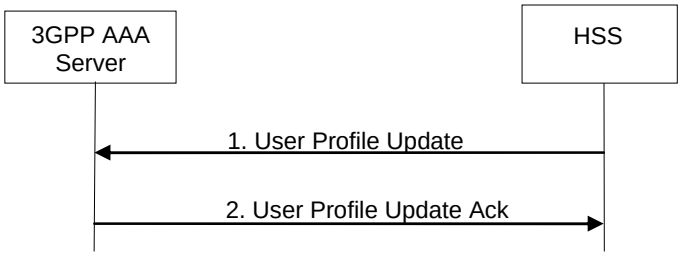


Figure 12.2.1-1: HSS-initiated User Profile Update Procedure

1. The HSS sends a User Profile Update (User Identity, Subscription Data) message to the 3GPP AAA Server. If the HSS is aware of the non-3GPP access type it may return only the subscription data that affects the non-3GPP access.

2. The 3GPP AAA Server updates its subscription data and acknowledges the User Profile Update message by returning a User Profile Update Ack (User Identity) message. As a result, the 3GPP AAA Server may need to update the non-3GPP access network and the PDN GW with new authorisation data, new service authorisation data and new subscribed QoS data.

12.2.2 AAA-initiated Provide User Profile Procedure

The 3GPP AAA Server may send a Provide User Profile request to the HSS when the user subscription profile of a subscriber is lost or is corrupt or for any other reason.

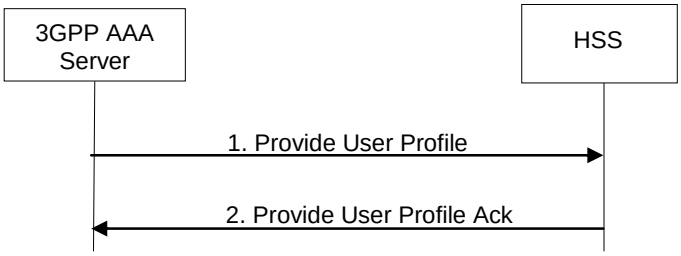


Figure 12.2.2-1: AAA-initiated Provide User Profile Procedure

1. The 3GPP AAA Server sends a Provide User Profile (User Identity) to the HSS.

2. The HSS checks that the user is known and that the stored 3GPP AAA Server address is the same one stored for the user and that it is the same server that previously requested authentication of the same user. If this is successful, the HSS returns a Provide User Profile Ack (user identity, subscription data). If the HSS is aware of the non-3GPP access type it may return only the subscription data that affects the non-3GPP access.

12.3 Authentication Procedures

The authentication procedures between HSS and 3GPP AAA Server are described in TS 33.402 [45].

The authentication procedures define the process in which the 3GPP AAA Server interacts with the HSS to acquire necessary data (i.e. Authentication Vectors for EAP-AKA or EAP-AKA') from the HSS to successfully authenticate the user for accessing the non-3GPP system.

13 Information Storage

13.0 General

This clause describes the additional information stored in different nodes while the UE is in non-3GPP access.

The information provided in clauses 13.1, 13.2 and 13.3 is incomplete in this Release of the specification and intended only for information. Detailed information is available in corresponding stage 3 specifications.

13.1 HSS

The data held in the HSS when non 3GPP accesses are not used is defined in TS 23.401 [4].

The additional data held in the HSS when non 3GPP accesses are used is defined in table 13.1-1 below.

Table 13.1-1: HSS EPS Data (additional aspects for non 3GPP accesses)

Field	Description
3GPP AAA Server name	The Identity of the 3GPP AAA Server serving the UE currently.
QoS profile per access	The quality of service profile subscribed for a particular access for a specific APN
ODB	Indicates that the status of the operator determined barring for a specific access.
Access Restriction	Indicates the access restriction subscription information.

13.2 MME

Information storage for the MME is described in TS 23.401 [4]. The additional data held in the MME when optimized interworking with CDMA2000 HRPD is used is defined in table 13.2-1 below.

Table 13.2-1: MME storage requirements to support optimized interworking with CDMA2000 HRPD

Field	Description
S101 HRPD access node IP address	The IP address of the HRPD AN used for the S101 tunnel for a UE. This is stored on a per UE basis.
S103 Forwarding Address	HS GW IP address used for data forwarding to the HRPD access over S103 interface. This is stored on a per UE basis.
S103 GRE key(s)	GRE Key(s) used for the data forwarding tunnel to the HS GW - one per PDN connection. This is stored on a per PDN connection basis.

13.3 S-GW

Information storage for the S-GW is described in TS 23.401 [4]. The additional data held in the S-GW when optimized interworking with CDMA2000 HRPD is used is defined in table 13.3-1 below.

Table 13.3-1: S-GW storage requirements to support optimized interworking with CDMA2000 HRPD

Field	Description
S103 Forwarding Address	HS-GW IP address used for data forwarding to the HRPD access over S103 interface. This is stored on a per UE basis.
S103 GRE key(s)	GRE Key(s) used for the data forwarding tunnel to the HS-GW - one per PDN connection. This is stored on a per PDN connection basis.

13.4 Handling of Wild Card APN

When the wild card APN is present in the subscription context, the UE is authorized to connect to APNs which are not present in the subscription context.

When a request is received for registering a PDN GW ID for such an active APN which is not present in the subscription context, the nodes (HSS/MME/ S4 SGSN/AAA Server/Non-3GPP access) shall store the PDN GW ID and the APN for the UE.

When a request is received for deregistering of PDN GW ID, for such an active APN which is not present in the subscription context, the nodes (HSS/MME/ S4 SGSN/AAA Server/Non-3GPP access) shall delete the PDN GW ID and the APN for the UE.

14 Void

15 Functional Description and Procedures for 3GPP Accesses with S2c

15.1 S2c Bootstrapping via DSMIPv6 Home Link

When connected over the UE home link (i.e. 3GPP access as defined in clause 4.1), the UE may trigger the establishment of S2c IKEv2 SA, e.g. to optimize future handovers to non-3GPP accesses using S2c. For each PDN connection, the S2c IKEv2 SA establishment has to be performed separately.

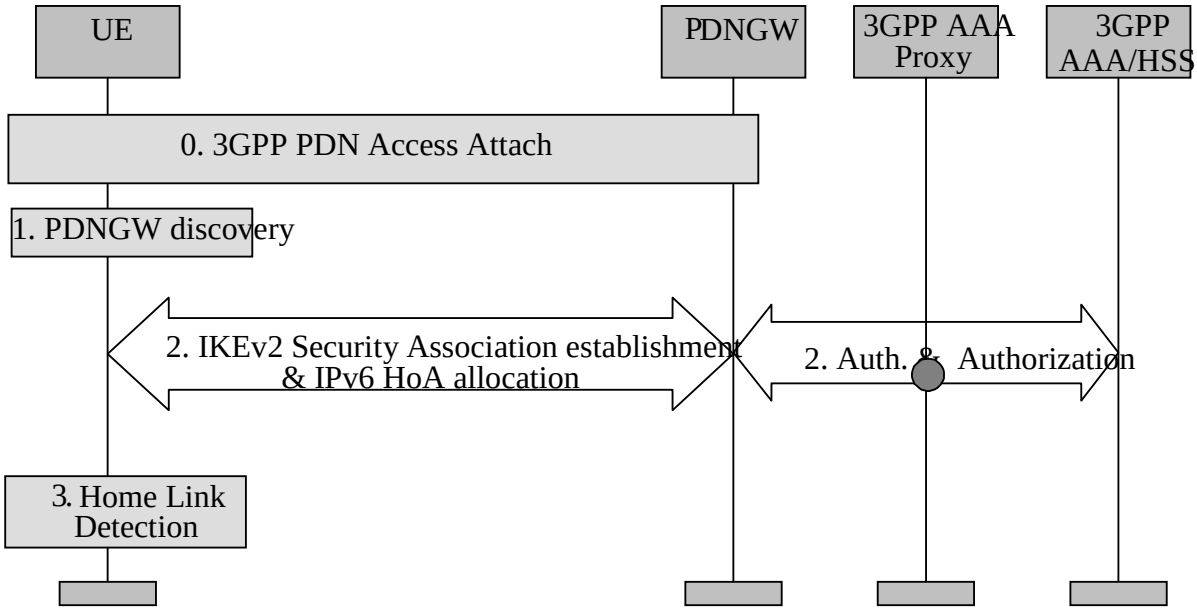


Figure 15.1-1: S2c PDN Attach via DSMIPv6 home link

0. In this procedure it is assumed that UE is already attached to the PDN over the 3GPP access system as defined in TS 23.401 [4]. This step, according to TS 23.401 [4] could be an initial attach to a default PDN or a UE initiated subsequent attach to another PDN.

1. The UE discovers the PDN GW providing access to the PDN it connected to in Step 0, as defined in the clause 4.5.2. To ensure reachability of the PDN GW, signalling associated with this step as well as step 2 below, should be performed over the connection established by step 0 above.

2. A security association is established between the UE and PDN GW to secure the DSMIPv6 messages related to this PDN connection between the UE and the PDN GW.

   The UE initiates the establishment of the security association using IKEv2 [9]; EAP [11] is used over IKEv2 for authentication purposes. The PDN GW communicates with the AAA infrastructure in order to complete the authentication.

   During this step an IPv6 home prefix is assigned by the PDN GW to the UE as defined in RFC 4877 [22]. During this step the UE shall include the IPv6 Home Address and may include the APN of the PDN it wants to access. The PDN GW address and APN associated with the UE's PDN Connectivity are registered by the AAA server with the HSS as described in clause 12.

   In this step, the PDN GW may be either in the HPLMN or in the VPLMN. When the PDN GW is in the VPLMN, the interaction between the PDN GW in the VPLMN with the AAA/HSS in the HPLMN may involve a 3GPP AAA Proxy in the VPLMN.

3. UE confirms that it is located in its DSMIPv6 home link for the given PDN, as described for DSMIPv6 Home Link Detection Function in clause 4.5.6.

   In some cases this procedure may result in a PDN GW that is different than the one the UE is connected to in step 0. In this case the PDN GW reallocation procedure defined in clause 6.10 is applied.

16 Architecture, Functional description and Procedures for GTP and PMIPv6 based S2a over Trusted WLAN Access

16.1 Architecture and Functional Description

16.1.1 Architecture

When the WLAN is considered as trusted by the operator, the Trusted WLAN Access Network (TWAN) is interfaced with the EPC as a trusted non-3GPP access via the STa interface to the 3GPP AAA Server/Proxy and the S2a interface to the PDN GW.

Roaming scenarios where the TWAN does not support a STa interface to the UE's registered PLMN or to the UE's HPLMN are not supported in this release of the specification.

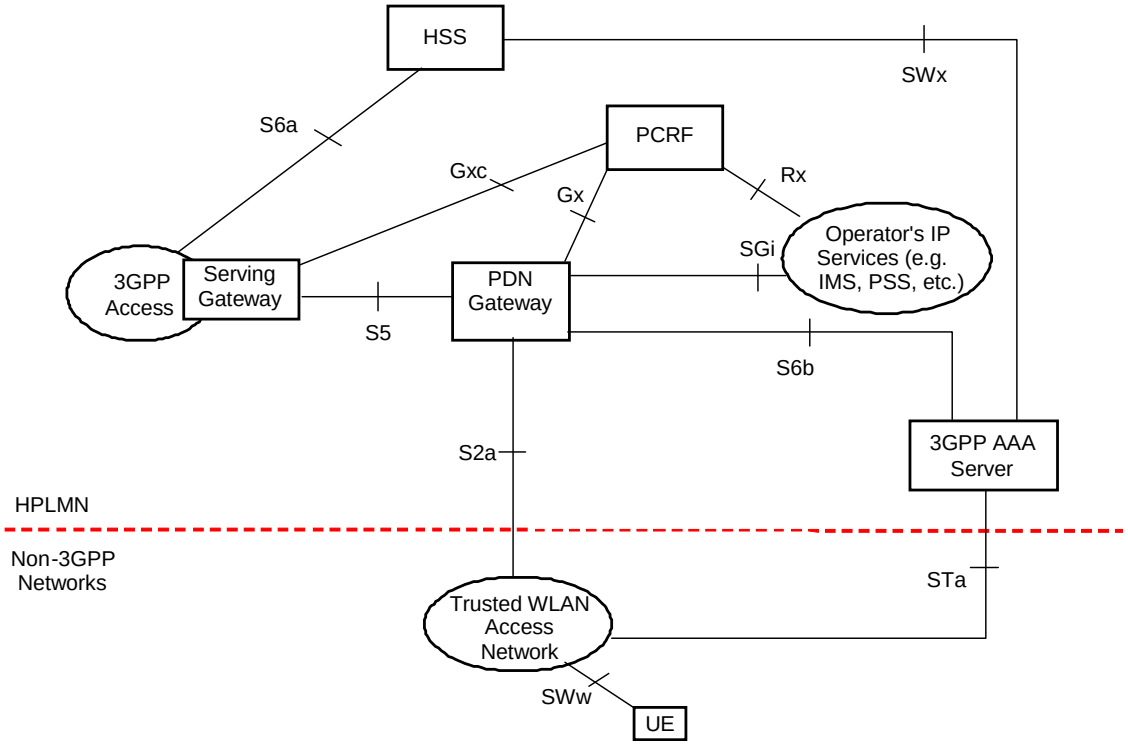


Figure 16.1.1-1: Non-roaming architecture for Trusted WLAN access to EPC

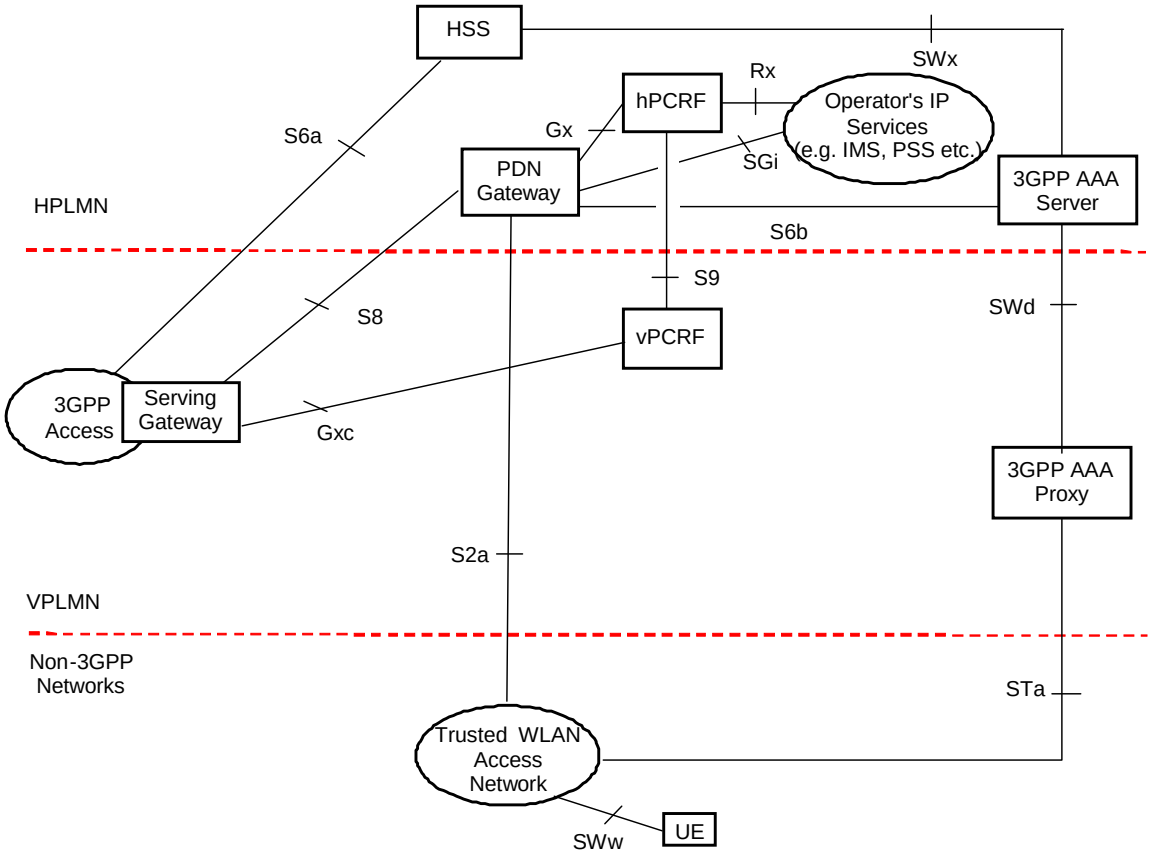


Figure 16.1.1-2: Roaming architecture for Trusted WLAN access to EPC - Home Routed, VPLMN provides WLAN service

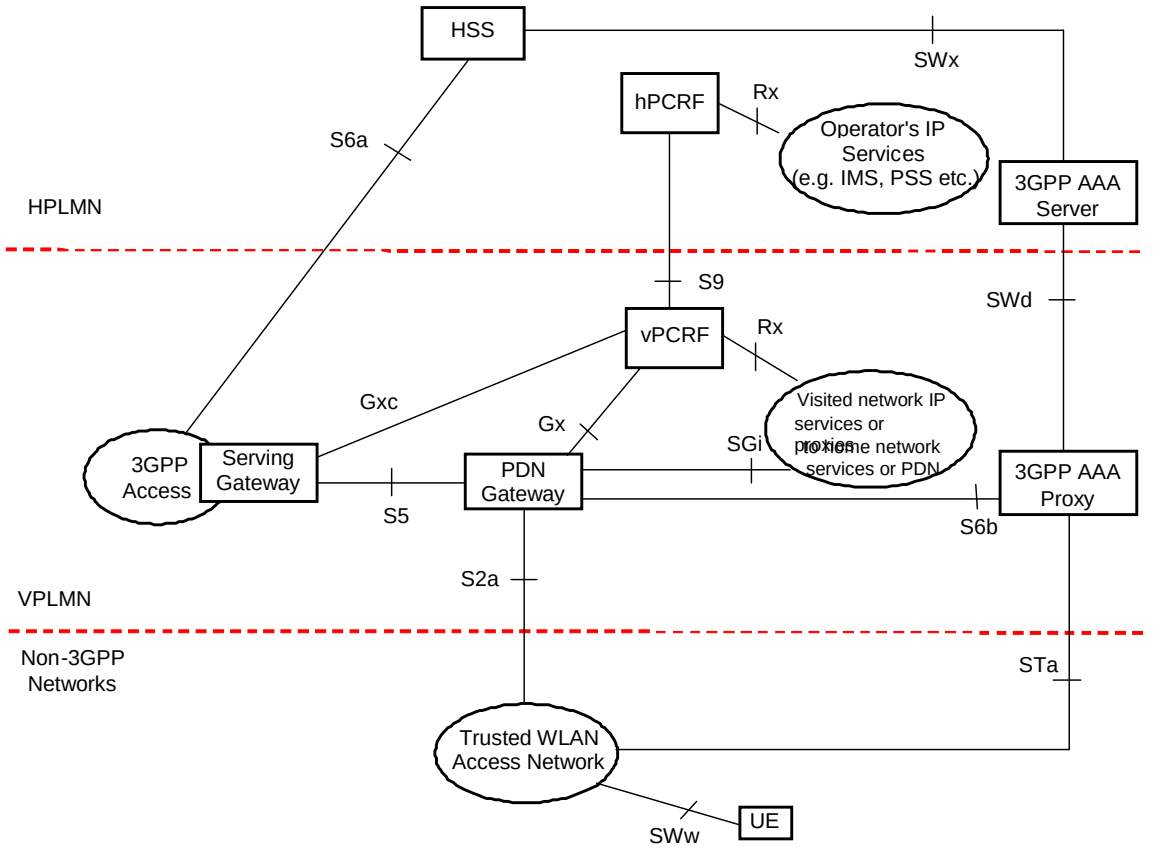


Figure 16.1.1-3: Roaming architecture for Trusted WLAN access to EPC - Local break-out

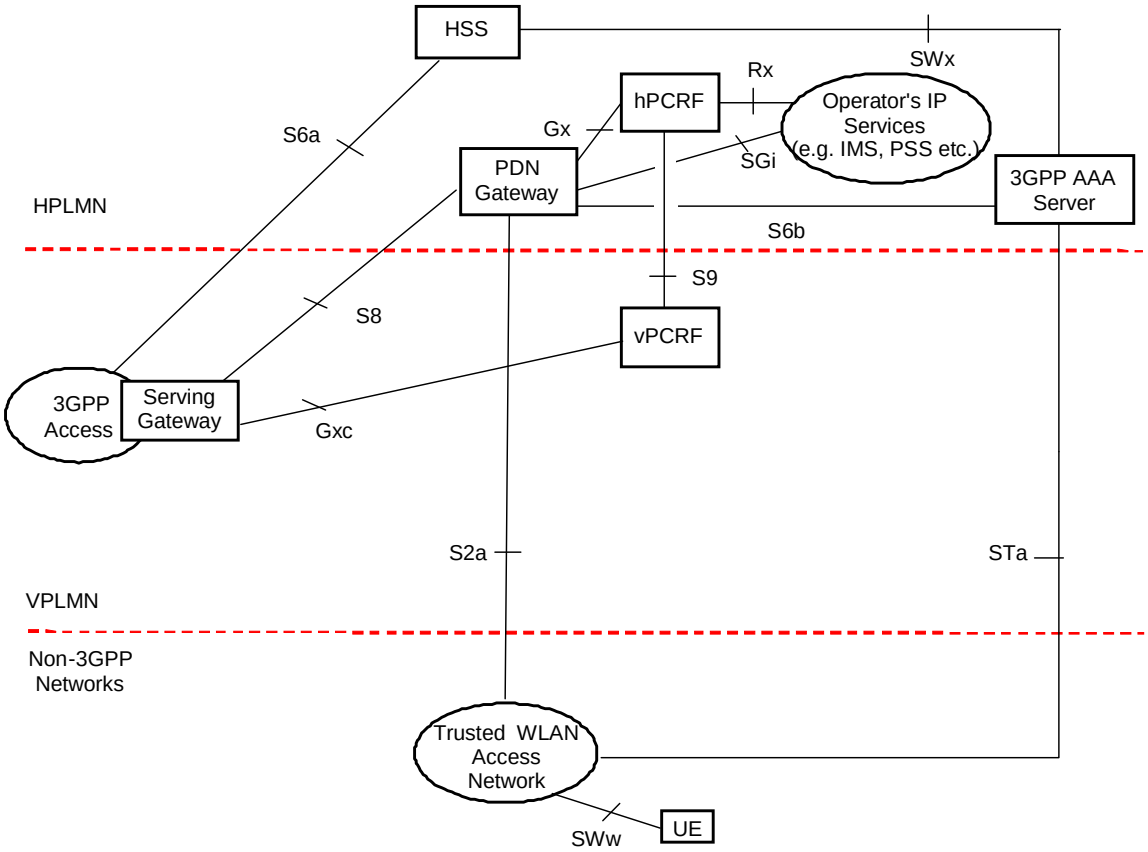


Figure 16.1.1-4: Roaming architecture for Trusted WLAN access to EPC - Home routed, HPLMN provides WLAN service

16.1.2 High level functions

The detailed functional split within a Trusted WLAN Access Network (TWAN) is not in the scope of 3GPP. Nevertheless, the procedures specified in the subsequent sections assume the following functions in the TWAN:

- A WLAN Access Network (WLAN AN). WLAN AN includes a collection of one or more WLAN access points. An access point terminates the UE's WLAN IEEE 802.11 link defined in IEEE Std 802.11-2012 [64].
- A Trusted WLAN Access Gateway (TWAG). This function terminates S2a.
  - When the TWAN provides access to EPC in Transparent Single-Connection mode or in Single-Connection mode, it forwards packets between the UE-TWAG point-to-point link and the S2a tunnel for that UE. The association in the TWAN between UE-TWAG point-to-point link and S2a tunnel is based on the UE MAC address.
  - When the TWAN provides access to EPC in Multi-Connection mode, it forwards user plane packets between the UE-TWAG point-to-point link corresponding to a specific PDN connection and the associated S2a tunnel for that UE. The UE's MAC address and a TWAG's MAC address that is assigned for a specific PDN connection are used to identify the point-to-point link between the UE and its serving TWAG, which corresponds to the S2a tunnel for the associated PDN connection.
  - When the TWAN provides access to EPC in Multi-Connection mode, the WLCP signaling is used between the UE and the TWAG.
- A Trusted WLAN AAA Proxy (TWAP). This function terminates STa. It relays the AAA information between the WLAN Access Network and the 3GPP AAA Server or Proxy in case of roaming. It establishes the binding of UE subscription data (including IMSI) with UE MAC address on the WLAN Access Network. If L2 attach triggers are used, it informs the TWAG of L2 attach events. It is aware of UE L2 Detach from the WLAN Access Network and informs the TWAG of L2 Detach events. It provides the TWAG with UE subscription data during initial attach or at UE subscription data modification.

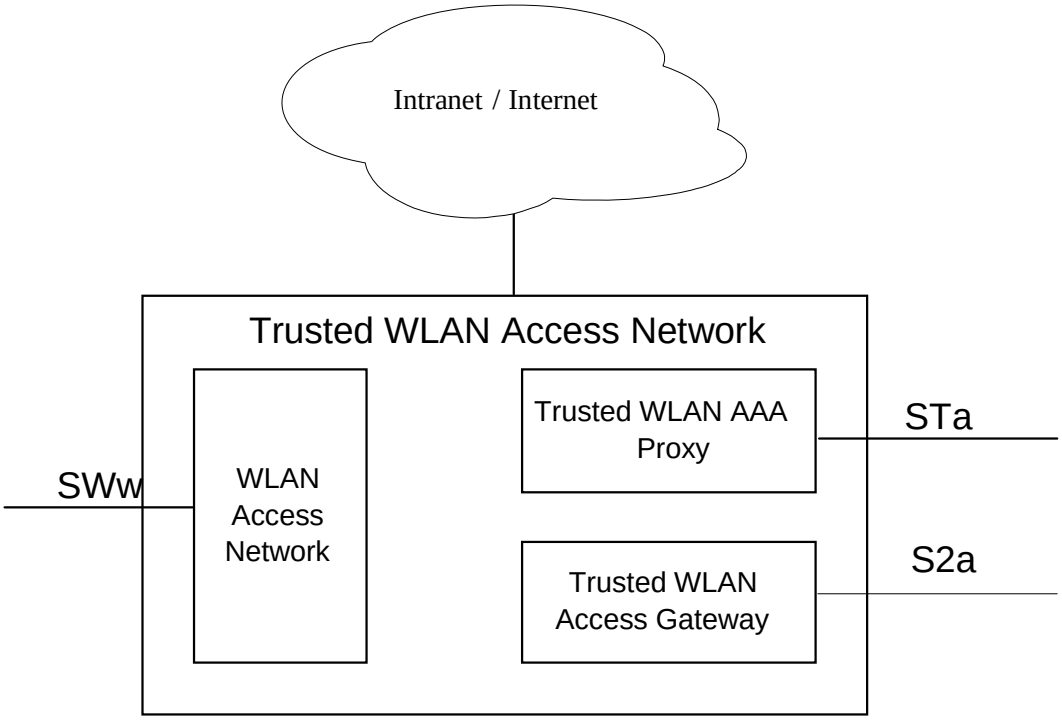


Figure 16.1.2-1: Trusted WLAN Access Network functional split

A per-UE point-to-point link between the UE and the TWAG is required when traffic for that UE is routed via S2a. Additionally, in Multi-Connection mode, one point-to-point link between an UE and its serving TWAG is required for transporting user plane traffic for every PDN connection. The UE's MAC address and an associated TWAG's MAC address are used to identify the point-to-point link between the UE and its serving TWAG that is associated to a specific PDN connection. In particular,it is assumed that the WLAN AN enforces upstream and downstream forced-forwarding between the UE's WLAN IEEE 802.11 association and the TWAG. The aspects of point-to-point link described in RFC 5213 [8] and RFC 5844 [17] also apply to the point-to-point link between UE and TWAG. The implementation of the point-to-point link, including how and when it is setup, is out-of-scope of 3GPP.

NOTE 1: In TSCM from the UE's perspective the SWw reference point appears as a shared medium / link as any other IEEE 802.11 WLAN and thus the UE can use the subnet prefix / mask and the default GW address for its packet routing decisions. The point-to-point nature of the link is realized by the TWAN enforcing that packets sent from, and received by the UE are respectively forwarded to, and forwarded by the TWAG.
In SCM and MCM from the UE's perspective an EPC routed PDN connection over the SWw reference point appears as a point-to-point link similar to how it is in 3GPP access. Shared link parameters such as netmask and default router IP address are not used in these modes.

NOTE 2: Gxa interface is not used for S2a-PMIP in Trusted WLAN within this Release of the specification. No policy interworking solution based on S9a is defined for Fixed Broadband access interworking via S2a within this Release of the specification.

NOTE 3 : Whether multiple TWAN functions are mapped to a single entity, or a single TWAN function is distributed among multiple entities is out-of-scope of 3GPP.

In order to support EPC access through S2a over Trusted WLAN the following functions shall be supported by the UE:

- WLAN specifications as per IEEE Std. 802.11-2012 [64].
- 3GPP-based network access authentication with EPC over WLAN as defined in clause 4.9.1, using IEEE Std 802.1X-2004 [65].
- IPv4 and/or IPv6 support:
  - For IPv4: IETF RFC 791 [66], IETF RFC 2131 [28]
  - For IPv6: IETF RFC 2460 [67], IETF RFC 4861 [38], and IETF RFC 4862 [58]

Three different modes of operation are distinguished: Transparent Single-Connection mode, Single-Connection mode and Multi-Connection mode. The UE and the network negotiate the mode of operation as part of the authentication procedure based on extensions to the EAP-AKA', (IETF RFC 5448 [72]) signaling between the UE and the network.

The Single-Connection mode only supports NSWO or a single PDN connection at a given time over a Trusted WLAN. On the other hand, the Multi-Connection mode supports simultaneous one or more PDN connections and/or NSWO over Trusted WLAN. Both Single-Connection mode and Multi-Connection modes support IP address preservation between 3GPP and Trusted WLAN access and PDN connectivity to a non-default APN.

The Single-Connection mode does not require additional protocols than EAP-AKA' in order to establish NSWO or PDN connectivity.

The multi connection mode uses a specific protocol (WLCP, specified in clause 16.1.4A3.1) after the access authentication procedure to trigger PDN connection establishment / release.

The negotiation of connection mode is further detailed in clause 16.4.A.1.

In Transparent Single-Connection mode, handover-indicator from the UE, APN indication from the UE and PCO via WLAN are not supported. As a consequence the following features are not supported: handover between TWAN and 3GPP access with IP address preservation; connectivity to a non-default APN; UE initiated connectivity to additional PDN.

16.1.3 Reference points

16.1.3.1 STa reference point

In addition to STa reference point features specified for any non-3GPP IP access network, STa reference point specification is enhanced with the following features for the support of EPC access through S2a over Trusted WLAN:

- A way for the TWAN to provide the 3GPP AAA server with following information:
  - An indication on whether the TWAN supports S2a, non-seamless offload or both;
  - An indication on whether the TWAN supports Transparent Single-Connection, Single-Connection mode or Multi-Connection mode or a combination of them;
  - The PDN addresses provided by the PGW for EPC access in Single-Connection mode;
  - The TWAG control plane IP address to be used for WLCP if the TWAN supports the Multi-Connection Mode;
  - The SSID selected by the UE to access the TWAN.
  - A Session Management back-off timer to be sent to the UE in Single-Connection mode.
- A way for the 3GPP AAA server to provide the TWAN with following information:
  - Whether access to EPC is allowed for the UE on the TWAN;
  - As for any Trusted Non-3GPP Access, when the UE is allowed to access EPC via TWAN, the subscription data of the user including the default APN to be associated with the user for EPC access; the TWAN uses the default APN to establish the PDN connection with the PDN GW in the absence of UE signalling of the APN it desires to reach over the Trusted WLAN. Based on the HPLMN operator configuration the HSS may provide the 3GPP AAA server with a default APN for Transparent Single-Connection mode different from the 3GPP access default APN;
  - An indication on whether the Single-Connection mode or Multi-Connection mode is selected for the UE. No indication provided by the 3GPP AAA server implies Transparent Single-Connection mode of operation.

16.1.3.2 SWw reference point

The SWw reference point connects the WLAN UE to the WLAN Access Network per IEEE Std 802.11-2012 [64]. The definition of IEEE Physical and Medium Access Control layers protocols (e.g. Layer 1 and Layer 2 defined by IEEE Std 802.11-2012 [64]) is out of the scope of 3GPP.

The SWw reference point also includes:

- The support of EAP (IETF RFC 3748 [11]) and EAP-AKA' (IETF RFC 5448 [72]) for UE authentication and authorization, as well as extensions to EAP-AKA' described in clause 16.1.4A.1;
- The support of WLCP signalling protocol used for establishment / release of PDN connections in the case of Multi-Connection mode;
- The support of multiple TWAG MAC addresses as user plane transport mechanism for the multiplexing of multiple PDN connections user data in the case of Multi-Connection mode.

16.1.3.3 S2a reference point

The S2a reference point connects the TWAN to the PDN GW. It supports two possible protocol variants: GTP and PMIPv6, to be chosen by the TWAN.

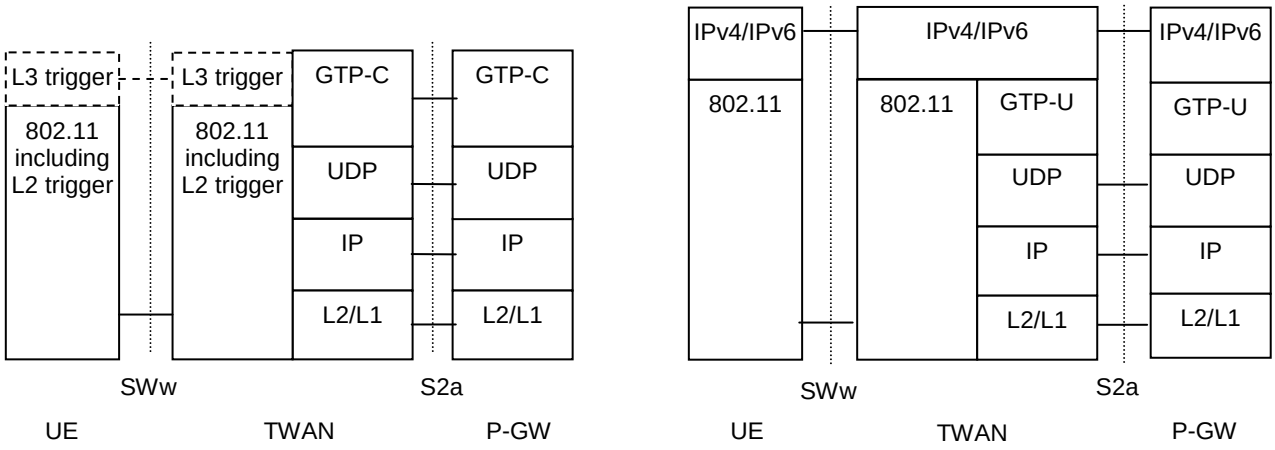
16.1.4 Protocol Stacks

The following protocols are supported on S2a:

- GTP.
- PMIPv6.

IPv4 address and IPv6 prefix allocation considerations are equally valid for GTP and PMIPv6 S2a options.

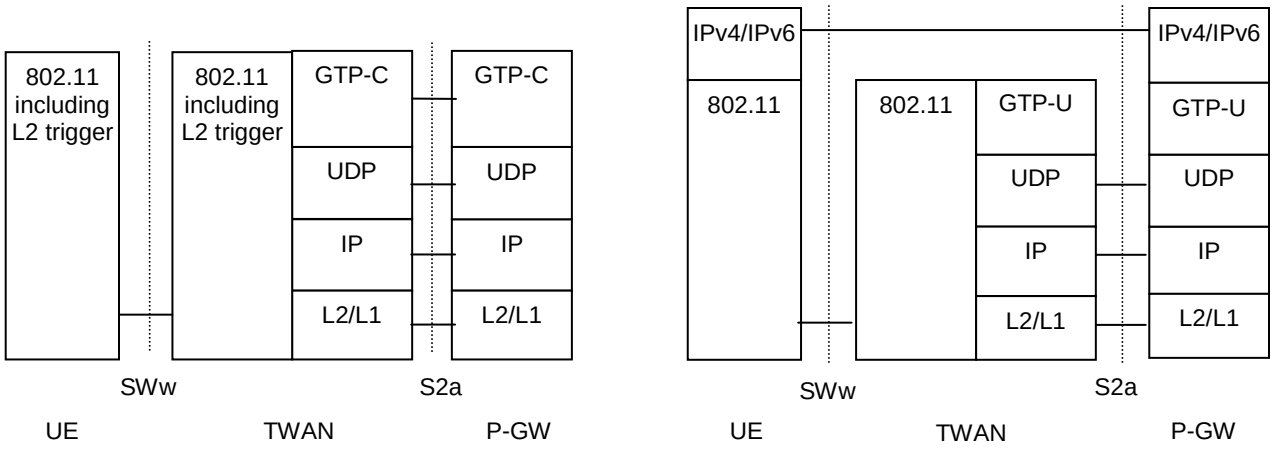
The figure below illustrates the control plane for S2a Tunnel Management and the user plane for GTP option, respectively for Transparent Single-Connection mode, Single-Connection mode and for Multi-Connection mode.



Control Plane for Tunnel Management **User Plane**

Legend:
802.11: This refers to Layer 1 and Layer 2 defined by IEEE Std 802.11-2012 [64]. Layer 2 of 802.11 is used as L2 attach and detach triggers. L2 attach trigger is mandatory with IPv6 and IPv4v6 PDN Types, and optional for IPv4 PDN Type.
L3 trigger: This refers to DHCPv4 which can be used as optional L3 attach trigger with IPv4 PDN Type.
GTP-C: The GPRS Tunnelling Protocol control plane consists of signalling messages between the Trusted WLAN Access Gateway and the PDN- GW over the S2a interface. It is defined in TS 29.274 [57].
GTP-U: The GPRS Tunnelling Protocol user plane tunnels user data between the Trusted WLAN Access Gateway and the PDN GW over the S2a interface. It is defined in TS 29.281 [63].
UDP: This is the transport layer protocol onto which both GTP-C and GTP-U are layered.
IPv4/IPv6: This refers to network layer protocols. On the TWAN this includes termination of the UE-TWAN link-local protocols (e.g. IPv6 Neighbor Discovery, ARP) and forwarding of user plane IP packets between the UE-TWAN point-to-point link and the relevant S2a tunnel.

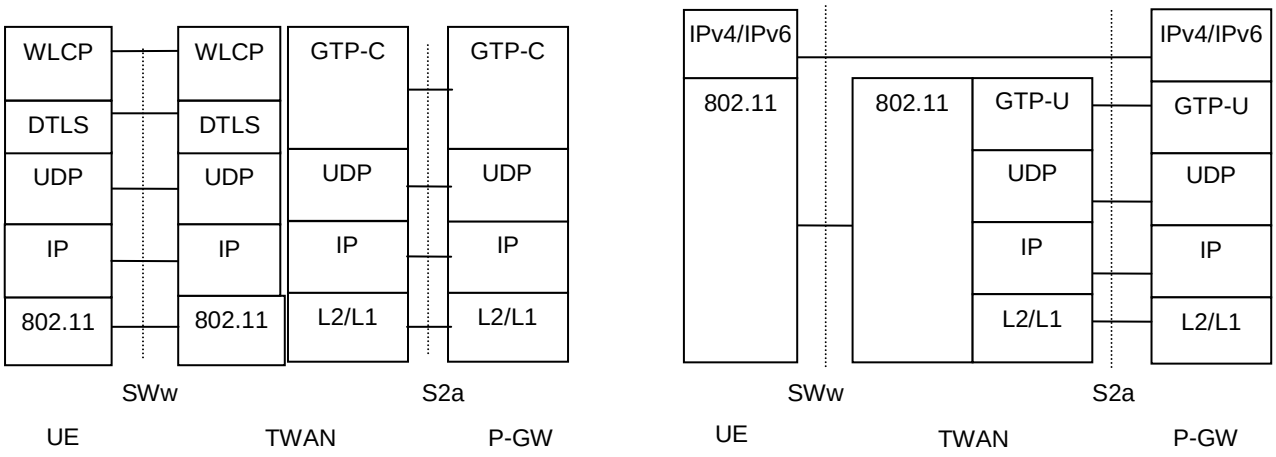
Figure 16.1.4-1: Protocols for control and user planes of GTP-based S2a for Transparent Single-Connection mode



Control Plane for Tunnel Management **User Plane**

Legend:
802.11: This refers to Layer 1 and Layer 2 defined by IEEE Std 802.11-2012 [64]. Layer 2 of 802.11 is used as L2 attach and detach triggers.
GTP-C: The GPRS Tunnelling Protocol control plane consists of signalling messages between the Trusted WLAN Access Gateway and the PDN- GW over the S2a interface. It is defined in TS 29.274 [57].
GTP-U: The GPRS Tunnelling Protocol user plane tunnels user data between the Trusted WLAN Access Gateway and the PDN GW over the S2a interface. It is defined in TS 29.281 [63].
UDP: This is the transport layer protocol onto which both GTP-C and GTP-U are layered.
IPv4/IPv6: This refers to network layer protocols.

Figure 16.1.4-2: Protocols for control and user planes of GTP-based S2a for Single-Connection mode



Control Plane for Tunnel Management **User Plane**

Legend:
802.11: This refers to Layer 1 and Layer 2 defined by IEEE Std 802.11-2012 [64]. The TWAG MAC address is used as a multiplexing identifier between multiple PDN connections which belong to the same UE.
WLCP: WLAN Control Protocol (WLCP) is used to establish and release PDN connections. The functionality of WLCP is defined in 16.1.4A.3.1.
GTP-C: The GPRS Tunnelling Protocol control plane consists of signalling messages between the Trusted WLAN Access Gateway and the PDN- GW over the S2a interface. It is defined in TS 29.274 [57].
GTP-U: The GPRS Tunnelling Protocol user plane tunnels user data between the Trusted WLAN Access Gateway and the PDN GW over the S2a interface. It is defined in TS 29.281 [63].
DTLS: Datagram Transport Layer Security (DTLS) is used to protect WLCP signalling as described in TS 33.402 [45].
UDP: This is the transport layer protocol onto which both GTP-C and GTP-U are layered.
IPv4/IPv6: This refers to network layer protocols.

Figure 16.1.4-3: Protocols for control and user planes for GTP-based S2a for Multi-Connection mode

When PMIP based S2a is used with Trusted WLAN, the PMIPv6 protocol stacks described in clause 6.1.1 apply.

16.1.4A Control Plane

16.1.4A.1 Negotiation of connection mode

The negotiation of the connection mode (Single-Connection mode, Multi-Connection mode or Transparent Single-Connection mode) takes place during the EAP-AKA' access authentication.

- The network indicates the supported connection modes (Transparent Single-Connection mode, Single-Connection mode, Multi-Connection mode or any combination of them).

- The UE then requests either Single-Connection mode or Multi-Connection mode. If none of these modes is supported by both UE and network, Transparent Single-Connection mode is used if supported by the network. In case the UE requests Single-Connection mode, it includes also a request for either EPC-routed traffic or NSWO. In case the UE requests Single-Connection mode and EPC-routed traffic, the UE may further indicate e.g. handover, APN and PDN type.

- If both the UE and the network support Multi-Connection mode, the UE requests multi connection mode.

- The network provides an appropriate result code to the UE, depending on if the request is granted or rejected.

A Multi-Connection mode capable UE may or may not be able to operate in single connection mode.

When a Multi-Connection mode capable UE connects to a network that is only capable of single connection mode, the UE operates in single connection mode, if the UE supports single connection mode.

The EAP-AKA' enhancements needed are described on clause 16.1.4A.2

16.1.4A.2 EAP-AKA' extensions

EAP-AKA ' authentication signaling [72] is extended in order to negotiate the connection mode: Single-Connection mode, Multi-Connection mode or Transparent Single-Connection mode, and to carry additional information needed for single connection mode.

NOTE 1: The selection by the UE and the use of Transparent Single-Connection mode (pre-Rel-12) do not require the support of any following EAP-AKA' extension.

EAP-AKA' authentication signaling is extended in order to exchange the following parameters:

1) In the UE to network direction:

   - The requested connection mode (Single-Connection mode or Multiple-Connection mode);
   - In case Single-Connection mode is requested;
     - The requested connectivity (NSWO or PDN connection), and
     - In case the requested connectivity is a PDN connection: the PDN type (IPv4, IPv6, or IPv4v6), an optional hand-over indicator, optionally the requested APN (mandatory if the handover indication is provided), optionally a Protocol Configuration Options (PCO)

2) In the network to UE direction:

   - The supported network connection modes (Transparent Single-Connection mode and/or Single Connection mode and/or Multi Connection mode);

   The supported TWAG WLCP IP version(s) if Multi-connection mode is supported;

   - In case Single-Connection mode is requested:
     - Whether the requested connectivity (NSWO or a PDN connection) has been granted;
     - For PDN connection: the Selected APN, the selected PDN type (IPv4, IPv6, or IPv4v6), and optionally Protocol Configuration Options (PCO), Session Management back-off timer.
   - In case Multi-Connection mode was requested:
     - Whether NSWO is allowed or not.
     - The TWAG IP address(es) of the control plane to be used for WLCP.

NOTE 2: For Multi-Connection mode, WLCP is always used for PDN connection establishment once the UE has been successfully authenticated.

16.1.4A.3 PDN connection management Control plane

16.1.4A.3.1 WLAN Control Protocol (WLCP)

WLCP is a control protocol between UE and TWAG. It applies to the support of Multi-Connection mode and enables management of PDN connectivity over a Trusted WLAN Access Network.

WLCP provides session management functionality required for:

- Establishment of PDN connections;
- Handover (from a 3GPP access) of PDN connections;
- Request the release of a PDN connection by the UE or notify the UE of the release of a PDN connection;
- IP address assignment (i.e. delivery of the IPv4 address through WLCP);

NOTE: Both IPv4 address assignment and IPv6 address assignment (SLAAC) can be supported in conjunction with WLCP.

The following PDN parameters are used:

- APN, PDN/PDP type, UE IP address/prefix, Protocol Configuration Options (PCO), Request type (initial request, handover) and optionally a Session Management back-off timer;
- The TWAG MAC address associated to the PDN connection.

WLCP signalling is protected using DTLS as described in TS 33.402 [45].

WLCP signalling is transported over DTLS, UDP and IP between the UE and the TWAG. The UE and the TWAG shall use a specific UDP port dedicated to WLCP when transporting the WLCP signalling. The WLCP/UDP traffic shall be carried with one of the following options:

- via IPv6 with link local addressing scope;
- via IPv4.

The UE uses the IPv6 link local address configured on the WLAN interface or the IPv4 address assigned via DHCPv4 by the network as the source IP address for WLCP. If NSWO is not authorized, then the UE is not expected to send traffic other than WLCP protocol traffic from this source IP address. The UE receives an indication from the AAA via EAP whether the TWAG supports IPv4 or IPv6, or both for WLCP. If the network indicates that it only supports one IP version for WLCP and the UE does not support this IP version for WLCP, then the UE may operate in Single Connection mode (if the UE and network support Single Connection mode), or Transparent Single Connection mode may be used if supported by the network.

The UE receives a TWAG IPv6 address with link local scope or a TWAG IPv4 address, or both as part of the EAP authentication, as descried in clause 16.2.1, to be used for WLCP signalling.

The selection of IPv4 and IPv6 is UE implementation dependant if both versions are supported by the UE and the TWAG for WLCP.

NOTE 1: WLCP protocol is a specific 3GPP protocol for which the details are defined in TS 24.244 [76].

NOTE 2: Aspects, such as segmentation, retransmission, are specified in stage 3 specifications.

16.1.4B User plane

16.1.4B.1 User plane for PDN connection

There is a one-to-one mapping between the PDN connection and the S2a tunnel, and there is a one-to-one mapping between the PDN connection and the point-to-point link between UE and TWAG. When the PDN connection is established during the UE initiated WLCP procedure, the TWAG sends a MAC address, which is specific for the PDN connection, to UE to be used by the UE as the MAC address of the TWAG for user plane packets. The TWAG maintains the mapping between the MAC address and the PDN connection.

The UE also maintains the mapping between the PDN connection and the TWAG MAC address corresponding to the PDN connection received during the WLCP procedure.

16.1.5 IP address allocation

16.1.5.1 General

In this Release of the specification, deferred IPv4 address allocation is not supported.

When using Single-connection mode and Multi-connection mode, the UE sees the PDN Connection as a point-to-point link similar to how it is in 3GPP access. Shared link parameters such as netmask and default router IP address are not used.

In Transparent Single-connection Mode, TWAG shall act as DHCPv4/v6 server for the UE.

In Single-connection mode and Multi-connection mode, the link model is described below:

- To support IPv4 connectivity, the IPv4 address shall be allocated and sent to the UE during PDN connection establishment.

- To support IPv6 connectivity, the PGW handles the RS/RA messages in GTP-based S2a scenario, while the TWAG handles the RS/RA messages in PMIP-based S2a scenario.

- To support IPv6 parameter configuration UE may use stateless DHCPv6. The PGW acts as DHCPv6 server. With PMIP-based S2a the TWAG may act as DHCPv6 relay.

16.1.5.2 IP address allocation in Transparent Single-Connection Mode

In order to enable IPv4 connectivity the TWAN shall support DHCPv4 server functionality for IPv4 parameter configuration and IP address allocation as specified in RFC 2131 [28] and RFC 4039 [29]. For this case the following applies:

- If the PDN type in the user subscribtion data is IPv4 or IPv4v6, the TWAN requests IPv4 address in the Proxy Binding Update or GTP Create Session Request from the PDN GW. The IPv4 address is delivered to the TWAN during the PMIPv6 or GTP tunnel establishement. When the UE requests the IPv4 address via DHCPv4, the TWAN delivers the received IPv4 address to the UE within DHCPv4 signalling after the PMIPv6 or GTP tunnel is established between the TWAN and the PDN GW.

NOTE 1: As a consequence the PDN GW configuration for the default APN used via Trusted WLAN access cannot dictate the use of deferred IPv4 address allocation.

NOTE 2: After releasing the IPv4 address using DHCPv4 Release procedure, the UE may subsequently request an IPv4 address for the same PDN connection. If the PDN connection is not released at this point of time, a subsequent IPv4 address request by the UE will result in the allocation of the same IP address, as the IPv4 address assigned to the UE has not been released in the PDN GW and TWAN.

In order to enable IPv6 the TWAN shall support of prefix advertisement for IPv6 prefix received from PDN GW in PMIPv6 Proxy Binding Acknowledgement or in the GTP Create Session Response. Moreover the TWAN may support DHCPv6 server functionality for IPv6 parameter configuration as specified in RFC 3736 [30]. This functionality is required to support DHCPv6 based parameter configuration mechanism in the UE. The TWAN may also support IPv6 RA options for DNS configuration accorduing to RFC 6106 [68].

NOTE 3: Configuration parameters are received from the PDN GW within PMIPv6 PBA message or within GTP Create Session Response message.

After the PDN GW releases the IPv4 address and/or IPv6 prefix, the PDN GW should not assign the same IPv4 address and/or IPv6 prefix to another UE immediately.

In case of static IP address allocation, the TWAN may receive a static IP address (i.e. a static IPv4 address and/or a static IPv6 prefix) from HSS/AAA during access authentication and authorization procedure. Then the TWAN should forward the static IP address to the PDN GW during the tunnel establishment request (in PBU or in Create Session Request message).

16.1.5.3 IP address allocation in Single-Connection Mode

Similar mechanism as described in TS 23.401 [4] clause 5.3.1.1 is used to decide the PDN type, with the following exceptions:

- The UE indicates the requested PDN type during EAP authentication procedure.

- The TWAG selects the PDN type according to the subscription data in the same way as the MME selects it when 3GPP access is used, as described in TS 23.401 [4].

- If the requested PDN type is IPv4v6, and both IPv4 and IPv6 PDN types are allowed by subscription but not IPv4v6, the TWAG shall set the PDN type to IPv4 or IPv6 where the selection between IPv4 and IPv6 is implementation specific. Then the UE shall not initiate the UE requested PDN connectivity procedure to this APN in order to activate a second PDN connection with the other single address PDN type.

If the PDN Type associated with the PDN connection is IPv4:

- The PDN GW shall allocate and send the IPv4 address to the TWAG in the Create Session Response or Proxy Binding Acknowledgement message. The IPv4 address received from the PDN GW is provided to the UE during the EAP authentication procedure. The PDN GW also sends IPv4 configuration parameters to the UE via PCO.

If the PDN Type associated with the PDN connection is IPv6:

- With GTP-based S2a, the PDN GW shall allocate and send the IPv6 network prefix to the UE in RA message. Because any prefix that the PDN GW will advertise to the UE is unique, there is no need for the UE to perform Duplicate Address Detection for global uniqueness for any IPv6 address configured from the allocated IPv6 network prefix. However, the PDN GW shall respond with Neighbor Advertisement upon receiving Neighbor Solicitation messages from a given UE. For example, the UE may perform Neighbor Unreachability Detection towards the PGW, the PGW supports the DAD related functionality as described in TS 23.401 [4]. Moreover, to ensure that link-local address generated by the UE does not collide with the link-local address of the PGW, the PDN GW shall provide an interface identifier to the UE and the UE shall use this interface identifier to configure its link-local address.

- With PMIP-based S2a, the PDN GW shall allocate and send the IPv6 network prefix to the TWAG in the Proxy Binding Acknowledgement. The TWAG sends it to the UE in RA message. Because any prefix that the TWAG will advertise to the UE is unique, there is no need for the UE to perform Duplicate Address Detection for global uniqueness for any IPv6 address configured from the allocated IPv6 network prefix. However, TWAG shall respond with Neighbor Advertisement upon receiving Neighbor Solicitation messages from a given UE, similar to that supported by PGW in the case of GTP based S5/S8 described in TS 23.401 [4], clause 5.3.1.2.2. Otherwise the PGW has the same functions as it is defined in TS 23.401 [4], clause 5.3.1.2.2. Moreover, to ensure that link-local address generated by the UE does not collide with the link-local address of the TWAG, the PDN GW shall provide an interface identifier to the UE and the UE shall use this interface identifier to configure its link-local address. The PDN GW shall also provide a link-local address to the TWAG and the TWAG shall use the link-local address on the access link shared with the UE.

- The PGW may support DHCPv6 server functionality for IPv6 parameter configuration as specified in RFC 3736 [30]. When the UE requests IPv6 parameter configuration via DHCPv6 procedure, the TWAG delivers DHCPv6 signallings between the UE and the PGW as a DHCPv6 relay in PMIP-based S2a scenario.

If the PDN type associated with the PDN connection is IPv4v6:

- The TWAG shall request both IPv6 network prefix and IPv4 address in the Create Session Request or Proxy Binding Update message.

- The IPv4 address allocation and IPv4 parameter configuration are the same as for PDN type IPv4 defined in previous bullets.

- The IPv6 network prefix allocation via IPv6 Stateless Address auto-configuration procedure and IPv6 parameter configuration via Stateless DHCPv6 procedure are the same as for PDN type IPv6 defined in previous bullets.

After the PDN GW releases the IPv4 address and/or IPv6 prefix, the PDN GW should not assign the same IPv4 address and/or IPv6 prefix to another UE immediately.

In case of static IP address allocation, the TWAG may receive a static IP address (i.e. a static IPv4 address and/or a static IPv6 prefix) from HSS/AAA during access authentication and authorization procedure. Then the TWAG should forward the static IP address to the PDN GW during the tunnel establishment request (in PBU or in Create Session Request message).

16.1.5.4 IP address allocation in Multi-Connection Mode

Similar mechanism as described in TS 23.401 [4] clause 5.3.1.1 is used to decide the PDN type, with the following exceptions:

- The UE indicates the request PDN type in WLCP signalling.

- The TWAG selects the the PDN type according to the subscription data received from the HSS/AAA in the same way as the MME selects it when 3GPP access is used, as described in TS 23.401 [4].

If the PDN Type associated with the PDN connection is IPv4:

- The PDN GW shall allocate and send the IPv4 address to the TWAG in the Create Session Response or Proxy Binding Acknowledgement message. The TWAG shall send the IPv4 address received from the PDN GW to the UE in WLCP message. The PDN GW also sends IPv4 configuration parameters to the UE via PCO.

If the PDN Type associated with the PDN connection is IPv6:

- The same considerations as above for PDN type IPv6 in single connection mode apply.

If the PDN type associated with the PDN connection is IPv4v6:

- The TWAG shall request both IPv6 network prefix and IPv4 address in the Create Session Request or Proxy Binding Update message.
- The IPv4 address allocation and IPv4 parameter configuration are the same as for PDN type IPv4 defined in previous bullets.
- The IPv6 network prefix allocation via IPv6 Stateless Address auto-configuration procedure and IPv6 parameter configuration via Stateless DHCPv6 procedure are the same as for PDN type IPv6 defined in previous bullets.

After the PDN GW releases the IPv4 address and/or IPv6 prefix, the PDN GW should not assign the same IPv4 address and/or IPv6 prefix to another UE immediately.

In case of static IP address allocation, the TWAG may receive a static IP address (i.e. a static IPv4 address and/or a static IPv6 prefix) from HSS/AAA during access authentication and authorization procedure. Then the TWAG should forward the static IP address to the PDN GW during the tunnel establishment request (in PBU or in Create Session Request message).

16.1.6 Bearer model for PDN connectivity service with GTP based S2a

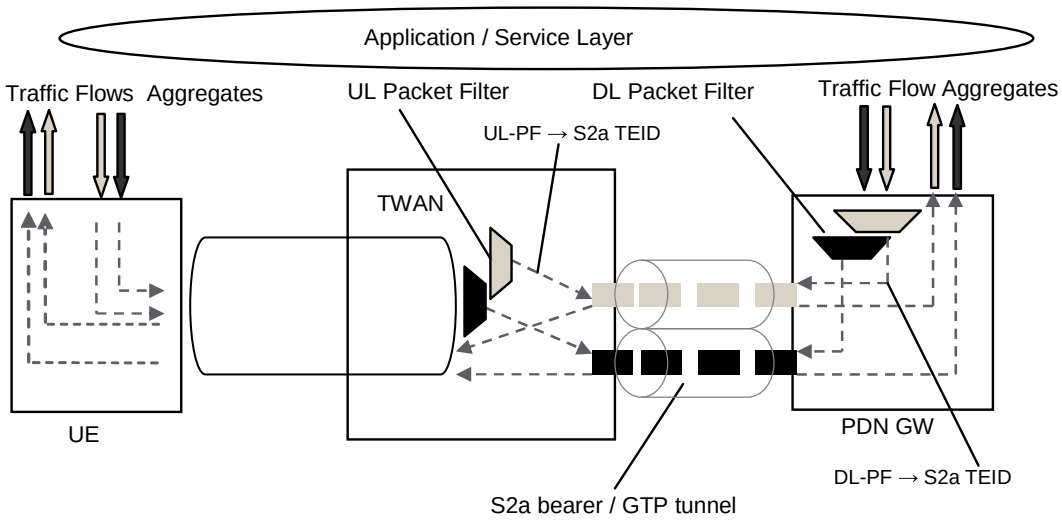


Figure 16.1.6-1: Two Unicast S2a bearers (GTP based S2a)

For Trusted WLAN access to the EPC, the PDN connectivity service is provided by the point-to-point connectivity between the UE and the TWAG concatenated with S2a bearer(s) between the TWAG and the PDN GW.

The bearer model of GTP based S2a interface is similar to that of GTP based S5/S8 interface and GTP based S2b interface. The TWAN handles the uplink packets based on the uplink packet filters in the TFTs received from the PDN GW for the S2a bearers of the PDN connection, in the same way as an ePDG does for GTP based S2b interface.

16.1.7 Access Network information reporting in case of a TWAN Access

In order for an Application Function (e.g. the P-CSCF) to be able to determine the NPLI (Network Provided location Information) of an UE in case of a TWAN access, the TWAN shall report over S2a TWAN related Access Network

Information at PDN connection establishment, at bearer creation / modification / release and at PDN connection release. Such TWAN related Access Network Information may correspond to a "TWAN Identifier" and/or to a UE Time Zone.

The TWAN Identifier (reported over S2a, Gx, Gy, ...) shall include the SSID of the access point to which the UE is attached and shall include at least one of the following elements, unless otherwise determined by the TWAN operator's policies:

- the BSSID (see IEEE Std 802.11-2012 [64]);
- civic address information of the AP to which the UE is attached;
- . line identifier (Logical Access ID see ETSI ES 282 004 [77]) of the access point to which the UE is attached.

NOTE 1: The SSID can be the same for several WLAN APs and SSID only may not provide a location, but it might be sufficient for charging purposes.

NOTE 2: The Information carried as part of theTWAN Identifier should be defined to cater for extension in future releases.

The TWAN Id may also contain the identifier of the operator of the TWAN. When the TWAN is operated by a mobile operator, this corresponds to a PLMN-ID. When the TWAN is not operated by a mobile operator, this corresponds to an operator Name (e.g. in Realm format).

16.2 Initial Attach in WLAN on S2a

16.2.1 Initial Attach in WLAN on GTP S2a

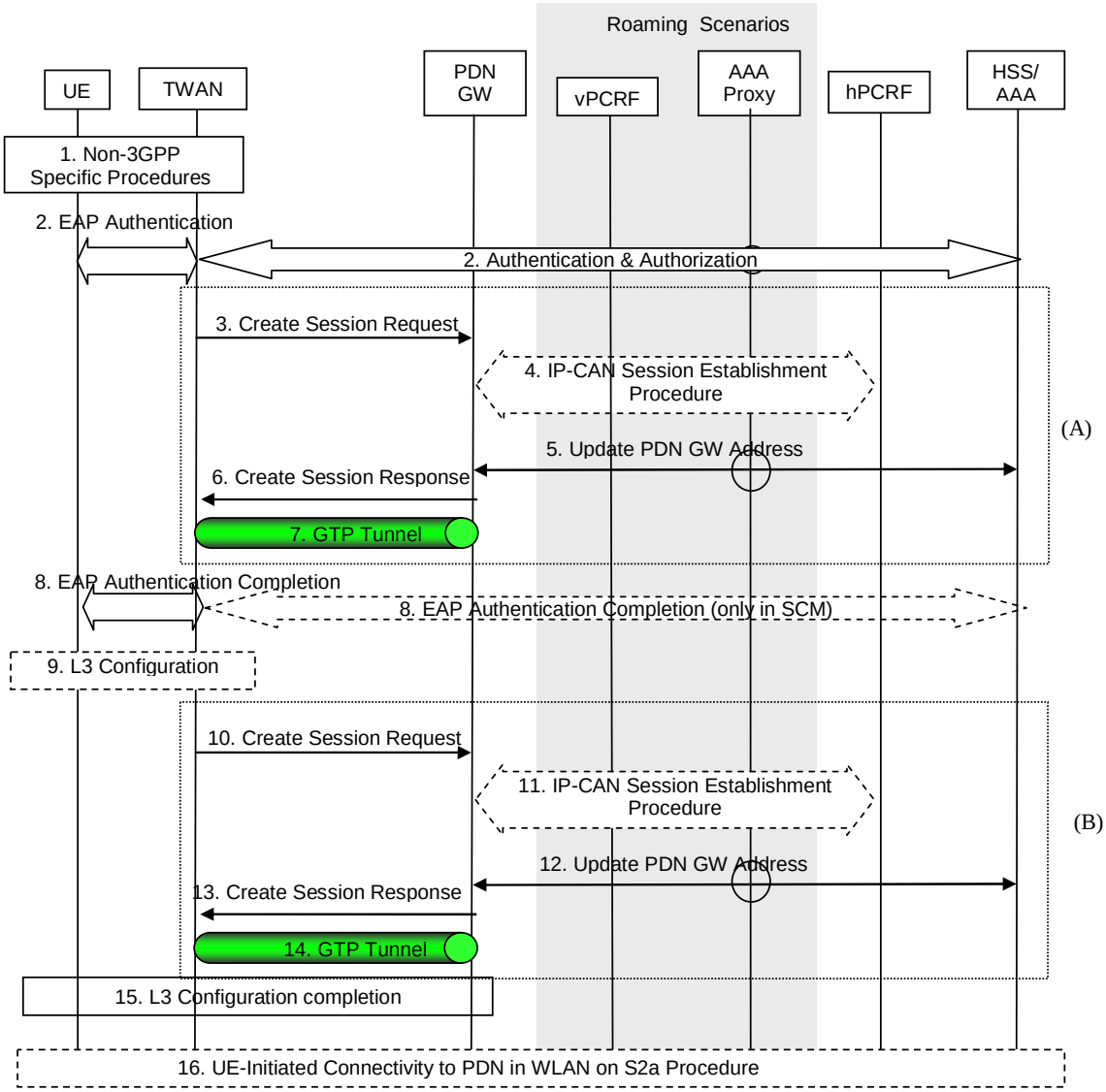


Figure 16.2.1-1: Initial attachment in WLAN on GTP S2a for roaming, LBO and non-roaming scenarios

The home routed roaming, LBO and non-roaming scenarios are depicted in the figure 16.2.1-1:

- In the LBO case, the 3GPP AAA Proxy acts as an intermediary, forwarding messages from the 3GPP AAA Server in the HPLMN to the PDN GW in the VPLMN and vice versa. Messages between the PDN GW in the VPLMN and the hPCRF in the HPLMN are forwarded by the vPCRF in the VPLMN.

- In the home routed roaming and non-roaming cases, the vPCRF is not involved. In the non-roaming cases, the 3GPP AAA Proxy is not involved. In home routed roaming case, the 3GPP AAA Proxy is not involved in steps 5 and 12.

This procedure is also used to establish the first PDN connection over a trusted WLAN with S2a when the UE already has active PDN connections only over a 3GPP access and wishes to establish simultaneous PDN connections to different APNs over multiple accesses.

Either scenario (A) or scenario (B) is performed:

- Scenario (A) is defined as the TWAP sending the layer 2 attach trigger to the TWAG. This is done at successful EAP authentication (step 2). Completion of EAP authentication with the TWAP informing the UE of EAP

success is deferred until step 8 after the tunnel was established (steps 3-7). The attach trigger signal sent from TWAP to TWAG includes MAC address and subscription data (including IMSI) of the UE. Steps 10-14 are omitted in scenario (A). Scenario (A) is applicable for all existing PDN Types (IPv4, IPv6, IPv4v6) and is the recommended way. Scenario (A) is only applicable for single-connection mode and transparent single-connection mode.

- Scenario (B) is defined as the TWAG using the layer 3 attach request (i.e. a DHCPv4 message) sent by the UE as the attach trigger. In this scenario steps 3-7 are omitted. Step 9 triggers the TWAG to establish the tunnel (steps 10-14). Between step 2 and step 10, the TWAG obtains subscription data (including IMSI) for the UE from the TWAP, based on the MAC address of the UE. How this is performed is out-of-scope for 3GPP. Scenario (B) is only applicable for transparent single-connection mode with PDN Type IPv4.

The steps below only refer to TWAN, not to specific functions internal to TWAN (i.e. TWAG, TWAP and WLAN AN).

1. The initial TWAN specific L2 procedures are performed. These procedures are TWAN specific and are outside the scope of 3GPP.

2. The EAP authentication procedure is initiated and performed involving the UE, the TWAN and the 3GPP AAA Server. In the roaming case, there may be several AAA proxies involved. When receiving the first EAP message from the UE, the TWAN transfers it to the AAA server with an indication of the modes of operation that it supports and, if TWAN supports multi-connection mode, with the supported TWAG IPv4, IPv6 or both control plane addresses for WLCP transport. Subscription data is provided to the TWAN by the HSS/AAA in this step. The list of all the authorized APNs, including additional PDN GW selection information is returned to the TWAN as part of the reply from the 3GPP AAA Server to the TWAN as described in clause 4.5.1. The Subscription data may also include a default APN for WLAN that, in case of transparent single-connection mode, may be different from the default APN for other accesses. The 3GPP AAA Server also returns to the TWAN the User Identity to be used to identify the UE in the Create Session Request (step 3 or 10).

   During the EAP authentication procedure, the UE may negotiate with the AAA Server a connection mode (e.g. single-connection or multi-connection mode) as described in clause 16.1.4A. In addition, the UE may provide connectivity parameters during EAP authentication, as described below.

   During the EAP authentication procedure the 3GPP AAA Server may request the UE to provide its IMEI(SV). In that case the UE shall signal its IMEI(SV) to the 3GPP AAA Server. The 3GPP AAA Server forwards IMEI(SV) received from the UE to the TWAN (over STa).

   If the UE requests single-connection mode, the UE provides a connectivity parameter indicating the type of requested connectivity, i.e. whether it requests EPC access or non-seamless WLAN offload. If the UE requests EPC access, it may provide additional connectivity parameters such as the PDN type, attach type (initial attach), the requested APN and Protocol Configuration Options. These connectivity parameters are sent to the 3GPP AAA Server during the EAP-AKA' authentication procedure. The 3GPP AAA Server sends these connectivity parameters to the TWAN.

   If the UE requests multi-connection mode and, if this request is accepted by the network, the UE is also made aware if non-seamless WLAN offload is authorized. If non-seamless WLAN offload is authorized, then the UE receives the address or prefix of the non-seamless WLAN offload connection as part of steps 9 and 15. In multi-connection mode, steps 3-7 and steps 10-14 are skipped. If the UE requests multi-connection mode and this request is accepted by the network, the AAA server using EAP-AKA' procedure provides the UE with the supported TWAG control plane address(es), among which the UE selects a single address to be used for WLCP.

   If the 3GPP AAA server does not provide network connection mode capabilities or, if the 3GPP AAA server does not receive a connection mode request from the UE, then the transparent single-connection mode is used.

NOTE 1: If the transparent single-connection mode is used, then it is recommended that the default APN for TWAN is different from any APN that the UE may use on the 3GPP side. Nevertheless, for an UE the default APN for TWAN may be used on other access technologies. In that case:

- The TWAN may select a single or different PDN GWs for PDN connections to this APN that are active at the same time via the 3GPP access network and the TWAN. If a single PDN GW is selected then the APN-AMBR is enforced for all PDN connections for that APN. If different PDN GWs are selected then the APN-AMBR is enforced separately in the respective PDN GW for the PDN connection, i.e. the UE will receive double amount of bandwidth for the APN;

- The PDN GW identity provided by the 3GPP AAA server to HSS as part of the Initial Attach on TWAN may be different from and overwrite the PDN GW identity provided, for the same APN, by the MME/SGSN or by another PDN GW. Therefore, to avoid interfering with the PDN Connections over 3GPP access, the HSS should not be updated with the selected PDN GW identity for Trusted WLAN access. The 3GPP AAA Server could be configured to not provide the PDN GW identity selected as part of the Initial Attach on TWAN to HSS. This applies to step 5 and step 12 of this procedure. Depending on operator deployment there may also be proprietary means in the HPLMN to ensure that the HSS is not updated with the selected PDN GW identity for Trusted WLAN access.

- The PDN GW identity provided by the MME/SGSN to HSS as part of the Initial Attach on 3GPP may be different from the PDN GW identity selected for the same APN by the TWAN. As there is no mobility support, no action from the TWAN is expected when the TWAN is updated with the selected PDN GW identity for 3GPP access;

- PMIP-based S5/S8 with dynamic PCC can not be deployed since it will result in wrong session linking between Gateway Control Session and Gx session in the PCRF.

IEEE Std 802.1X-2004 [65] is used over the WLAN air link to carry EAP as defined by IEEE Std 802.11-2012 [64].

The TWAN may provide to the 3GPP AAA server via STa the SSID selected by the UE to access the TWAN and an indication whether it supports S2a, non-seamless offload, or both.

If the transparent single-connection mode is used, then the HSS/AAA may indicate via STa whether access to EPC via S2a or the use of NSWO or both are allowed for this subscriber. The HSS/AAA decision to allow EPC access or NSWO or both could be based on information elements such as subscriber profile, access network, and/or SSID selected. If the HSS/AAA decides to allow both EPC access and NSWO, the TWAN determines based on pre-configured information whether or not to establish S2a. If the TWAN determined that S2a shall not be used steps 3-7 and 10-14 are skipped. Instead, if it is authorized, the TWAN performs NSWO for the subscriber.

NOTE 2: For transparent single-connection mode, the authorization of both NSWO and EPC routed traffic by the 3GPP AAA is only applicable in non-roaming scenarios.

If the UE requests single-connection mode, the HSS/AAA indicates via STa its decision to accept the single-connection mode with either EPC access or NSWO. The TWAN determines based on the indication from HSS/AAA whether or not to perform PDN GW selection and S2a connection establishment. If the UE requested NSWO and it was accepted by the network, steps 3-7 and 10-14 are skipped.

The following steps 3-7 are only performed in scenario (A):

3. The TWAN selects the S2a protocol variant (either GTP or PMIP; GTP in this case). The TWAN may be configured with the S2a protocol variant(s) on a per HPLMN granularity, or may retrieve information regarding the S2a protocol variants supported by the PDN GW (PMIP or/and GTP) from the Domain Name Service function.

   The TWAN selects the PGW as per the PGW selection procedure in clause 4.5.1; if the TWAN receives a PGW Identity under the form of a FQDN, it shall derive from the FQDN an IP address of a PGW for the selected mobility management protocol (GTP in this case).

   NOTE 3: As for existing principles, to support separate PDN GW addresses at a PDN GW for different mobility protocols (e.g. PMIP or GTPv2), when deriving a PDN GW address with the Domain Name Service function, the PDN GW Selection function takes into account the mobility protocol type.

   If the UE did not provide a requested APN in step 2, the TWAN selects the default APN according to the subscription data received in step 2. If the UE requested EPC access and indicated an APN in step 2, the TWAN verifies that it is allowed by subscription and selects that APN. The TWAN sends a Create Session Request (IMSI, APN, RAT type, TWAN TEID of the control plane, PDN Type, PDN Address, EPS Bearer Identity, Default EPS Bearer QoS, TWAN Address for the user plane, TWAN TEID of the user plane, APN-AMBR, Selection Mode, Dual Address Bearer Flag, Trace Information, Charging Characteristics, Serving Network, Additional parameters, Initial Attach Indication, IMEI(SV)) message to the PDN GW. The RAT type indicates the non-3GPP IP access technology type. The PDN Type shall be set based on the result of step 2. The TWAN shall set the Dual Address Bearer Flag when the PDN type is set to IPv4v6. The TWAN shall include Trace Information if PDN GW trace is activated. The Serving Network parameter identifies the selected PLMN used

for 3GPP-based access authentication i.e. the VPLMN in roaming case, and the HPLMN in non-roaming case. The optional Additional Parameters may contain information, for example, Protocol Configuration Options. Additionally, the Create Session Request includes the current TWAN Identifier as described in clause 16.1.7 and the UE Time Zone. The IMEI(SV) shall be provided to the PDN GW if received from the AAA server.

The PDN GW creates a new entry in its bearer context table and generates a Charging Id. The new entry allows the PDN GW to route user plane PDUs between the TWAN and the packet data network and to start charging.

NOTE 4: The EPS Bearer Identity and Default EPS Bearer QoS parameters convey the S2a bearer identity and the default S2a bearer QoS.

4. The PDN GW initiates the IP-CAN Session Establishment Procedure with the PCRF, as specified in TS 23.203 [19]. The PDN GW provides information to the PCRF used to identify the session. The PCRF creates IP-CAN session related information and responds to the PDN GW with PCC rules and event triggers. The PCRF may modify the APN-AMBR and send the APN-AMBR to the PDN GW in the response message.

5. The selected PDN GW informs the 3GPP AAA Server of its PDN GW identity and the APN corresponding to the UE's PDN Connection. The message includes information that identifies the PLMN in which the PDN GW is located. This information is registered in the HSS as described in clause 12.

   When informing the 3GPP AAA Server of the PDN GW identity, the selected PDN GW also indicates the selected S2a protocol variant (GTP in this case); this allows the option for the 3GPP AAA Server or 3GPP AAA Proxy not to return to the PDN GW PMIP specific parameters (e.g. static QoS Profile, Trace Information, APN-AMBR) if GTP is used over S2a; the PDN GW shall ignore those parameters if received from the 3GPP AAA Server or 3GPP AAA Proxy.

6. The PDN GW returns a Create Session Response (PDN GW Address for the user plane, PDN GW TEID of the user plane, PDN GW TEID of the control plane, PDN Type, PDN Address, EPS Bearer Identity, EPS Bearer QoS, APN-AMBR, Additional parameters possibly including Protocol Configuration Options, Cause) message to the TWAN, including the IP address(es) allocated for the UE.

   The PDN GW may initiate the creation of dedicated bearers on GTP based S2a (as it does on GTP based S5/S8 for an Attach on 3GPP access).

7. The GTP tunnel is set up between the TWAN and the PDN GW as described in step 3.

8. In single-connection mode, the TWAN informs the 3GPP AAA Server of the result of the tunnel setup, including APN, TWAG User Plane MAC address, accepted PDN Type, PDN Address and Additional Parameters received from the PGW. The UE is made aware if the requested connectivity type (non-seamless WLAN offload, EPC access with a requested APN) is accepted by the 3GPP AAA server. The TWAG User Plane MAC address is the MAC address of the TWAN which is used by the UE and the TWAN for encapsulating user plane packets. The 3GPP AAA server also indicates to the UE the TWAG User Plane MAC address, accepted PDN type, PDN Address, Additional Parameters. Also, if the UE requested EPC access without indicating a requested APN, then the network indicates the selected (default) APN. If the requested connectivity feature is not possible, the 3GPP AAA server rejects the request with a relevant authorization failure cause code.

   In multi-connection mode, the TWAN shall be configured to accept WLCP traffic from the UE; otherwise the TWAN shall discard WLCP traffic from the UE.

   TWAN sends EAP success to the UE thus completing EAP authentication.

   After EAP authentication, UE traffic over the WLAN air link may be confidentiality and integrity protected as defined by IEEE Std 802.11-2012 [64].

NOTE 5: In transparent single-connection mode, it is implementation dependent if step 8 is performed before, after or in parallel to steps 3-7.

9. In transparent single-connection mode, the UE may send layer 3 attach request, (e.g. a DHCPv4 request as per IETF RFC 2131 [28]). In multi-connection mode, if UE uses IPv4, the UE obtains an IPv4 address to be used for WLCP transport and NSWO (if authorized) at this step.

NOTE 6: The UE may send IPv6 Router Solicitation at any time after step 8.

NOTE 7: It is assumed that, to identify the UE, the L3 attach request is transported in an L2 frame that contains the UE L2 address (MAC address).

10-14. These steps are equal to step 3-7.

NOTE 8: These steps are only performed for scenario (B), which is only possible in the case of transparent single-connection mode when the PDN type is IPv4 and a DHCPv4 request was sent in step 9.

15. In transparent single connection mode and in multi-connection mode, a DHCPv4 message with allocated IPv4 address and/or Router Advertisement with IPv6 prefix is sent to the UE. The UE may perform additional IP layer configuration with the TWAN as per standard IETF procedures, e.g. IPv6 Stateless Address Autoconfiguration as per IETF RFC 4862 [58], and Stateless DHCPv6 as per IETF RFC 3736 [30].

    For single-connection mode, a Router Advertisement with IPv6 prefix may be sent to the UE. The UE may perform additional IP layer configuration as per standard IETF procedures, e.g. IPv6 Stateless Address Autoconfiguration as per IETF RFC 4862 [58], and Stateless DHCPv6 as per IETF RFC 3736 [30].

NOTE 9: For transparent single connection mode, a UE may request to get some IP configuration parameters (e.g. DNS server) by means of DHCP. These parameters sent by TWAN (acting as a DHCP server) to the UE in a DHCP reply. These parameters are retrieved by the TWAN from the PGW within Create Session Response.

NOTE 10: For scenario (A), after step 8, the TWAN may send unsolicited IP layer configuration signalling, e.g. RA, over the point-to-point link towards the UE.

16. In multi-connection mode, the procedure "UE initiated PDN connectivity request procedure in WLAN on S2a" in clause 16.8 may be performed to establish a PDN connection.

16.2.2 Initial Attach in WLAN on PMIP S2a

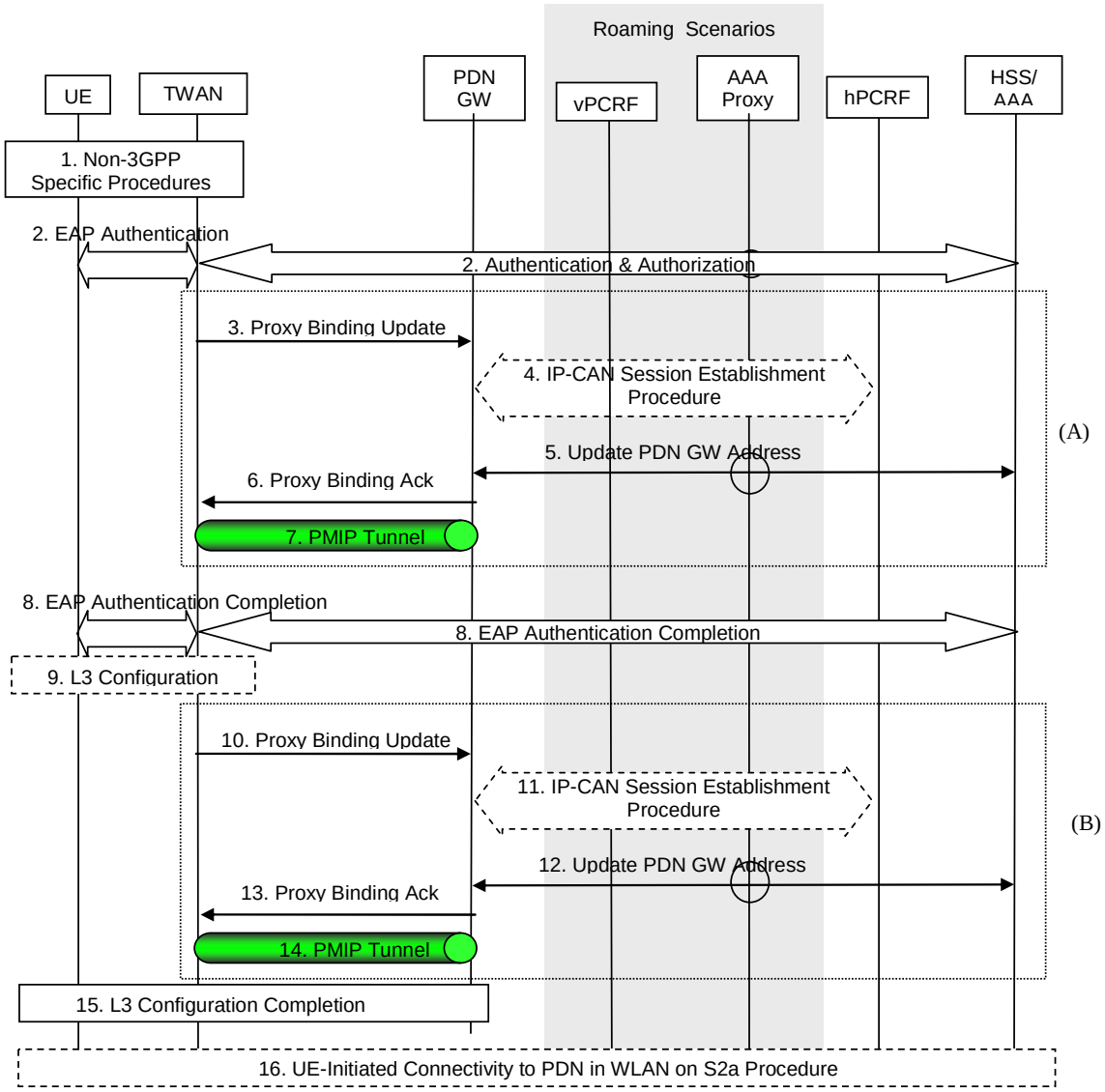


Figure 16.2.2-1: Initial attachment in WLAN on PMIP S2a for roaming, LBO and non-roaming scenarios

The home routed roaming, LBO and non-roaming scenarios are depicted in the figure 16.2.2-1:

- In the LBO case, the 3GPP AAA Proxy acts as an intermediary, forwarding messages from the 3GPP AAA Server in the HPLMN to the PDN GW in the VPLMN and vice versa. Messages between the PDN GW in the VPLMN and the hPCRF in the HPLMN are forwarded by the vPCRF in the VPLMN.

- In the home routed roaming and non-roaming cases, the vPCRF is not involved. In the non-roaming cases, the 3GPP AAA Proxy is not involved. In home routed roaming case, the 3GPP AAA Proxy is not involved in steps 5 and 12.

This procedure is also used to establish the first PDN connection over a trusted WLAN with S2a when the UE already has active PDN connections only over a 3GPP access and wishes to establish simultaneous PDN connections to different APNs over multiple accesses.

This procedure is based on clause 16.2.1 with the following key differences:

- In step 3 and 10 the TWAN selects S2a protocol variant, PMIPv6. The TWAN sends a Proxy Binding Update message. The details of the Proxy Binding Update message are described in step 5 in clause 6.2.1. Additionally, Proxy Binding Update includes the current TWAN Identifier as described in clause 16.1.7 and the UE Time

Zone. The TWAN shall also provide also the IMEI(SV) in Proxy Binding Update when it has received this information from the AAA server

- Step 5 and 12 is the same as described in step 7 in clause 6.2.1, except that the Proxy Binding Update message shall contain the Serving Network parameter, which identifies the selected PLMN used for 3GPP-based access authentication i.e. the VPLMN in roaming case, and the HPLMN in non-roaming case.

- In step 6 and 13 the PDN GW sends a Proxy Binding Acknowledgement message. The details of the Proxy Binding Acknowledgement message are described in step 8 in clause 6.2.1.

- In step 7 and 14 the established tunnel between the TWAN and PDN GW is a PMIPv6 tunnel.

NOTE 1: For transparent single-connection mode, the UE may request to get some IP configuration parameters (e.g. DNS server) by means of DHCP. These parameters sent by TWAN (acting as a DHCP server) to the UE in a DHCP reply. These parameters are retrieved by the TWAN from the PDN GW within Proxy Binding Ack.

16.2.3 HSS retrieval of information about an UE from the TWAN serving that UE

The procedure described in this clause supports the HSS retrieval of information about an UE from the TWAN serving that UE.

The information that the HSS can fetch corresponds to user location (TWAN ID) and/or UE Time Zone information (this information may e.g. be provided to an IMS AS that has requested the information as detailed in Annex R of TS 23.228 [74]). The User location information sent to the HSS contains information on the last known time of radio contact.

The TWAN ID is defined in clause 16.1.7.

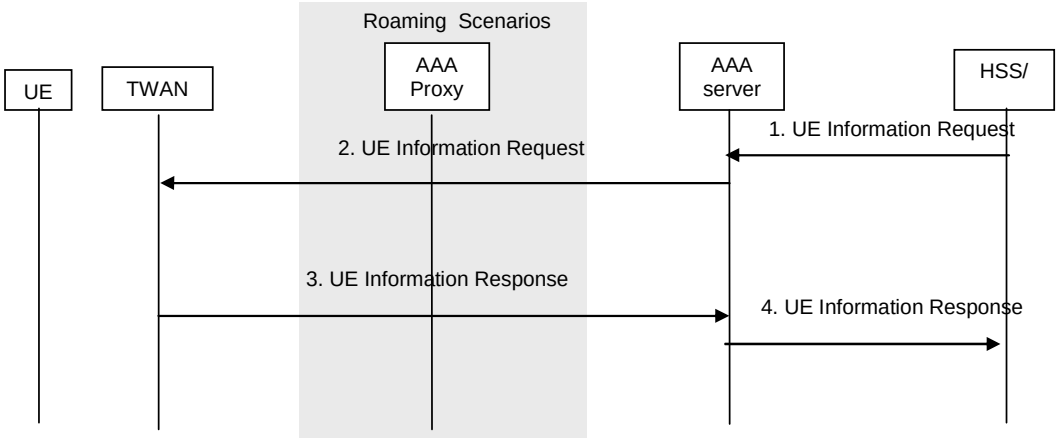


Figure 16.2.3: HSS retrieval of information about an UE from the TWAN

1) The HSS determines that it needs to get from the TWAN access Information about the UE (defined above the figure). The HSS sends an UE Information Request (UE Identity (IMSI), Nature of the Information to fetch) via the 3GPP AAA server supporting this UE.

2) The 3GPP AAA server determines the TWAN supporting an UE and transfers the request to the TWAN. In case of roaming a 3GPP AAA proxy is used.

3) The TWAN answers by an UE Information Response (UE Identity (IMSI), Information requested). In case of roaming a 3GPP AAA proxy is used

4) The UE Information Response is relayed from 3GPP AAA server to HSS.

16.3 Detach and PDN disconnection in WLAN on S2a

16.3.1 Detach and PDN disconnection in WLAN on GTP S2a

16.3.1.1 UE/TWAN Initiated Detach and UE/TWAN requested PDN Disconnection Procedure in WLAN on GTP S2a

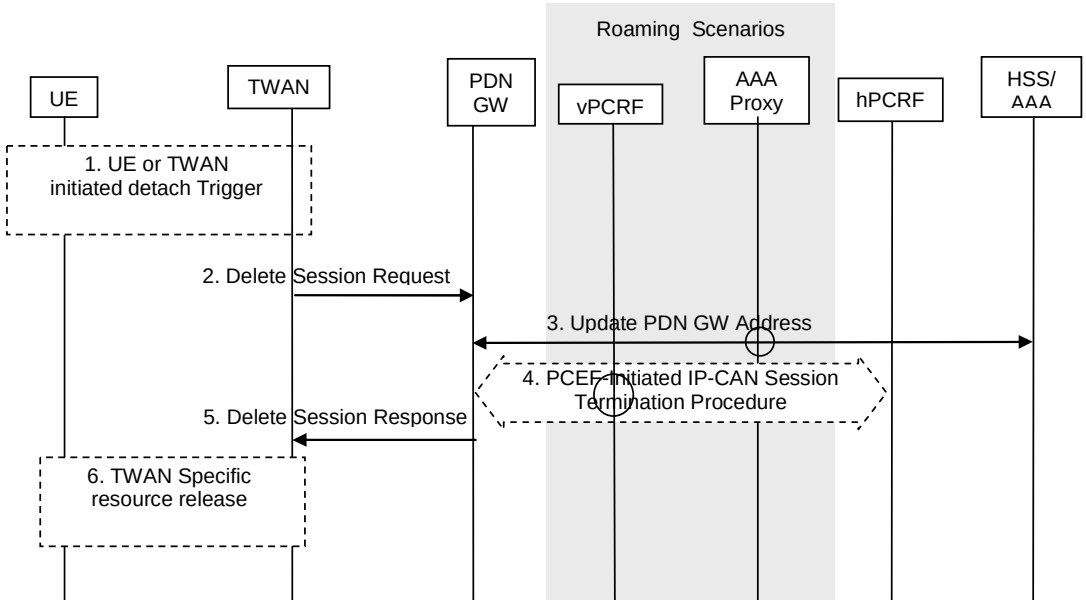


Figure 16.3.1.1-1: UE/TWAN Initiated Detach and UE/TWAN requested PDN Disconnection on GTP S2a

The procedure for UE/ TWAN Initiated Detach is represented in Figure 16.3.1.1-1 and described below.

This procedure applies to the transparent single-connection mode. This procedure also applies to the single-connection mode with the exception that step1 refers to clause 16.7.1.1.

This procedure applies to the Non-Roaming, Home Routed Roaming and Local Breakout cases. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF. In the Home Routed Roaming and LBO cases, the 3GPP AAA Proxy serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN. In the non-roaming and Home Routed Roaming case, the vPCRF is not involved at all.

If dynamic policy provisioning is not deployed, the optional steps of interaction between the PDN GW and PCRF do not occur. Instead, the PDN GW may employ static configured policies.

1) To detach from EPC, the UE can send a disassociation or deauthentication notification according to IEEE Std 802.11-2012 [64]. Any time after the UE releases the IPv4 address using DHCPv4 or IPv4 address lease time expires, and if the PDN Type is IPv4, the TWAN initiates "TWAN initiated PDN Disconnection Procedure" procedure. If there is no traffic received from the UE for a configurable duration and the TWAN detects the UE has left based on unanswered probes (e.g., ARP Request, Neighbor Solicitation message), the TWAN triggers PDN disconnection.

2) The TWAN releases the PDN connection by sending a Delete Session Request (Linked EPS Bearer ID, TWAN Release Cause if available) message for the PDN connection to the PDN GW. Additionally, the Delete Session Request includes the TWAN Identifier as described in clause 16.1.7, the Timestamp of this TWAN-Identifier and the UE Time Zone. TWAN Release Cause is only sent by the TWAN to the PDN GW if this is permitted according to TWAN operator's policy.

3) The PDN GW informs the 3GPP AAA Server of the PDN disconnection. If the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server notifies the HSS as described in clause 12.1.2.

4) The PDN GW deletes the IP-CAN session associated with the UE and executes a PCEF-Initiated IP-CAN Session Termination Procedure with the PCRF. If received from the TWAN, the PDN GW shall also provide the

TWAN Release Cause as well as, if available, the User Location Information that contains the TWAN Identifier and/or UE Time Zone and PCRF shall forward them to the Application Function as specified in TS 23.203 [19].

5) The PDN GW acknowledges with Delete Session Response (Cause).

6) The TWAN locally removes the UE context and deauthenticates and disassociates the UE at Layer 2 according to IEEE Std. 802.11-2012 [64].

NOTE: The L2 disassociation serves as an indication to the UE that the previous IPv4 address/IPv6 prefix might no longer be valid. When UE connects to the network next time, the UE proceeds with re-validation or re-acquisition of its IPv4 address / IPv6 prefix.

16.3.1.2 HSS/AAA Initiated Detach Procedure in WLAN on GTP S2a

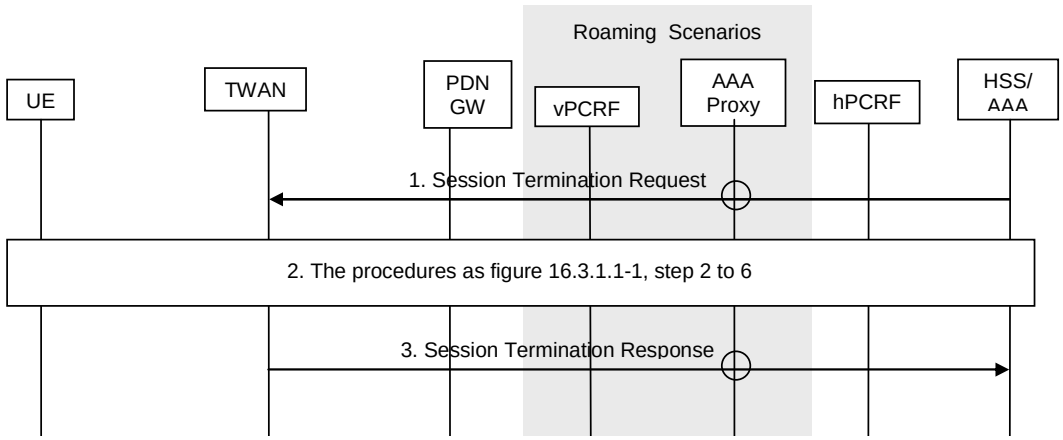


Figure 16.3.1.2-1: HSS/AAA Initiated Detach on GTP S2a

The procedure for HSS/AAA Initiated Detach from TWAN is represented in Figure 16.3.1.2-1 and described below.

This procedure applies to the transparent single-connection mode and the single-connection mode.

This procedure applies to the Non-Roaming, Home Routed Roaming and Local Breakout cases. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF. In the Home Routed Roaming and LBO cases, the 3GPP AAA Proxy serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN. In the non-roaming and Home Routed Roaming case, the vPCRF is not involved at all.

1) The HSS/AAA sends a Session Termination Request message to the TWAN to detach a specific UE.

2) The step 2 to 6 of the UE/TWAN Initiated Detach procedure described in clause 16.3.1.1 are followed.

3) TWAN sends a Session Termination Response message to 3GPP AAA Server. If the detach procedure was initiated from the 3GPP AAA Server and if the UE no longer has any context in the 3GPP AAA Server, the 3GPP AAA Server communicates the HSS as described in clause 12.1.2. If the detach procedure was initiated by HSS, the 3GPP AAA Server replies to the HSS as described in clause 12.1.3.

NOTE: The HSS/AAA may also send a detach indication message to the PDN GW. The PDN GW does not remove the GTP tunnels on S2a, since the TWAN is responsible for removing the GTP tunnels on S2a. The PDN GW acknowledges the receipt of the detach indication message to the 3GPP AAA Server.

16.3.2 Detach and PDN disconnection in WLAN on PMIP S2a

16.3.2.1 UE/TWAN Initiated Detach and UE/TWAN requested PDN Disconnection Procedure in WLAN on PMIP S2a

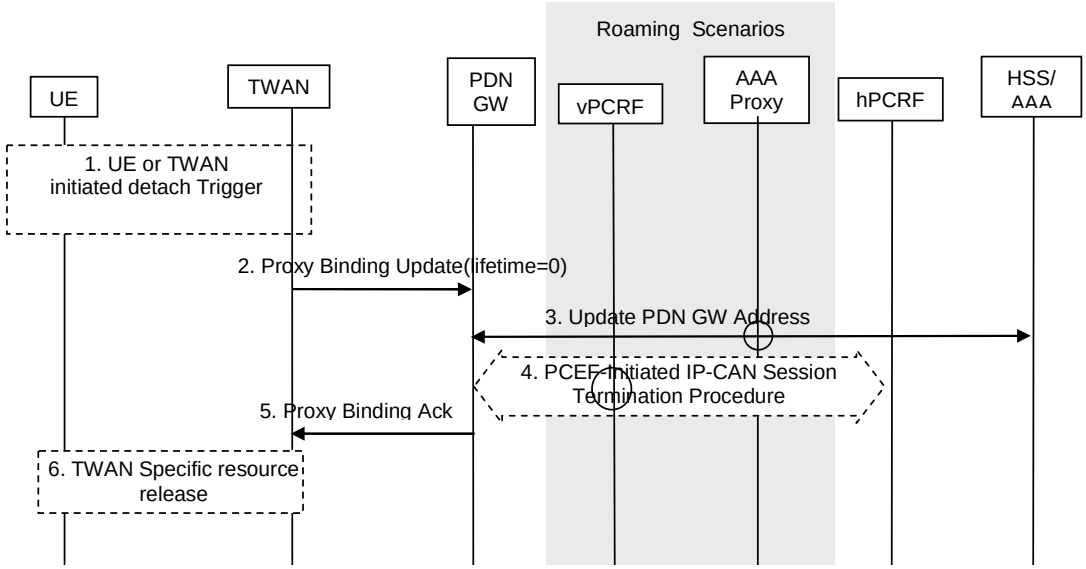


Figure 16.3.2.1-1: UE/TWAN Initiated Detach and UE/ TWAN requested PDN Disconnection on PMIP S2a

The procedure is similar to GTP based S2a call flows in clause 16.3.1.1, with the following differences:

- Step 2 is a Proxy Binding Update. The details of the Proxy Binding Update message are described in step 3 in clause 6.4.1.1. Additionally, the Proxy Binding Update includes the current TWAN Identifier as described in clause 16.1.7, the Timestamp of this TWAN-Identifier and the UE Time Zone.

- Step 5 is a Proxy Binding Acknowledgement. The details of the Proxy Binding Acknowledgement message are described in step 6 in clause 6.4.1.1.

16.3.2.2 HSS/AAA Initiated Detach Procedure in WLAN on PMIP S2a

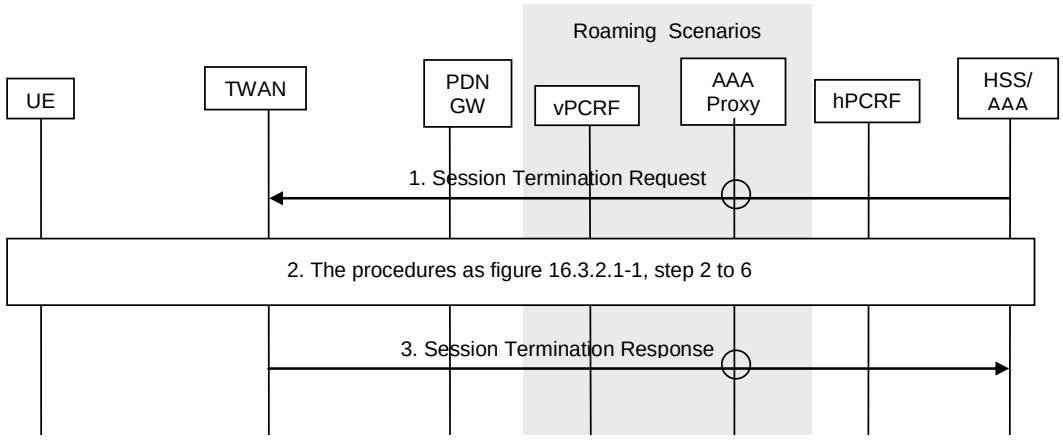


Figure 16.3.2.2-1: HSS/AAA Initiated Detach on PMIP S2a

The procedure is similar to GTP S2a call flow in clause 16.3.1.2, the difference is that step 2 refers to figure 16.3.2.1-1.

NOTE: The HSS/AAA may also send a detach indication message to the PDN GW. The PDN GW does not remove the PMIP tunnels on S2a, since the TWAN is responsible for removing the PMIP tunnels on S2a. The PDN GW acknowledges the receipt of the detach indication message to the 3GPP AAA Server.

16.4 PDN GW initiated Resource Allocation Deactivation in WLAN on S2a

16.4.1 PDN GW initiated Resource Allocation Deactivation in WLAN on GTP S2a

This procedure depicted in figure 16.4.1-1 can be used to deactivate an S2a dedicated bearer or deactivate all S2a bearers belonging to a PDN address, for e.g., due to IP-CAN session modification requests from the PCRF. If the default S2a bearer belonging to a PDN connection is deactivated, the PDN GW deactivates all S2a bearers belonging to the PDN connection.

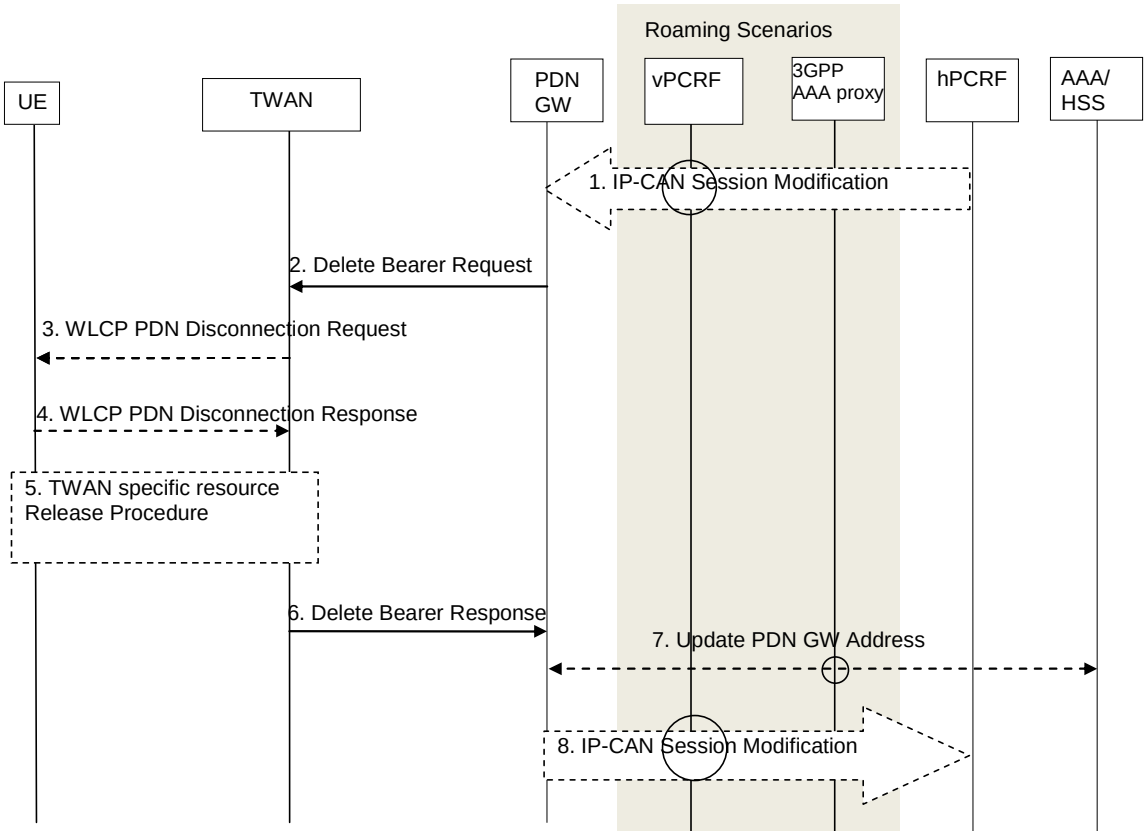


Figure 16.4.1-1: PDN GW Initiated Bearer Deactivation with GTP on S2a

This procedure applies to the Non-Roaming, Roaming and Local Breakout cases. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF. In the non-roaming and home routed roaming cases, the vPCRF is not involved at all.

The optional interaction steps between the PDN GW and the PCRF in the procedures in figure 16.4.1-1 only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured within the PDN GW.

1. If dynamic PCC is deployed, the PDN GW initiated Bearer Deactivation procedure may for example be triggered due to 'IP-CAN session Modification procedure', as defined in TS 23.203 [19]. In this case, the resources associated with the PDN connection in the PDN GW are released. If requested by the Application Function (e.g. P-CSCF), the PCRF may also include a request to provide the User Location Info and/or the Time zone to the PDN GW.

2. The PDN GW sends a Delete Bearer Request message (EPS Bearer Identity, Cause) to the TWAN. This message can include an indication that all bearers belonging to that PDN connection shall be released.

Steps 3-4 only apply in multi-connection mode:

3. In multi-connection mode, if all bearers belonging to a PDN connection are released, then the UE is informed of the PDN connection release by means of a WLCP PDN Disconnection Request (PDN Connection ID).

4. The UE acknowledges the disconnection request received in step 3.

5. If supported by the TWAN, the TWAN specific resources may be released in the TWAN. The details of this step are out of the scope of 3GPP.

6. The TWAN deletes the bearer contexts related to the Delete Bearer Request, and acknowledges the bearer deactivation to the PDN GW by sending a Delete Bearer Response (EPS Bearer Identity) message. Additionally, the Delete Bearer Response includes the TWAN Identifier as described in clause 16.1.7, the Timestamp of this TWAN-Identifier and the UE Time Zone.

7. In the case where the resources corresponding to the PDN connection are released in PDN GW, the PDN GW informs the 3GPP AAA Server/HSS of the PDN disconnection.

8. The PDN GW deletes the bearer context related to the deactivated S2a bearer. If the dedicated bearer deactivation procedure was triggered by receiving a PCC decision message from the PCRF, the PDN GW indicates to the PCRF whether the requested PCC decision was successfully enforced by completing the PCRF-initiated IP-CAN Session Modification procedure or the PCEF initiated IP-CAN Session Modification procedure as defined in TS 23.203 [19], proceeding after the completion of IP-CAN bearer signalling. If requested by the PCRF in step 1, the PDN GW provides the User Location Information, that contains the TWAN Identifier and/or UE Time Zone that will be forwarded to the Application Function as defined in TS 23.203 [19].

16.4.2 PDN GW initiated Resource Allocation Deactivation in WLAN on PMIP S2a

The procedure is similar to GTP based S2a call flows in clause 16.4.1 when the resources corresponding to the PDN connection is released, with the following differences:

- Step 2 is a Binding Revocation Request. The details of the Binding Revocation message are described in step 2 in clause 6.12.1.

- Step 6 is a Binding Revocation Acknowledgement. The details of the Binding Revocation Acknowledgement message are described in step 5 in clause 6.12.1. Additionally, the Binding Revocation Acknowledgement includes the current TWAN Identifier as described in clause 16.1.7, the Timestamp of this TWAN-Identifier and the UE Time Zone.

16.5 Dedicated bearer activation in WLAN on GTP S2a

The dedicated bearer activation procedure for GTP based S2a is depicted in figure 16.5-1.

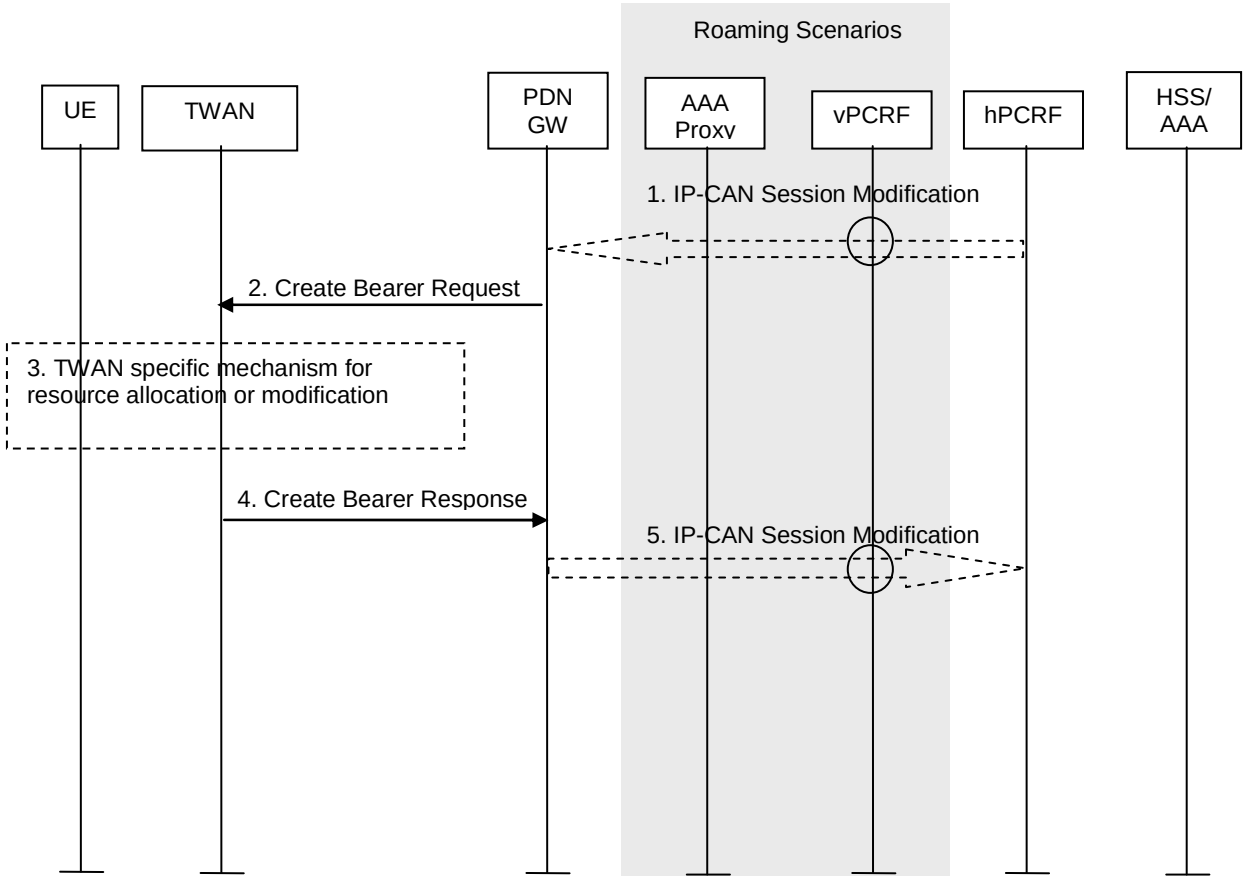


Figure 16.5-1: Dedicated S2a Bearer Activation Procedure with GTP on S2a

1. If dynamic PCC is deployed, the PCRF sends a PCC decision provision (QoS policy) message to the PDN GW. If the Application Function (e.g. P-CSCF) requests it, the PCRF may also include a request to provide the User Location Info and/or the Time zone. This corresponds to the initial steps of the PCRF-Initiated IP-CAN Session Modification procedure or to the PCRF response in the PCEF initiated IP-CAN Session Modification procedure as defined in TS 23.203 [19], up to the point that the PDN GW requests IP-CAN Bearer Signalling. If dynamic PCC is not deployed, the PDN GW may apply local QoS policy.

2. The PDN GW uses this QoS policy to assign the S2a bearer QoS, i.e., it assigns the values to the bearer level QoS parameters QCI, ARP, GBR and MBR. If this dedicated bearer is created as part of the handover from 3GPP access with GTP-based S5/S8, then the PDN GW applies the Charging ID already in use for the corresponding dedicated bearer while the UE was in 3GPP access (i.e. bearer with the same QCI and ARP as in 3GPP access). Otherwise, the PDN GW generates a new Charging ID for the dedicated bearer. The PDN GW sends a Create Bearer Request message (IMSI, EPS bearer QoS, TFT, PDN GW Address for the user plane, PDN GW TEID of the user plane, Charging Id, LBI) to the trusted WLAN access network. The Linked EPS bearer Identity (LBI) is the EPS bearer Identity of the default bearer.

3. A TWAN specific resource allocation/modification procedure may be executed in this step. The details of this step are out of the scope of 3GPP.

4. The TWAN selects an EPS bearer Identity, which has not yet been assigned to the UE. The TWAN then stores the EPS bearer Identity and links the dedicated bearer to the default bearer indicated by the Linked Bearer Identity (LBI). The TWAN uses the uplink packet filter (UL TFT) to determine the mapping of uplink traffic flows to the S2a bearer. The TWAN then acknowledges the S2a bearer activation to the PGW by sending a Create Bearer Response (EPS bearer Identity, TWAN Address for the user plane, TWAN TEID of the user plane) message. Additionally, the Create Bearer Response includes the current TWAN Identifier as described in clause 16.1.7 and the UE Time Zone.

5. If the dedicated bearer activation procedure was triggered by a PCC Decision Provision message from the PCRF, the PDN GW indicates to the PCRF whether the requested PCC decision (QoS policy) could be enforced or not, allowing the completion of the PCRF-Initiated IP-CAN Session Modification procedure or the PCEF initiated IP-CAN Session Modification procedure as defined in TS 23.203 [19], after the completion of IP-CAN bearer

signalling. If requested by the PCRF in step 1, the PDN GW provides the User Location Information that contains the TWAN identifier and/or UE Time Zone that will be forwarded to the Application Function as defined in TS 23.203 [19].

16.6 Network-initiated bearer modification in WLAN on GTP S2a

16.6.1 PDN GW Initiated Bearer Modification

The PDN GW initiated bearer modification procedure for a GTP based S2a is depicted in figure 16.6.1-1. This procedure is used to update the TFT for an active default or dedicated S2a bearer, or in cases when one or several of the S2a bearer QoS parameters QCI, GBR, MBR or ARP are modified (including the QCI or the ARP of the default S2a bearer e.g. due to the HSS Initiated Subscribed QoS Modification procedure, as described in clause 16.6.2).

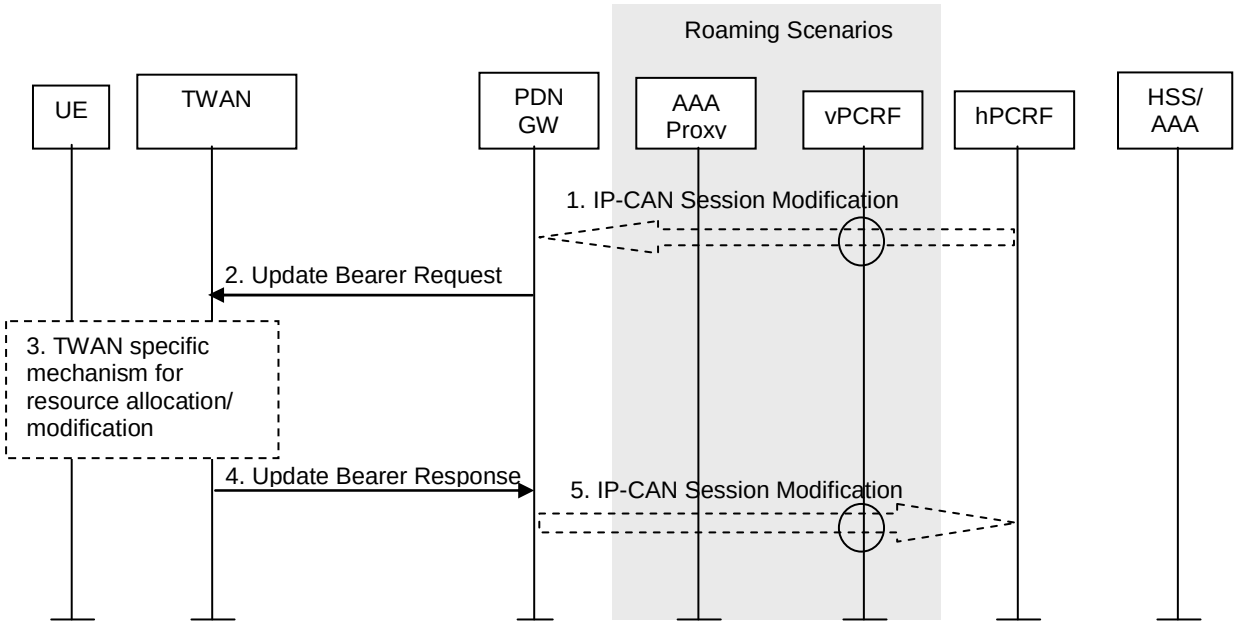


Figure 16.6.1-1: PDN GW-initiated S2a Bearer Modification Procedure with GTP on S2a

1. If dynamic PCC is deployed, the PCRF sends a PCC decision provision (QoS policy) message to the PDN GW. If the Application Function (e.g. P-CSCF) requests it, the PCRF may also include a request to provide the User Location Information and/or the Time zone. This corresponds to the initial steps of the PCRF-Initiated IP-CAN Session Modification procedure or to the PCRF response in the PCEF initiated IP-CAN Session Modification procedure as defined in 3GPP TS 23.203 [19], up to the point that the PDN GW requests IP-CAN Bearer Signalling. If dynamic PCC is not deployed, the PDN GW may apply local QoS policy.

2. The PDN GW uses this QoS policy to determine that a service data flow shall be aggregated to or removed from an active S2a bearer or that the authorized QoS of a service data flow has changed. The PDN GW generates the TFT and updates the S2a bearer QoS to match the traffic flow aggregate. The PDN GW then sends the Update Bearer Request (EPS bearer Identity, EPS bearer QoS, TFT) message to the trusted WLAN access network.

3. A TWAN specific resource allocation/modification procedure may be executed in this step. The details of this step are out of the scope of 3GPP.

4. The TWAN uses the uplink packet filter (UL TFT) to determine the mapping of traffic flows to the S2a bearer and acknowledges the S2a bearer modification to the PGW by sending an Update Bearer Response (EPS bearer Identity) message. Additionally, the Update Bearer Response includes the current TWAN Identifier as described in clause 16.1.7 and the UE Time Zone.

5. If the Bearer modification procedure was triggered by a PCC Decision Provision message from the PCRF, the PDN GW indicates to the PCRF whether the requested PCC decision (QoS policy) could be enforced or not by sending a Provision Ack message allowing the completion of the PCRF-Initiated IP-CAN Session Modification procedure or the PCEF initiated IP-CAN Session Modification procedure as defined in TS 23.203 [19], after the completion of IP-CAN bearer signalling. If requested by the PCRF in step1, the PDN GW provides the User

Location Information that contains the TWAN identifier and/or UE Time Zone that will be forwarded to the Application Function as defined in TS 23.203 [19].

16.6.2 HSS Initiated Bearer Modification

The HSS Initiated Subscribed QoS Modification for a GTP-based S2a is depicted in figure 16.6.2-1.

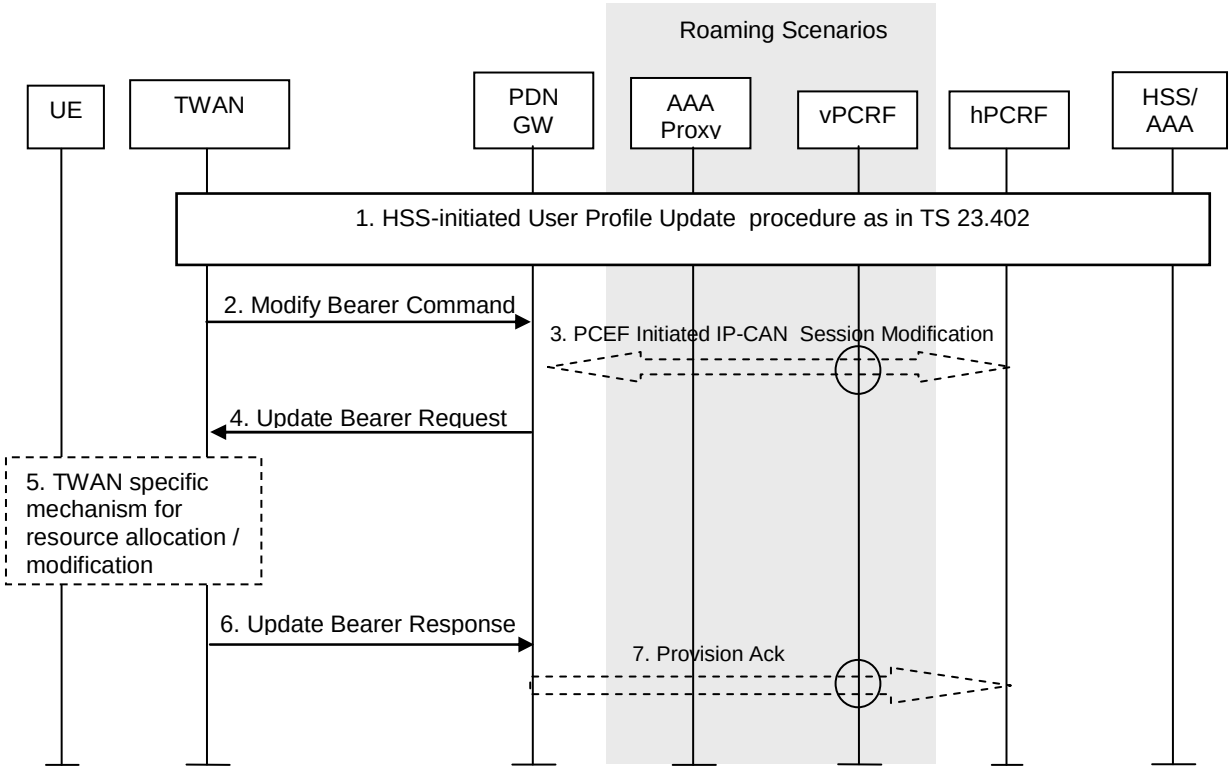


Figure 16.6.2-1: HSS Initiated Subscribed QoS Modification

1. The HSS updates the User Profile as specified in clause 12.2.1.

2. If the QCI and/or ARP and/or subscribed APN-AMBR has been modified and there is a related active PDN connection with the modified QoS Profile, the trusted WLAN access network sends the Modify Bearer Command (EPS bearer Identity, EPS bearer QoS, APN AMBR) message to the PDN GW. The EPS bearer Identity identifies the default bearer of the affected PDN connection. The EPS bearer QoS contains the EPS subscribed QoS profile to be updated.

3. If PCC infrastructure is deployed, the PDN GW informs the PCRF about the updated EPS bearer QoS. The PCRF sends the new updated PCC decision to the PDN GW. This corresponds to the PCEF-initiated IP-CAN Session Modification procedure as defined in TS 23.203 [19].

   The PCRF may modify the APN-AMBR and the QoS parameters (QCI and ARP) associated with the default bearer in the response to the PDN GW as defined in TS 23.203 [19].

4. The PDN GW modifies the default bearer of each PDN connection corresponding to the APN for which subscribed QoS has been modified. If the subscribed ARP parameter has been changed, the PDN GW shall also modify all dedicated S2a bearers having the previously subscribed ARP value unless superseded by PCRF decision. The PDN GW then sends the Update Bearer Request (EPS bearer Identity, EPS bearer QoS, TFT, APN AMBR) message to the TWAN.

5. A TWAN specific resource allocation/modification procedure may be executed in this step. The details of this step are out of the scope of 3GPP.

6. The TWAN acknowledges the bearer modification to the PDN GW by sending an Update Bearer Response (EPS bearer Identity) message. If the bearer modification fails the PDN GW deletes the concerned S2a Bearer.

7. The PDN GW indicates to the PCRF whether the requested PCC decision was enforced or not by sending a Provision Ack message.

16.7 Detach in WLAN on S2a for Multi-connection Mode

16.7.1 Detach in WLAN on GTP S2a

16.7.1.1 UE/TWAN Initiated Detach Procedure in WLAN on GTP S2a

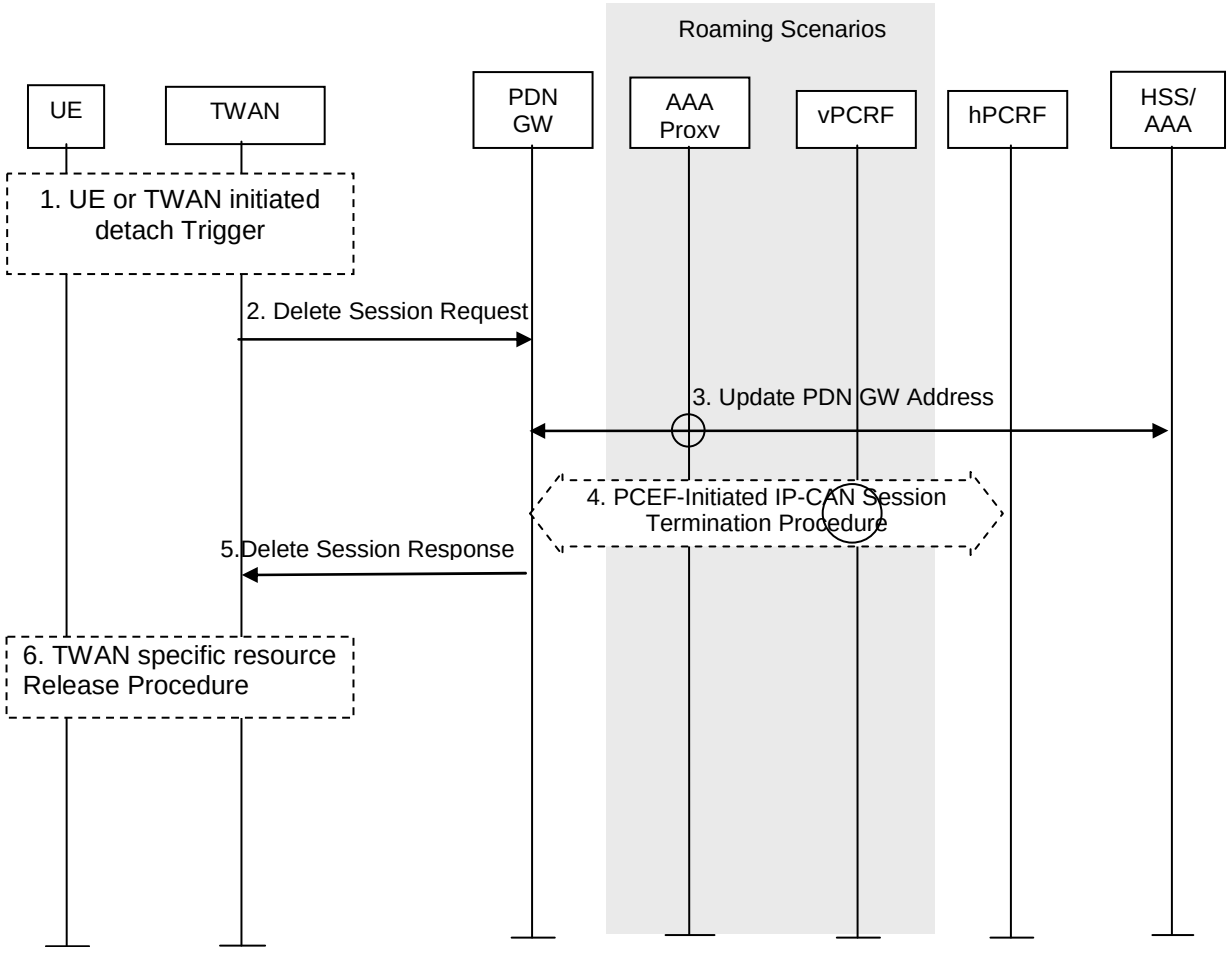


Figure 16.7.1.1-1: UE/TWAN-Initiated Detach in WLAN on GTP S2a

The procedure is similar to in clause 16.3.1.1, with the following differences:

- Step1: To detach from EPC, the UE can send a disassociation or deauthentication notification according to IEEE Std 802.11-2012 [64]. If there is no traffic received from the UE for a configurable duration and the TWAN detects the UE has left based on unanswered probes (e.g. ARP Request, Neighbor Solicitation message), the TWAN initiates the detach procedure.
- Step 2 to Step 5 refers to clause 16.9.1.
- In the case of connectivity with multiple PDNs, the steps 2 to 5 are repeated for each PDN the UE is connected to.

16.7.1.2 HSS/AAA Initiated Detach Procedure in WLAN on GTP S2a

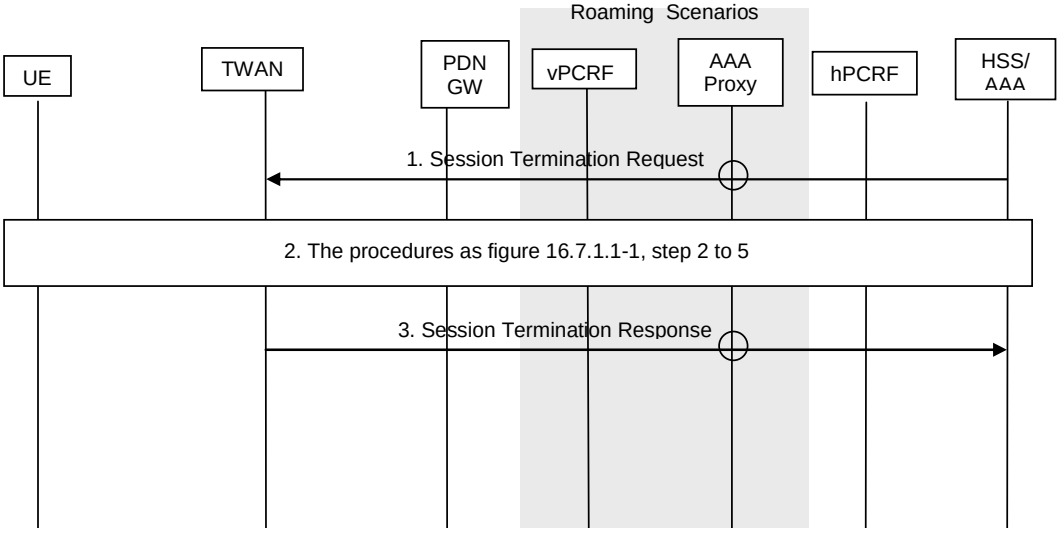


Figure 16.7.1.2-1: HSS/AAA-Initiated Detach in WLAN on GTP S2a

The procedure is similar to in clause 16.3.1.2, with the following differences:

- Step 2 refers to Figure 16.7.1.1-1.

16.7.2 Detach in WLAN on PMIP S2a

16.7.2.1 UE/TWAN Initiated Detach Procedure in WLAN on PMIP S2a

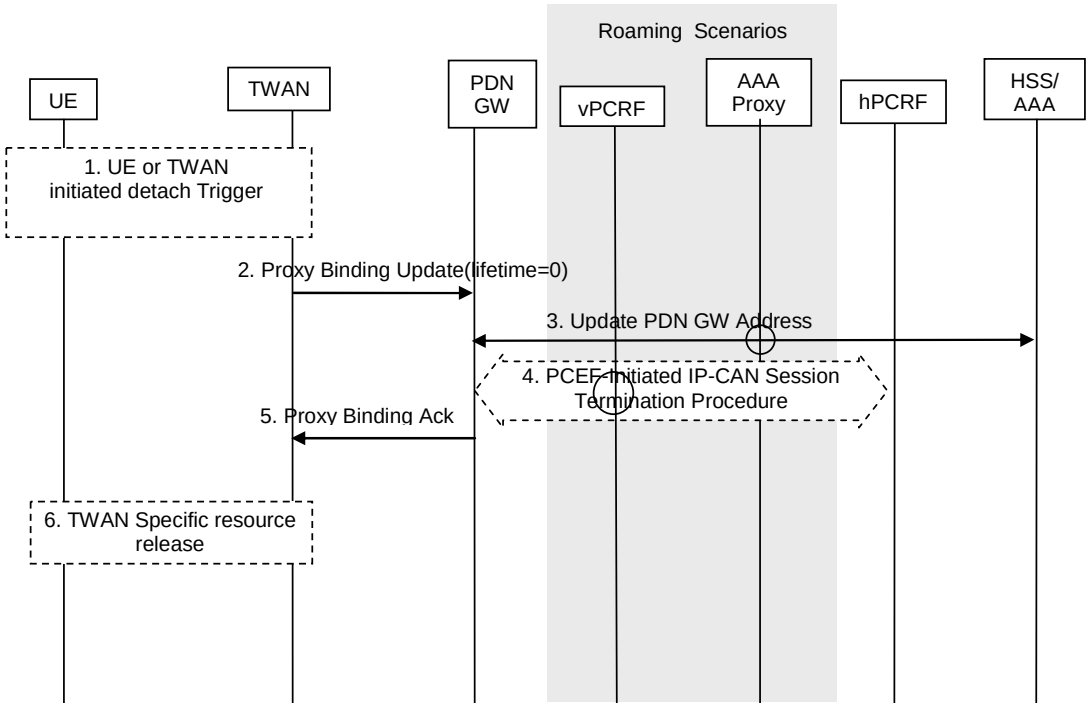


Figure 16.7.2.1-1: UE/TWAN Initiated Detach in WLAN on PMIP S2a

The procedure is similar to GTP based S2a call flows in clause 16.7.1.1, with the following differences:

- Step 2 is a Proxy Binding Update. The details of the Proxy Binding Update message are described in step 3 in clause 6.4.1.1. Additionally, the Proxy Binding Update includes the current TWAN Identifier as described in clause 16.1.7, the Timestamp of this TWAN-Identifier and the UE Time Zone.

- Step 5 is a Proxy Binding Acknowledgement. The details of the Proxy Binding Acknowledgement message are described in step 6 in clause 6.4.1.1.

16.7.2.2 HSS/AAA Initiated Detach Procedure in WLAN on PMIP S2a

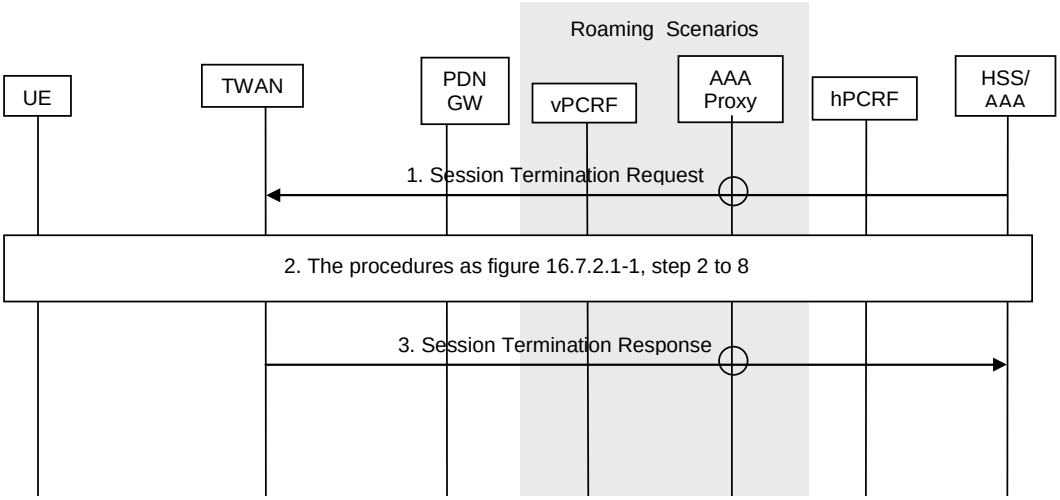


Figure 16.7.2.2-1: HSS/AAA Initiated Detach in WLAN on PMIP S2a

The procedure is similar to GTP S2a call flow in clause 16.3.1.2, the difference is that step 2 refers to figure 16.7.2.1-1.

NOTE: The HSS/AAA may also send a detach indication message to the PDN GW. The PDN GW does not remove the PMIP tunnels on S2a, since the TWAN is responsible for removing the PMIP tunnels on S2a. The PDN GW acknowledges the receipt of the detach indication message to the 3GPP AAA Server.

16.8 UE Initiated PDN connectivity request procedure in WLAN on S2a for Multi-connection Mode

16.8.1 Supporting GTP S2a

When the UE is connected to a trusted WLAN and the multi-connection mode has been selected (as described in clause 16.2.1), the UE may use the PDN connectivity request procedure specified below in order to establish a PDN connection over the connected WLAN. This procedure is also used to request for connectivity to an additional PDN over a trusted WLAN with GTP on S2a when the UE is simultaneously connected to E-UTRAN and a trusted WLAN, and the UE already has active PDN connections over both the accesses.

There can be more than one PDN connection per APN when GTP is used between the TWAN and the PDN GW. During the establishment of a new PDN connection, the TWAN allocates and sends a default EPS bearer ID to the PDN GW. The default EPS bearer ID is unique in the scope of the UE within a TWAG, i.e. the IMSI and the default EPS bearer ID togther identify a PDN connection within a TWAG. In order to be able to identify a specific established PDN connection, both the TWAG and the PDN GW shall store the default EPS bearer ID.

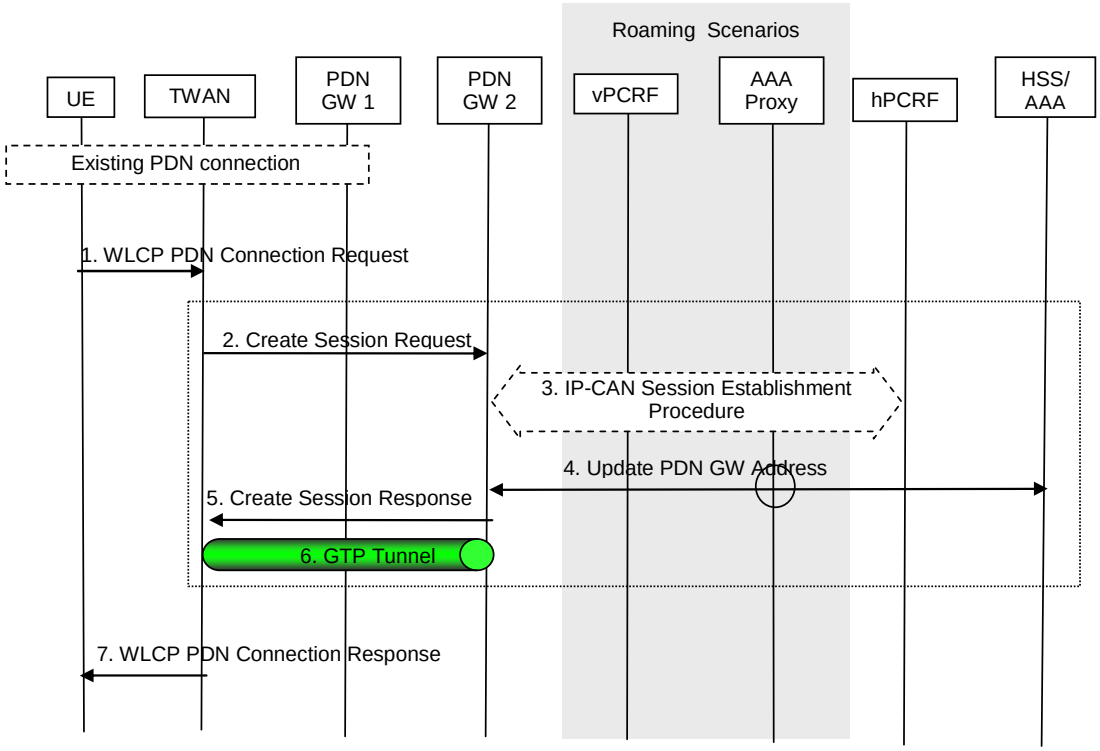


Figure 16.8.1-1: UE-Initiated Connectivity to PDN in WLAN on GTP S2a

This procedure applies to the Non-Roaming, Home Routed Roaming and Local Breakout cases. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF. In the Home Routed Roaming and LBO cases, the 3GPP AAA Proxy serves as an intermediary between the Trusted Non-3GPP IP Access and the 3GPP AAA Server in the HPLMN. In the non-roaming and Home Routed Roaming case, the vPCRF is not involved at all.

If dynamic policy provisioning is not deployed, the optional steps of interaction between the PDN GW and PCRF do not occur.

1. The UE sends a WLCP PDN Connection Request (APN, PDN Type, Protocol Configuration Options, Request Type) to the TWAN. The UE sends the WLCP PDN Connection Request to the control plane address of TWAN it received during EAP authentication and authorization procedure as described in clause 16.2.1. The Request Type indicates "initial request" when the UE requests new PDN connection over the WLAN access network. The UE may indicate the requested APN. If the UE does not indicate an APN, then the default APN will be used in the following steps. The Protocol Configuration Options (PCO) may be sent to transfer parameters to the PDN GW, and is sent transparently through the TWAN.

2-6. Step 2 to Step 6 are described as Step 3 to Step 7 in clause 16.2.1.

7. The TWAN returns a WLCP PDN Connection Response (APN, PDN Type, PDN Address, PDN Connection ID, User Plane Connection ID, Protocol Configuration Options) message to the UE to acknowledge the establishment of a new point-to-point link between the UE and the TWAG. The User Plane Connection ID is the MAC address of the TWAN which is used by the UE and the TWAN for encapsulating user plane packets for this PDN connection. If the UE did not indicate the APN in the WLCP PDN Connection Request, then the response indicates the APN selected by the network (e.g. the default APN). The PDN Connection ID is stored in the TWAN to associate the established point-to-point link between the UE and TWAG with all the S2a bearers for this PDN connection. The PDN Connection ID is sent to and stored in the UE to identify this new established PDN connection. The UE will use this PDN Connection ID in subsequent procedures, such as PDN disconnection procedure.

   If the IPv6 prefix is allocated, a Router Advertisement with the IPv6 prefix is sent to the UE after step 7. The UE may perform additional IP layer configuration as per standard IETF procedures, e.g. IPv6 Stateless Address Autoconfiguration according to IETF RFC 4862 [58], and Stateless DHCPv6 according to IETF RFC 3736 [30].

16.8.2 Supporting PMIP S2a

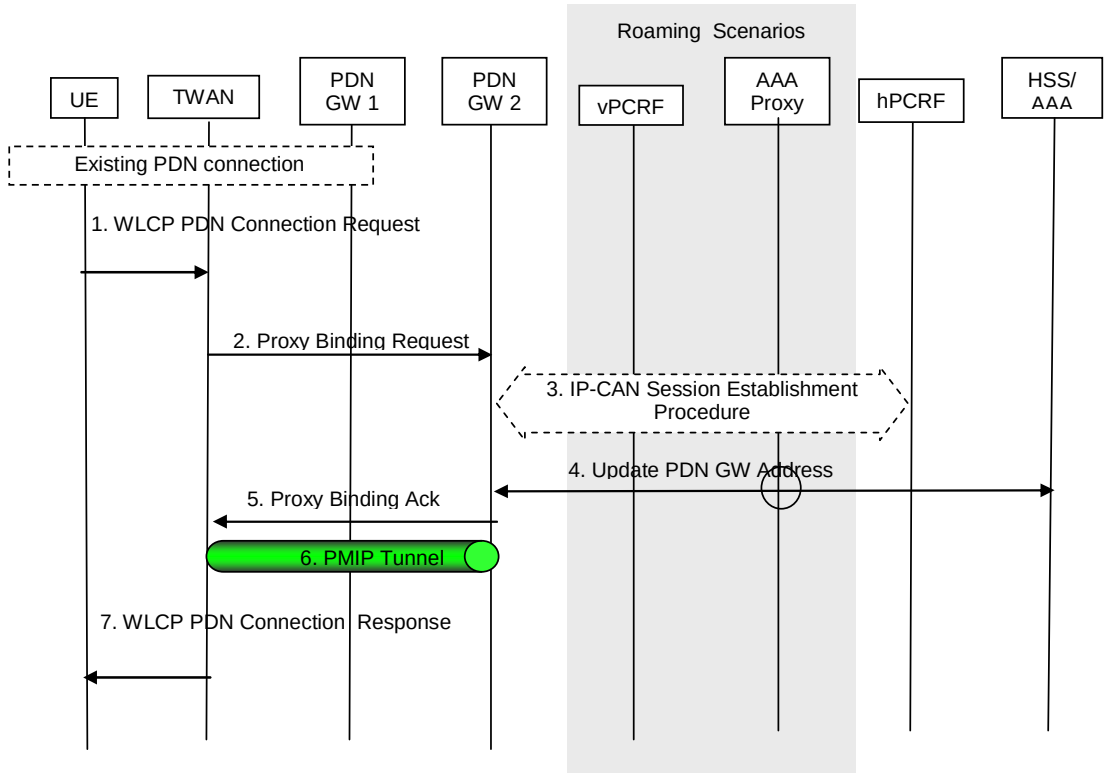


Figure 16.8.2-1: UE-Initiated Connectivity to PDN in WLAN on PMIP S2a

When the UE is connected to a trusted WLAN and the multi-connection mode has been selected (as described in clause 16.2.2), the UE may use the PDN connectivity request procedure in order to establish a PDN connection over the connected WLAN. This procedure is also used to request for connectivity to an additional PDN over a trusted WLAN with PMIPv6 on S2a when the UE is simultaneously connected to E-UTRAN and a trusted WLAN, and the UE already has active PDN connections over both the accesses.

The procedure is similar to GTP based S2a call flows in clause 16.8.1 with the following differences:

- Step 2 is a Proxy Binding Update as described in Step 3 in clause 16.2.2.
- Step 5 is a Proxy Binding Acknowledgement as described in Step 6 in clause 16.2.2.

16.9 UE/TWAN Initiated PDN disconnection for Multi-connection Mode

16.9.1 Supporting GTP S2a

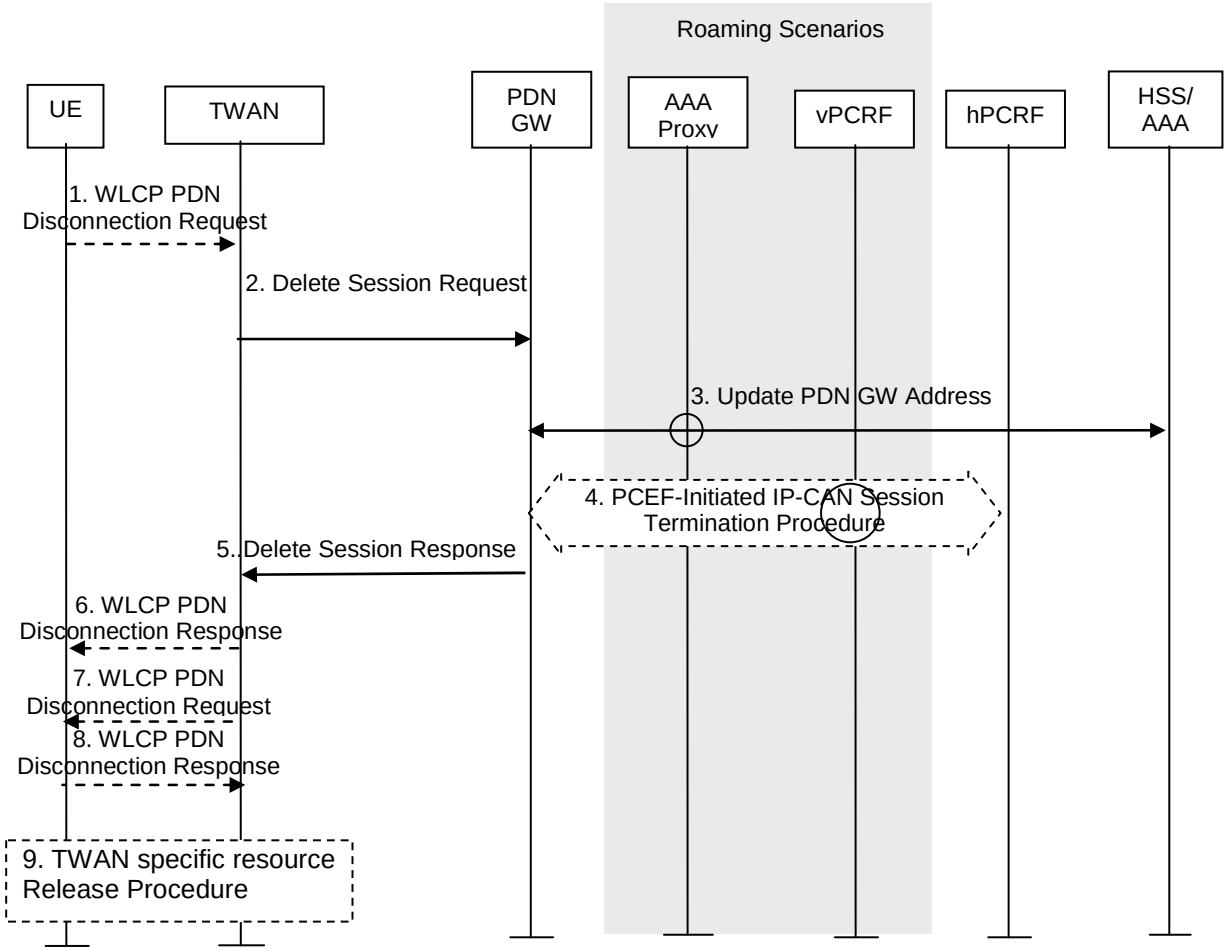


Figure 16.9.1-1: UE/TWAN requested PDN disconnection procedure in WLAN on GTP S2a for Multi-Connection Mode

This procedure applies to the Non-Roaming, Roaming with home routed and romaing with local breakout. In the Local Breakout case, the vPCRF forwards messages between the PDN GW and the hPCRF. In the LBO cases, the 3GPP AAA Proxy serves as an intermediary between the Trusted WLAN Access and the 3GPP AAA Server in the HPLMN. In the non-roaming and Home Routed Roaming case, the vPCRF is not involved at all.

If dynamic policy provisioning is not deployed, the optional steps of interaction between the PDN GW and PCRF do not occur.

1. If the PDN disconnection is initiated by the UE, the UE sends a WLCP PDN Disconnection Request containing a PDN Connection ID to the TWAG.

2-5. Steps 2-5 are the same as steps 2-5 in clause 16.3.1.1.

6. If the PDN disconnection was initiated by the UE in step 1, then the UE is informed of the disconnection by means of a WLCP PDN Disconnection Response.

7. If the PDN disconnection was initiated by the TWAG, then the UE is informed of the disconnection by means of a WLCP PDN Disconnection Request containing the PDN Connection ID.

NOTE 1: Steps 2-5 and Steps 7-8 may occur in parallel.

8. The UE acknowledges the disconnection request received in step 7.
9. The TWAN specific reousces belonging to the PDN connection are released with a method which is out of 3GPP scope.

NOTE 2: Either step 1 and 6, or step 7 and 8, are performed

16.9.2 Supporting PMIP S2a

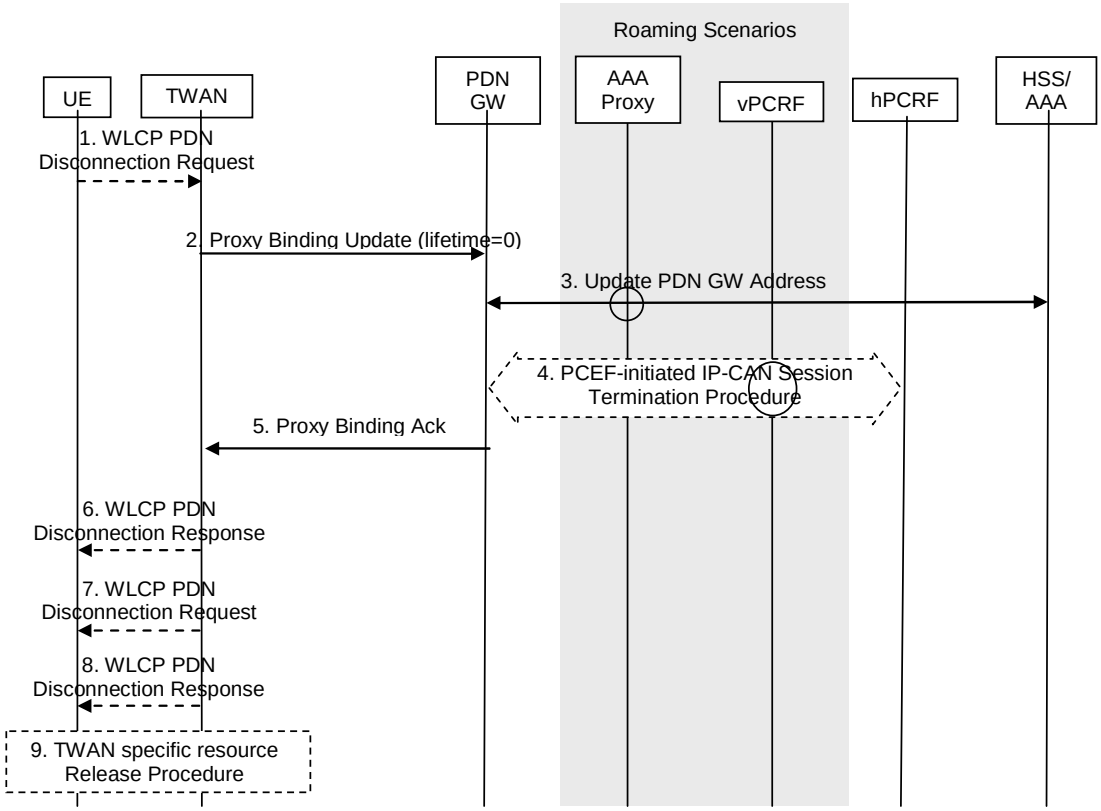


Figure 16.9.2-1: UE/TWAN requested PDN disconnection in WLAN on PMIP S2a for Multi-connection Mode

The procedure is similar to GTP based S2a call flows in clause 16.9.1 with the following differences:

- Step 2 is a Proxy Binding Update (lifetime=0) for the PDN connection to be deleted sent by TWAN to the PDN GW. The details of the Proxy Binding Update message are described in step3 in clause 6.4.1.1. Additionally, the Proxy Binding Update includes the current TWAN Identifier as described in clause 16.1.7, the Timestamp of this TWAN-Identifier and the UE Time Zone.
- Step 5 is a Proxy Binding Acknowledgement sent by the PDN GW to TWAN. The details of the Proxy Binding Acknowledgement message are described in step6 in clause 6.4.1.1.

16.10 Handover procedure from 3GPP access to WLAN on S2a

16.10.1 Handover procedure from 3GPP access to WLAN on S2a in single-connection mode

16.10.1.1 Handover in single-connection mode from 3GPP access to WLAN on GTP S2a

This procedure is used in the single-connection mode to hand over a single PDN Connection from 3GPP access to WLAN. The decision to use the single-connection mode is made during authentication as described in clause 16.2.

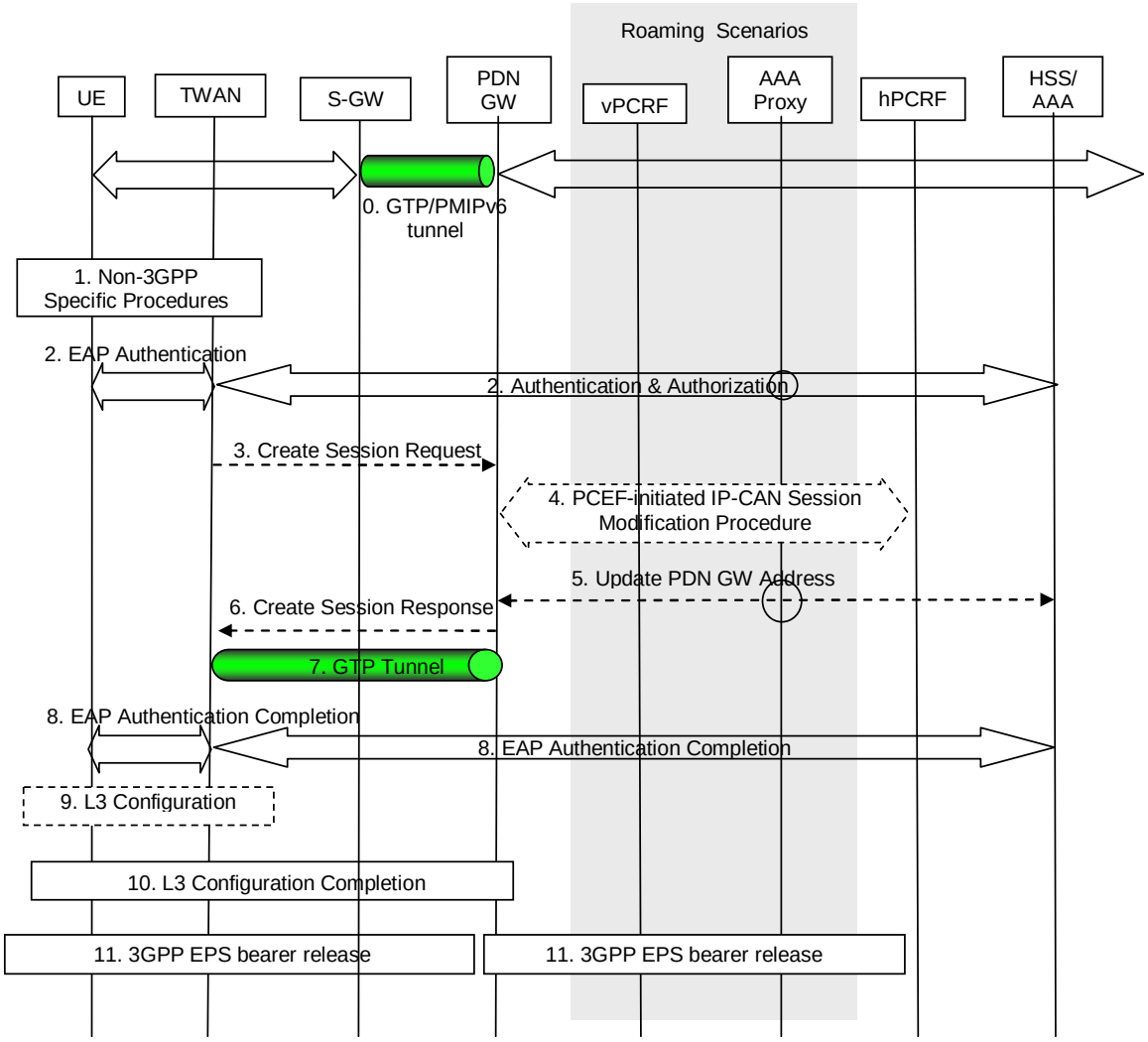


Figure 16.10.1.1-1: Handover in single-connection mode from 3GPP access to Trusted WLAN on GTP S2a for roaming and non-roaming scenarios

The home routed roaming, LBO and non-roaming scenarios are depicted in the figure 16.2.1-1:

- In the LBO case, the 3GPP AAA Proxy acts as an intermediary, forwarding messages from the 3GPP AAA Server in the HPLMN to the PDN GW in the VPLMN and vice versa. Messages between the PDN GW in the VPLMN and the hPCRF in the HPLMN are forwarded by the vPCRF in the VPLMN.

- In the home routed roaming and non-roaming cases, the vPCRF is not involved, except for the authentication and authorization in step 2.

- In the non-roaming cases, the 3GPP AAA Proxy is not involved. In home routed roaming case, the 3GPP AAA Proxy is not involved in step 5.

The steps in figure 16.10.1-1 are based on figure 16.2.1-1, with the following changes:

- Step 0. The UE is connected in the 3GPP Access and has a PMIPv6 or GTP tunnel on the S5/S8 interface.

- Step 2. This step is the same as step 2 in 16.2.1 with the following addition: If the UE indicates single-connection, then the UE indicates also handover via EAP-AKA' to 3GPP AAA.

- Step 3. This step is the same Aas step 3 in 16.2.1 with the following addition: The handover indication is set in the Create Session Request to allow the PDN GW to re-allocate the same IP address or prefix that was assigned to the UE while it was connected to the 3GPP access and to initiate a PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF.

- Step 4. The PDN GW executes a PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19]. The Event Report indicates the change in Access Type.

  If the PDN GW decides to allocate a new IP address/prefix instead of preserving the old IP address/prefix, as described in clause 4.1.3.2.3, the PDN GW executes an IP-CAN session Establishment Procedure with the PCRF instead of a PCEF-Initiated IP-CAN Session Modification Procedure.

- Step 6. The PDN GW responds with a Create Session Response (PDN GW Address for the user plane, PDN GW TEID of the user plane, PDN GW TEID of the control plane, PDN Type, PDN Address, EPS Bearer Identity, EPS Bearer QoS, APN-AMBR, Charging ID, Cause). The Create Session Response contains the IP address and/or the prefix that was assigned to the UE while it was connected to the 3GPP IP access. The Charging Id provided by the PGW is the Charging Id previously assigned to the default bearer of the PDN connection in the 3GPP access.

  Depending upon the active PCC rules, the PDN GW may create dedicated bearers on S2a interface. And in that case, it applies the Charging ID previously in use for the corresponding dedicated bearer(s) while the UE was connected to the 3GPP IP access (i.e. bearer with the same QCI and ARP as in 3GPP access).

- Step 10: This step is the same as step 15 in 16.2.1.

- Step 11. The PDN GW shall initiate the PDN GW Initiated PDN Disconnection procedure in 3GPP access as defined in clause 5.6.2.2 or the PDN GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [4], clause 5.4.4.1.

16.10.1.2 Handover in single-connection mode from 3GPP access to WLAN on PMIP S2a

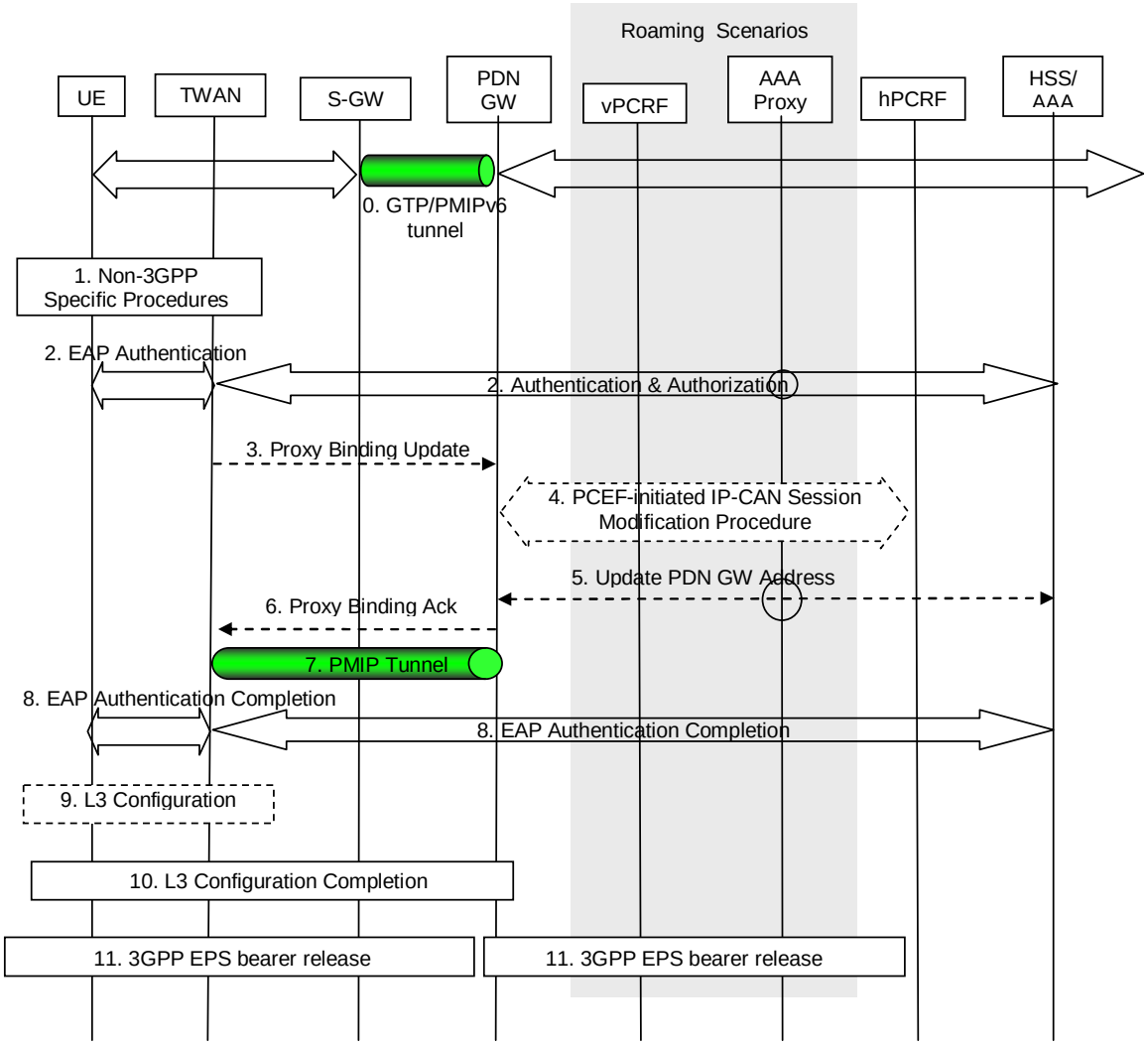


Figure 16.10.1.2-1: Handover in single-connection mode from 3GPP access to Trusted WLAN on PMIP S2a for roaming and non-roaming scenarios

The procedure is based on clause 16.2.2 with the following differences:

- Step 0. The UE is connected in the 3GPP Access and has a PMIPv6 or GTP tunnel on the S5/S8 interface.
- Step 2. This step is the same as step 2 in 16.2.2 with the following addition: If the UE indicates single-connection, then the UE indicates also handover via EAP-AKA' to 3GPP AAA. If the UE requests a PDN type, and this PDN type is not possible, then the request is rejected with a relevant authorization failure.
- Step 3. This step is the same as step 3 in 16.2.2 with the following addition: The handover indicator is set in the Proxy Binding Update to allow the PDN GW to re-allocate the same IP address or prefix that was assigned to the UE while it was connected to the 3GPP access and to initiate a PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF.
- Step 4: The PDN GW executes a PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19]. The Event Report indicates the change in Access Type.
- Step 6: Tthe PDN GW sends a Proxy Binding Acknowledgement message. The details of the Proxy Binding Acknowledgement message are described in step 6 in clause 16.2.2. The Proxy Binding Acknowledgement message contains the IP address and/or the prefix that was assigned to the UE while it was connected to the 3GPP IP access.

- Step 10: This step is the same as step 15 in 16.2.2.

- Step 11. The PDN GW shall initiate the PDN GW Initiated PDN Disconnection procedure in 3GPP access as defined in clause 5.6.2.2 or the PDN GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [4], clause 5.4.4.1.

16.10.2 Handover procedure from 3GPP access to WLAN on S2a in multi-connection mode

16.10.2.1 Handover in multi-connection mode from 3GPP access to WLAN on GTP S2a

The following procedure is used to handover one or more PDN connections from 3GPP access to the Trusted WLAN.The steps involved in this procedure are depicted below for both the non-roaming and roaming cases. It is assumed that while the UE is served by the 3GPP access, PMIPv6 or GTP tunnel(s) are established between the Serving GW and the PDN GW in the EPC.

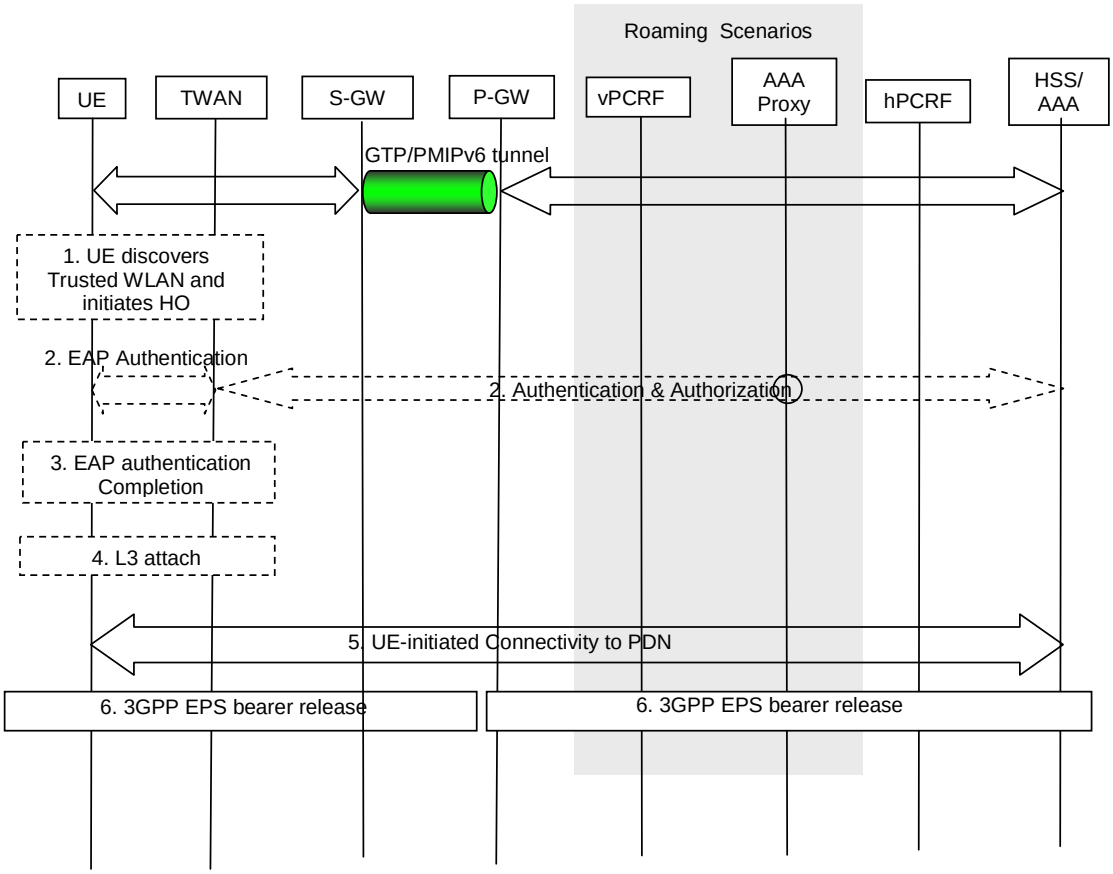


Figure 16.10.2.1-1: Handover from 3GPP access to Trusted WLAN on GTP S2a for roaming and non-roaming scenarios

In the Local Breakout case, the 3GPP AAA Proxy forwads messages from the 3GPP AAA Server in the HPLMN to the PDN GW in the VPLMN and vice versa. Messages between the PDN GW in the VPLMN and the hPCRF in the HPLMN are forwarded by the vPCRF in the VPLMN. In the home routed roaming and non-roaming cases, the vPCRF and the 3GPP AAA Proxy are not involved, except for the authentication and authorization in step 2.

For connectivity to multiple PDNs the following applies:

- If the UE is connected to both 3GPP access and TWAN before the handover of PDN connection(s) to Trusted WLAN is triggered, steps 1 to 4 shall be skipped and the UE shall only perform step 5 for each PDN connection that is being transferred from 3GPP access.

- If the UE is connected only to 3GPP access before the handover of PDN connection(s) to Trusted WLAN is triggered, steps 1 to 4 shall be performed. The UE shall then repeat step 5 for each of the PDN connections that is being transferred from 3GPP access.

- Step 6 shall be repeated for each PDN connection that is being transferred from 3GPP access.

Step 5 can occur in parallel for each PDN connection. Other impacts related to the handover for multiple PDNs are described in clause 8.1.

0. The UE is connected in the 3GPP access and has PMIPv6 or GTP tunnel(s) on the S5/S8 interface.

1. The UE discovers the trusted WLAN access and determines to transfer one or more of its active PDN connections from the currently used 3GPP access to the discovered trusted WLAN.

2. The UE performs access authentication and authorization in the trusted WLAN. This step is the same as step 2 of the initial attach procedure in clause 16.2.1, where in this case Multi-Connection Mode is requested by the UE.

3. TWAN sends EAP success to the UE and completing EAP authentication. This step is the same as step 8 of the initial attach procedure in clause 16.2.1.

4. If NSWO is authorized for the UE in step 2, anytime after step 3 the UE may send a L3 attach request to the TWAN for NSWO and receive the address or prefix of the NSWO from TWAN.

5. The UE performs UE-initiated connectivity request procedure for Multi-Connection Mode according to clause 16.8.1 with the following exception:

   a) The UE sends a PDN Connectivity Request message to the TWAN with Request Type indicating "Handover".

   b) The UE indicates the APN corresponding to the PDN connection which is being handed over to TWAN in the PDN Connectivity Request message. If the APN is not provided, and the subscription context from HSS/AAA contains a PDN GW identity and APN pair corresponding to the default APN, the TWAN uses the default APN.

   c) Upon receiving the PDN Connectivity Request message, the TWAN selects the PDN GW as indicated in the subscription data received from the 3GPP AAA Server and sends Create Session Request to the selected PDN GW. Since the Request Type is "Handover", a Handover Indication is included in the Create Session Request.

   d) Since it is a handover, the IP-CAN Session Establishment is not performed. The PDN GW may execute a PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19] to report e.g. change in IP-CAN type.

   NOTE: In case there are multiple PDN connections to the same APN the PDN connection is selected by the PDN GW as it is specified in clause 8.1

6. The PDN GW shall initiate the PDN GW Initiated PDN Disconnection procedure in 3GPP access as defined in clause 5.6.2.2 or the PDN GW Initiated Bearer Deactivation procedure as defined in TS 23.401 [4], clause 5.4.4.1.

Depending upon the active PCC rules, the PDN GW may create dedicated bearers on S2a interface. And in that case, it applies the Charging ID previously in use for the corresponding dedicated bearer(s) while the UE was connected to the 3GPP IP access (i.e. bearer with the same QCI and ARP as in 3GPP access).

16.10.2.2 Handover in multi-connection mode from 3GPP access to WLAN on PMIP S2a

This procedure is as in clause 16.10.2.1 with the following differences:

Step 5 c) Upon receiving the PDN Connection Request message, the TWAN selects the PDN GW as indicated in the subscription data received from the 3GPP AAA Server and sends the Proxy Binding Update to the selected PDN GW by setting the Handover Indicatior to indicate handoff between two different interfaces of the UE. The details of the messages and parameters to be used are described in Steps 6 and 8 in 8.2.2. Additionally, the Proxy Binding Update includes the current TWAN Identifier as described in clause 16.1.7 and the UE Time Zone.

16.11 Handover procedure from WLAN on S2a to 3GPP access

This procedure is as in clause 8.2.1.1 (GTP-based S5/S8 for E-UTRAN), clause 8.2.1.2 (PMIP-based S5/S8 for E-UTRAN), clause 8.2.1.3 (GTP-based S5/S8 for UTRAN/GERAN) and clause 8.2.1.4 (PMIP-based S5/S8 for GERAN/UTRAN) with the following differences:

- Step 1. There is a GTP or PMIP tunnel between TWAN and PGW.
- Step 18 in 8.2.1.1, step 19 in clause 8.2.1.2 and step 17 in clause 8.2.1.3. The PDN GW shall initiate resource allocation deactivation procedure in the TWAN as defined in clause 16.4.

For handovers from GTP-based S2a to GTP-based S5/S8 the following additional changes apply:

On step 9 of clause 8.2.1.1 and step 11 of 8.2.1.3: the Charging Id provided by the PGW to the default and dedicated bearers in 3GPP access is the Charging Id previously assigned to the corresponding default and dedicated bearers (i.e. bearer with the same QCI and ARP) of the PDN connection in the non-3GPP access on the S2a interface, although the Charging Id still applies to the non-3GPP access.

NOTE 1: For UTRAN/GERAN access, the dedicated bearer establishment does not take place along with the default bearer establishment (i.e. sending of Create Session Response message). For E-UTRAN access, depending upon the support of the piggybacking feature in the network, the dedicated bearer can be created as part of default bearer establishment or immediately afterwards.

On step 13 of clause 8.2.1.1 and step 14 of 8.2.1.3: the Charging Id previously in use for the default and dedicated bearers in the non-3GPP access on the S2a interface now applies to the corresponding default and dedicated bearers in 3GPP access (i.e. bearer with the same QCI and ARP as in non-3GPP access).

17 E-UTRAN-HRPD Inter-RAT SON Support

17.1 Architecture and Interface

17.1.1 Architecture for E-UTRAN-HRPD Inter-RAT SON Support

Support of E-UTRAN-HRPD Inter-RAT SON as specified in TS 36.413 [69] makes use of the RIM procedures described in clause 5.15 of TS 23.401 [4]. The architecture is depicted in figure 17.1-1. The interfaces used are the S1 and the S121 interfaces.

An eNodeB is addressed by the Target eNodeB Identifier. An HRPD Access Network is addressed by HRPD Sector ID as defined in TS 29.276 [70].

For messages transferred between E-UTRAN and HRPD Access Network, the source access network node sends a message to its MME including the source and destination addresses. The MME decides, which access network node to send the message to, based on the destination address.

The MME performs relaying between S1 and S121 messages as described in TS 36.413 [69] and TS 29.276 [70].

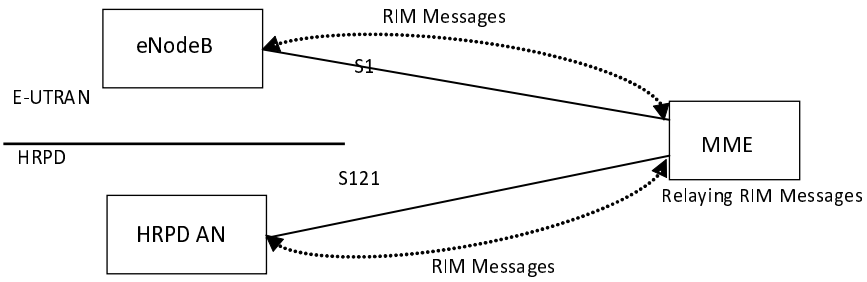


Figure 17.1-1: Basic Network Architecture for E-UTRAN-HRPD Inter-RAT SON Support

17.1.2 Reference Points

17.1.2.1 Reference Point List

S121: It enables interactions between E-UTRAN and HRPD access network to allow for the transfer of node level SON information.

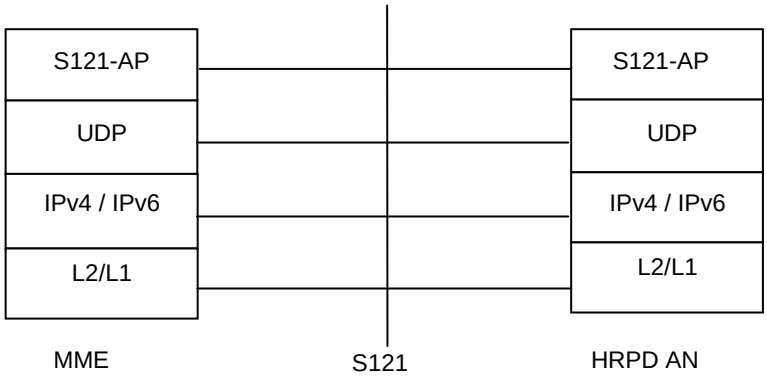
17.1.2.2 Requirements for the S121 interface

The S121 interface shall support the following requirements:

- SON information transferred between E-UTRAN and HRPD access network shall be transported as transparent containers without modifications by the MME.

17.1.2.3 S121 Protocol Stack

The figure below shows the protocol stack for the S121 interface.



Legend:
S121-AP: S121 Application Protocol is the Application Layer Protocol between the MME and HRPD AN. S121 Application Protocol (S121-AP) provides application layer reliability for its messages, if required.
UDP: User Datagram Protocol transfers messages. UDP is defined in RFC 768 [71].

Figure 17.1.2.3-1: Protocol Stack for S121 Reference Point

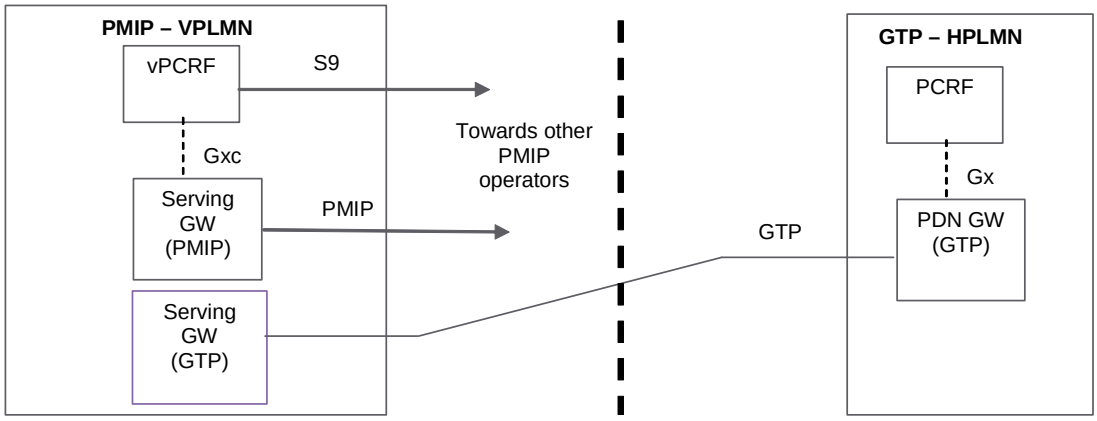
Annex A (informative): GTP - PMIP Roaming

The scenarios below identify and describe various deployment scenarios for interworking between EPC networks based on GTP and EPC networks based on PMIP. The scenario described here are the direct peering scenario and the proxy-based interworking.

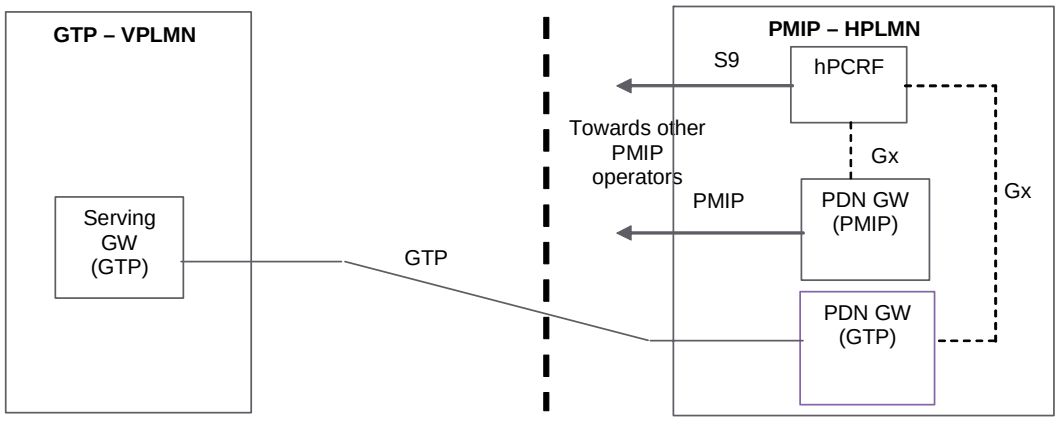
A.1 Direct Peering Scenario

The "direct peering" scenario consists in having one of the two roaming partners provide support for both variants of roaming flavour (e.g. a PMIP operator would support GTP-based roaming interface towards a GTP-only roaming partner, or vice versa) in order to make roaming possible.

The support for such roaming flavour can be provided either on the same GW node or on different GW nodes. Upon establishment of connectivity for a specific roaming UE, the Visited network chooses a GTP-based or a PMIP-based S8 interface (on the same GW node or on different GW nodes, note that for a single user only a single Serving GW is allocated when connecting to EPC), depending on the preferences of the roaming partner that owns the subscriber.



a) PMIP VPLMN – GTP HPLMN



b) GTP VPLMN – PMIP HPLMN

Figure A.1-1: Direct peering examples: a) PMIP-based VPLMN to GTP-based HPLMN; b) GTP-based VPLMN to PMIP-based HPLMN

Depicted in Figure A.1-1 (a) is an example of "direct peering" interworking between a GTP-based HPLMN and a PMIP-based VPLMN. When roamers whose subscription is owned by the GTP-based operator attach to the EPS network of the PMIP-based operator, they are assigned a GTP-capable GW acting in the role of S-GW. The S-GW selection is carried out by MME or SGSN based on the subscriber's HPLMN. In case of the Serving GW supporting

both GTP and PMIP, the MME/SGSN should indicate the Serving GW which protocol should be used over S5/S8 interface.

Depicted in Figure A.1-1 (b) is an example of "direct peering" interworking between a PMIP-based HPLMN and a GTP-based VPLMN. When roamers whose subscription is owned by the PMIP-based operator attach to the EPS network of the GTP-based operator, they are assigned a GTP-capable S-GW. The information provided by the PMIP-based HPLMN for the P-GW selection function must take into account that the Visited network is GTP-only, in order to return either the IP address (or an APN that can be resolved to an IP address according to the PDN GW resolution mechanism) that points to a GTP-capable PDN GW.

Figure A.1-2 depicts the scenario in which a UE from a GTP-based network roams in a PMIP-based network, local breakout is used, and home-routed bearers are also possible. As with the home-routed case, the MME or SGSN in the PMIP-based VPLMN selects a GTP-capable Serving GW, but it selects a PMIP capable PDN GW. As a result, the S-GW in this example supports both GTP and PMIP based S5/S8. This allows the local breakout bearer and any associated home-routed bearer for the user (e.g. the default bearer) to be served by the same Serving GW. Support of S9 may not be required in all local breakout scenarios.

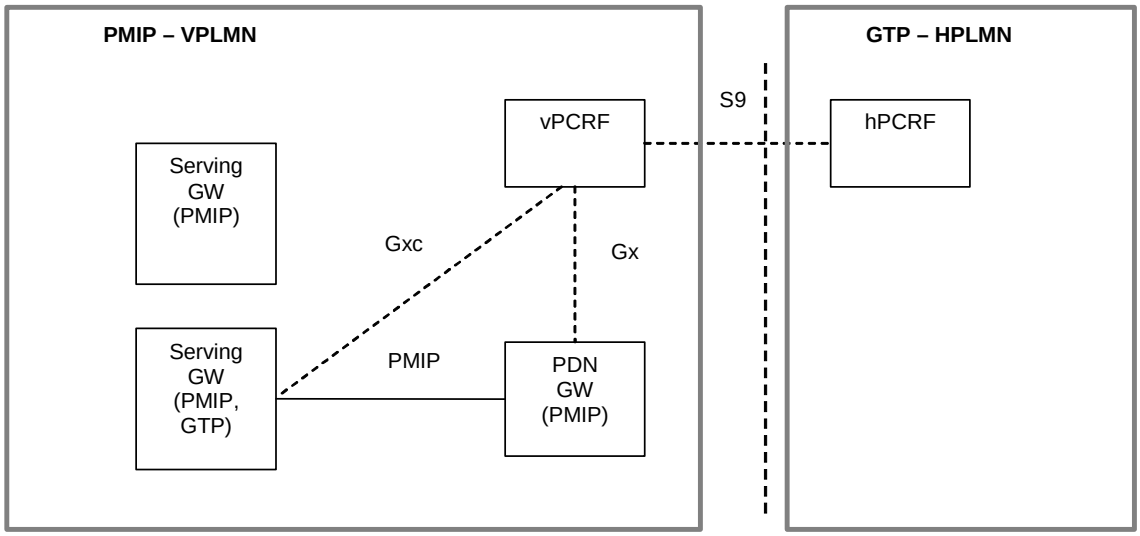


Figure A.1-2: Direct peering example: Local Breakout, UE from GTP HPLMN Roaming in PMIP VPLMN

Figure A.1-3 depicts the scenario in which a UE from a PMIP-based network roams into a GTP-based network and local breakout is used. As with the home-routed case, the MME/SGSN in the GTP-based VPLMN selects a GTP-capable Serving GW and the PDN GW selection function selects a GTP-capable PDN GW. This allows the local breakout bearer and any associated home-routed bearer for the user (e.g., the default bearer) to be served by the same Serving GW. Support of S9 may not be required in all local breakout scenarios.

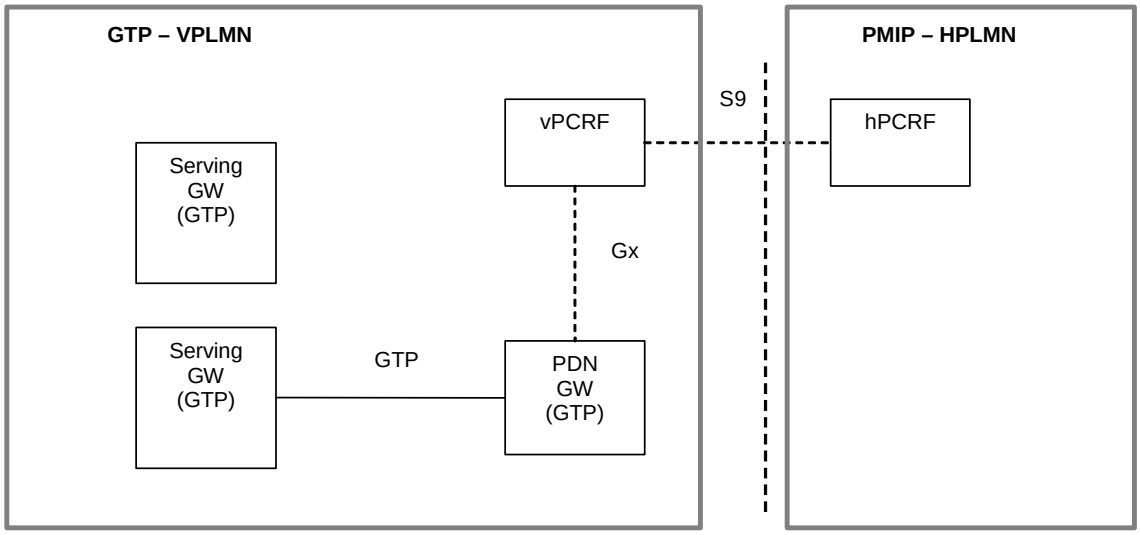
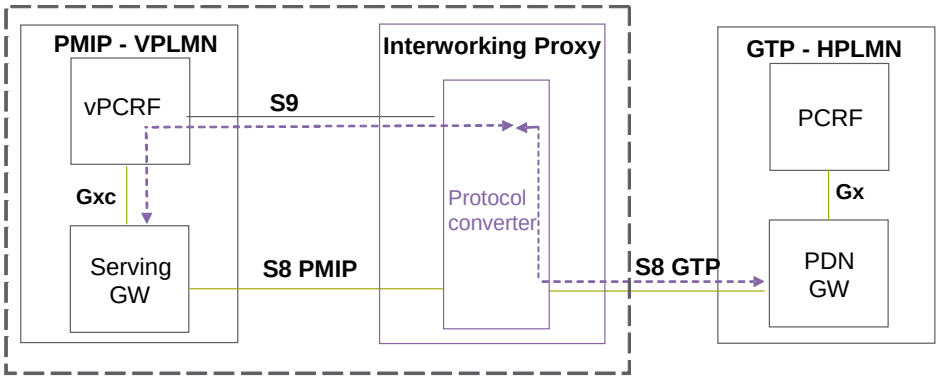


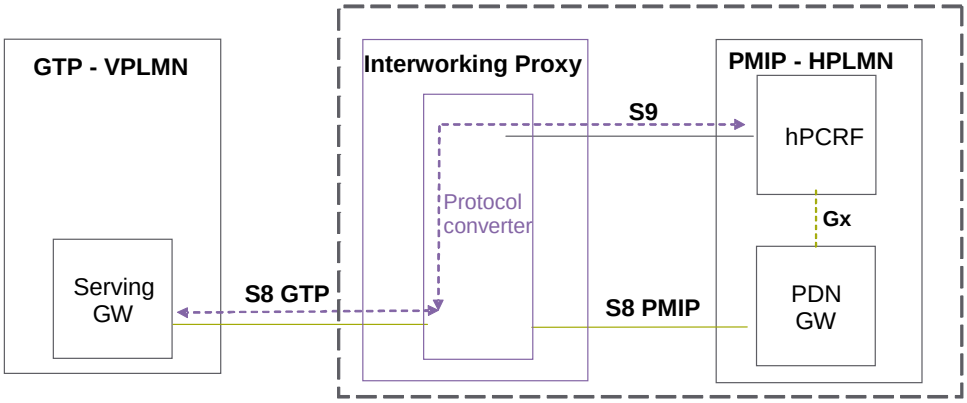
Figure A.1-3: Direct peering example: Local Breakout, UE from PMIP HPLMN Roaming in GTP VPLMN

A.2 Proxy-based interworking

In this scenario an Interworking Proxy (IWP) sits between the GTP-based PLMN and the PMIP-based PLMN to perform protocol conversion between the GTP protocol on one side and the PMIP and Diameter protocols on the other side.



a) GTP HPLMN - PMIP VPLMN



b) PMIP HPLMN - GTP VPLMN

Figure A.2-1: Roaming Via Interworking Proxy: a) GTP-based HPLMN to PMIP-based VPLMN; b) PMIP-based HPLMN to GTP-based VPLMN

The IWP is inserted transparently in the signalling and bearer path i.e. no changes to the GTP, PMIP and Diameter protocols are required.

Annex B (informative): Guidance for Contributors to this Specification

The following guidance is provided for drafting figures for TS 23.402 (this specification) that share some common procedures with TS 23.401 [4].

Representation of PMIP or GTP variants of S5/S8:

- Flows to TS 23.401 [4] will contain the complete procedures for GTP-based S5/S8.

- In TS 23.401 [4], clause(s) of a flow that is different for PMIP version of S5/S8 interface are shown surrounded by shaded box indexed by capital letter in ascending order, e.g. "A", "B", "C", etc.

  At the bottom of the flow, the following text should be included, e.g.

NOTE 1: Procedure steps (A) and (B) for an PMIP-based S5/S8 are defined in TS 23.402 (this specification).

- In TS 23.402 (this specification), each step for the relevant clause, belonging to say annex A, of the flow should be indicated by "A.1, A.2, …" . In TS 23.402 (this specification) common clauses of the flow captured in TS 23.401 [4], should be indicated by shaded boxes with text, e.g. "Procedures in TS 23.401 [4], Figure x.y.z-k, before A", "Procedures in TS 23.401 [4], Figure x.y.z-k, between A and B", etc.

For an illustrative example of the drafting guidelines rule, please refer to Figure 5.4.1-1 in TS 23.401 [4] and corresponding Figure 5.4.1-1-1 in this specification.

Representation of different architectural cases:

- For each case supported, indicate the presence of the optional network entities that may be included in the procedure step. These optional entities appear between the source and destination of the procedure interaction arc as a gray circle. For example, a vPCRF may stand between the Serving GW and the hPCRF.

- In text following a procedure diagram, list the different cases supported by the figure.

- For each case that is supported, indicated what the role of the optional network entity is, when it occurs in the interaction. For example, "In the roaming case, the vPCRF forwards messages between the Serving GW and the PDN GW".

While it is possible to describe these interactions in each step in which they might occur, this will tend to clutter and complicate the procedure diagrams and should be avoided. A single paragraph found beneath each procedure including optional network elements should suffice to clarify that procedure.

Representation of the impact of multiple PDN connectivity:

- In text following a procedure diagram, list the specific impacts arising from multiple PDN connectivity. This will chiefly include a description of which interactions in the figure may be repeated N times for each PDN connected to.

The following guidance is provided for drafting figures related to the S2b interface in TS 23.402 (this specification):

Representation of PMIP or GTP variants of S2b in this specification:

- PMIP-based S2b call flows will contain the complete procedures;

- Clause(s) of a PMIP-based S2b flow that is different for the GTP variant of the S2b interface are shown surrounded by shaded box indexed by capital letter in ascending order, e.g. "A", "B", "C", etc.

  At the bottom of the flow, the following text should be included, e.g.

NOTE 2: Procedure steps (A) and (B) for GTP-based S2b are defined in clause x.

- In GTP based S2b call flows, each step for the relevant clause, belonging to say annex A, of the flow should be indicated by "A.1, A.2, …" . Common clauses of the flow should be indicated by shaded boxes with text

referring to the PMIP based S2b call flow, e.g. "Procedures in Figure x.y.z-k, before A", "Procedures in Figure x.y.z-k, between A and B", etc.

Annex C (informative): Handover Flows Between Non-3GPP Accesses

C.1 General

This clause describes non-exhaustive examples of flows for handover between non-3GPP accesses connected to the EPC. The handover scenarios are based on the mechanisms defined in clause 8 of this document.

C.2 Trusted Non-3GPP IP Access to Trusted Non-3GPP IP Access with DSMIPv6 over S2c Handover

In this scenario, the session starts in (source) trusted non3GPP access using DSMIPv6 over S2c. The session hands over to another (target) trusted non-3GPP access system. The UE subsequently initiates DSMIPv6 with the same PDN GW to maintain the IP session.

In the non-roaming case, none of the optional entities in Figure C.2-1 are involved.

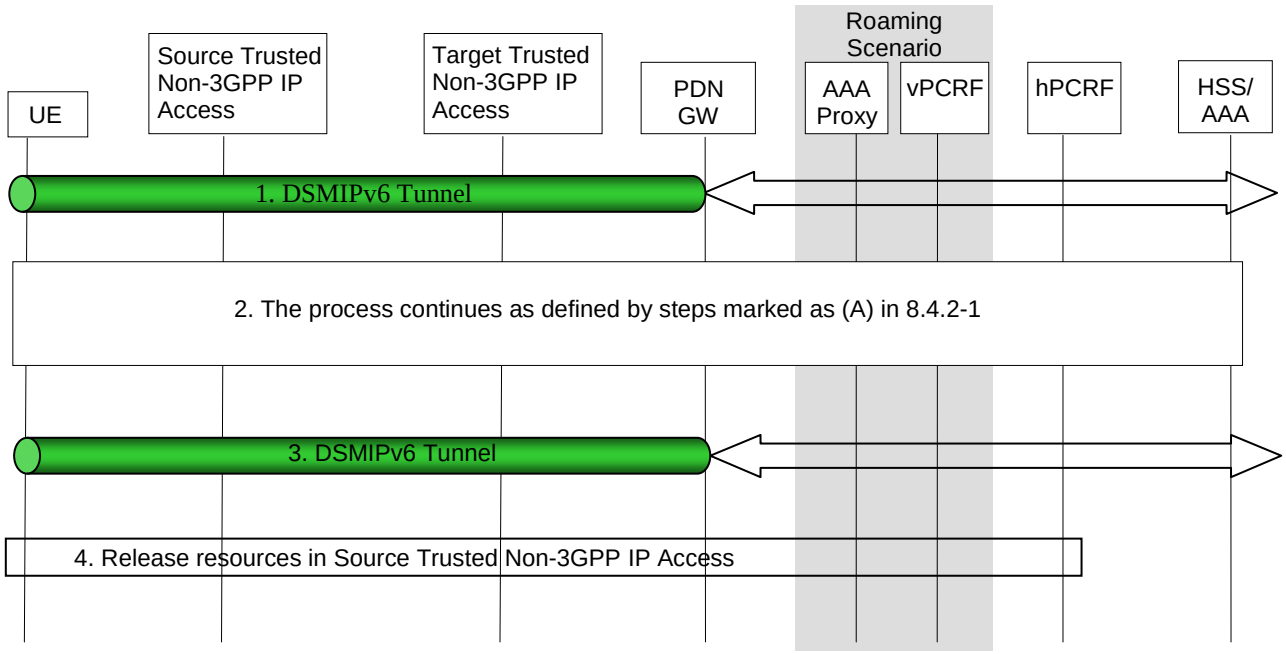


Figure C.2-1: Trusted non-3GPP to Trusted non-3GPP handover based on S2c

1. The UE uses a source Trusted non-3GPP IP access system. It has a local IP address from the non-3GPP system which is used as a care-of address in the DSMIPv6 registration to the PDN GW. The UE maintains a security association with the PDN GW.
2. The UE decides to initiate an access procedure with a new, target Trusted non-3GPP IP access. The procedure continues with the steps defined in Figure 8.6-1 (A)
3. The UE continues the ongoing session(s) via the same PDN GW maintaining the same IP address.
4. Resources in the source Trusted Non-3GPP IP access are released.

C.3 Untrusted Non-3GPP IP Access with PMIPv6 to Trusted Non-3GPP IP Access with PMIPv6 Handover in the Non-Roaming Scenario

This clause shows a call flow for a handover when UE moves from an untrusted non-3GPP IP access network to the trusted non-3GPP access network. PMIPv6 is assumed to be used on S2a and S2b interfaces.

NOTE: The procedure is also applicable to the handover within PMIP-based S2a interfaces or PMIP-based S2b interfaces.

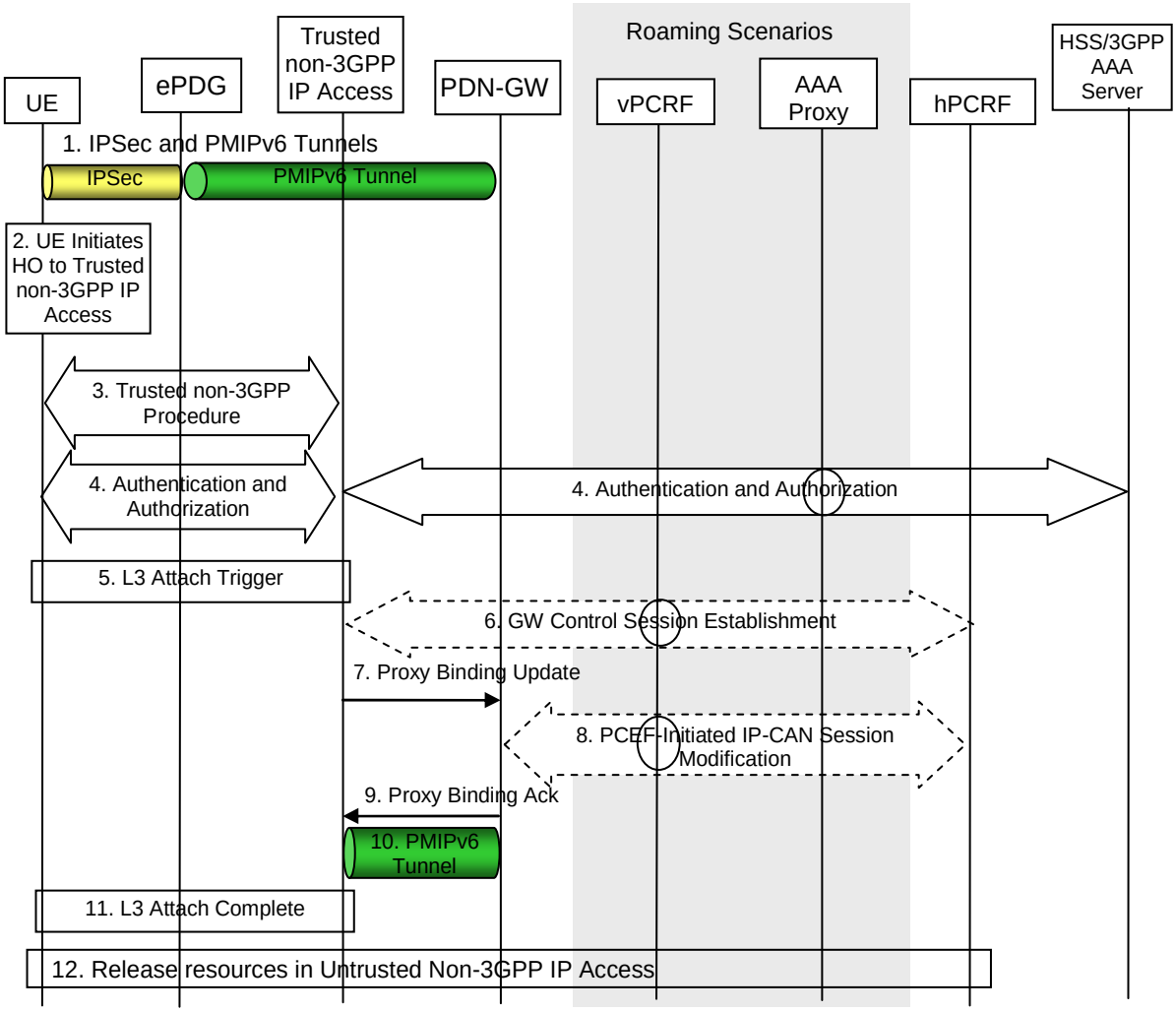


Figure C.3-1: S2b to S2a (PMIPv6) Handover

This procedure supports the non-roaming (Figure 4.2.2.1), home-routed roaming (Figure 4.2.3-1) and roaming with Local breakout (Figure 4.2.3-4) case. The PCRF in the HPLMN is informed of the change of access and any change in the policy that results is signalled to the Trusted non-3GPP IP Access. The signalling takes place through the vPCRF in the VPLMN. In the case of roaming with Local Breakout, the PDN GW in the VPLMN exchanges messages with the vPCRF.

The optional interaction steps between the gateways and the PCRF in the above figure only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateways.

1) The UE is connected to the untrusted Non-3GPP IP Access. There is an IPsec tunnel between the UE and the ePDG and a PMIPv6 tunnel between the ePDG and the PDN GW.

2) The UE moves to a Trusted Non-3GPP IP Access network.

3) The access specific procedures of the Trusted Non-3GPP IP Access are performed. These procedures are outside of the scope of 3GPP.

4) The EAP authentication procedure is initiated and performed involving the UE, Trusted Non-3GPP IP Access and the 3GPP AAA Server. In the roaming case, there may be several AAA proxies involved. As part of the authentication procedure, the information of the selected PDN GW, e.g. PDN GW's address, is conveyed to the MAG in the Trusted Non-3GPP IP Accesses.

5) After successful authentication and authorization, the L3 attach procedure is triggered.

6) The Trusted non-3GPP IP access initiates a Gateway Control Session Establishment Procedure with the PCRF as specified in TS 23.203 [19] to obtain the rules required for the Trusted non-3GPP IP access to perform the bearer binding.

7) The MAG function in the Trusted Non-3GPP IP Access sends Proxy Binding Update message to the PDN GW.

8) The PDN GW executes a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF as specified in TS 23.203 [19] to inform the PCRF of the new IP-CAN type and obtain the updates to the PCC rules.

9) The PDN GW processes the proxy binding update and creates a binding cache entry for the UE. The PDN GW allocates IP address for the UE. The PDN GW then sends a Proxy Binding Acknowledgement to the MAG function in the Trusted Non-3GPP IP Access, including the IP address(s) allocated for the UE. The IP address allocated is same as that was assigned to UE before over the Untrusted Non-3GPP Accesses.

10) The PMIPv6 tunnel is set up between the Trusted Non-3GPP IP Access and the PDN GW.

11) L3 attach procedure is completed. IP connectivity between the UE and the PDN GW is set up for uplink and downlink direction over the trusted non-3GPP IP access.

12) The PDN GW initiates resource allocation deactivation procedure in the untrusted non-3GPP IP access as defined in clause 6.12 or clause 7.9.

C.4 Trusted/Untrusted Non-3GPP IP Access with DSMIPv6 to Trusted Non-3GPP IP Access with PMIPv6 Handover in the Non-Roaming Scenario

This clause shows a call flow for a handover when UE moves from a source trusted/untrusted non-3GPP IP access network to a target trusted non-3GPP access network. PMIPv6 is assumed to be used on S2a and DSMIPv6 is assumed to be used on source trusted/untrusted access network.

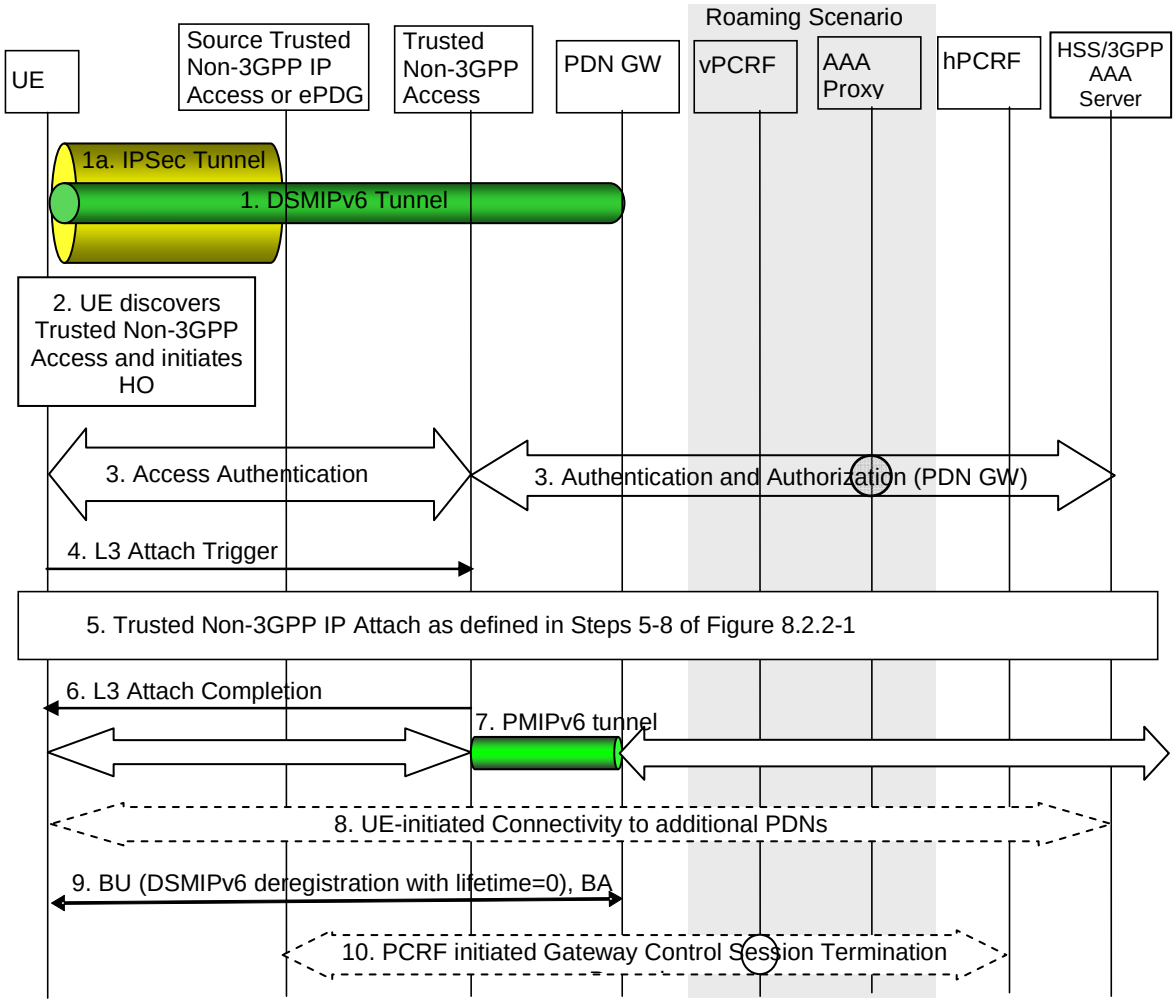


Figure C.4-1: S2c over trusted or untrusted Non-3GPP IP access to S2a (PMIPv6) Handover

This procedure supports the non-roaming (Figure 4.2.2.1), home routed roaming (Figure 4.2.3-1) and roaming with Local breakout (Figure 4.2.3-4) case. The PCRF in the HPLMN is informed of the change of access and any change in the policy that results is signalled to the Trusted non-3GPP IP Access. The signalling takes place through the vPCRF in the VPLMN. In the case of roaming with Local Breakout, the PDN GW in the VPLMN exchanges messages with the vPCRF.

The optional interaction steps between the gateways and the PCRF in the above figure only occur if dynamic policy provisioning is deployed. Otherwise policy may be statically configured with the gateways.

In case of connectivity to multiple PDNs, step 8 is repeated for each PDN the UE is connected to. This step can occur in parallel for each PDN. Other impacts related to the handover for multiple PDNs are described in clause 8.1. Alternatively, if supported by non-3GPP access technology and if the UE does not provide any APN upon handover attach in the trusted non-3GPP IP access, Step 5 is repeated for each PDN the UE is connected to, instead of Step 8. DSMIPv6 de-registration in step 9 will be performed for each PDN connection. These steps can occur in parallel for each PDN.

1. The UE is connected to the trusted/untrusted Non-3GPP Access using S2c.

1a. There is an IPsec tunnel between the UE and the ePDG if UE is connected over untrusted access network.

2. The UE moves to a Trusted Non-3GPP Access network.

3. The EAP authentication procedure is initiated and performed involving the UE, Trusted Non-3GPP IP Access and the 3GPP AAA Server. In the roaming case, there may be several AAA proxies involved. As part of the authentication procedure, the information of the selected PDN GW, e.g. PDN GW's address, is conveyed to the MAG in the Trusted Non-3GPP IP Accesses. The PDNs the UE is connected to are obtained from the HSS with the UE subscriber profile.

4. After successful authentication and authorization, the L3 attach procedure is triggered.
5. The UE continues the attach to the Trusted Non-3GPP IP Access as defined in Steps 5-8 of Figure 8.2.2-1, except that the IP CAN session modification defined in step 7 is triggered as explained below.
6. L3 attach procedure is completed. IP connectivity between the UE and the PDN GW is set for uplink and downlink direction over the trusted non-3GPP IP access.
7. The PMIPv6 tunnel is set up between the Trusted Non-3GPP IP Access and the PDN GW. The UE can send/receive IP packets at this point.
8. In case of connectivity to multiple PDNs, the UE establishes connectivity to all the PDNs besides the Default PDN that the UE was connected to before the handover as described in clause 6.8.1.
9. The UE sends a BU (lifetime) to the PDN GW to de-register its DSMIPv6 binding that was created while the UE was in non-3GPP access system. The PDN GW responds with a BA message.

   Any time after step 5, prior to receiving the de-registration Binding Update from the UE, the PDN GW may de-register the DSMIPv6 binding. In this case the PDN GW shall send a Binding Revocation Indication message to the UE.

   Following the de-registration of the DSMIPv6 binding due to reception of de-registration Binding update or due to triggering Binding Revocation, the PDN GW triggers PCEF initiated IP CAN session modification, instead of doing it as part of the step 5.
10. The PCRF initiates "PCRF-initiated Gateway Control Session Termination" procedure to release the resources in the non-3GPP access. This procedure is triggered by the PCEF-Initiated IP-CAN Session Modification Procedure with the PCRF.

C.5 Handover Between Two Untrusted Non-3GPP IP Accesses Connected to the Same ePDG

This handover case is handled by MOBIKE [18], i.e. the existing IPSec tunnel, via the first untrusted non-3GPP IP access, is only modified for the use with the second untrusted non-3GPP access (and not torn down and re-created from scratch). It is assumed that the MOBIKE support indication has been sent by UE to ePDG in the initial attach.

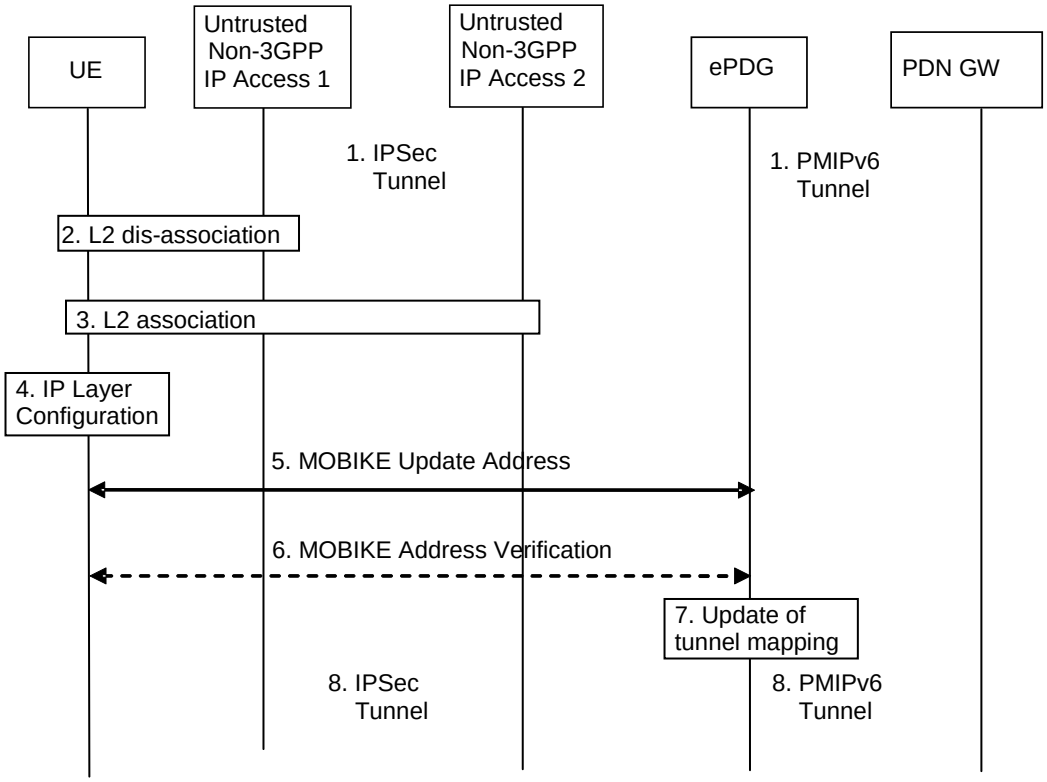


Figure C.5-1: Message flow for handover between two untrusted non-3GPP IP accesses based on MOBIKE

The following steps are performed:

1. The UE is connected via the IPSec tunnel to ePDG, from where a PMIPv6 tunnel is established to the PDN GW. The UE is utilizing a local IP address (for previous IKEv2 signalling and outer IP header address).
2. The UE disconnects on L2 from untrusted non-3GPP IP access 1.
3. UE establishes L2 connectivity to untrusted non-3GPP IP access 2.
4. Configuration of a local IP address. (In case of dual radio multihoming capability with respect to the local IP address is required).
5. MOBIKE update address message exchange (in both directions, initiated by UE).
6. MOBIKE address verification, initiated by ePDG; this step is optional as per MOBIKE [18].
7. The tunnel mapping (between PMIPv6 tunnel and IPSec tunnel) is updated.
8. The modified IPSec tunnel is now in operation.

For dual radio, step 2 is done after step 8.

C.6 Handovers between APs of a Non-3GPP Trusted WLAN Access on S2a

No specific mechanisms are defined to support AP-to-AP handover with and without TWAG relocation. However, this does not preclude the support of IP address preservation in handovers without TWAG relocation when supported by procedures out of 3GPP scope.

Annex D (informative): Void

Annex E (informative): Gateway Relocation in the Trusted Non-3GPP IP Access

Gateway relocation within the Trusted Non-3GPP IP Access is possible using the procedures defined in this clause. The trigger for gateway relocation and any mechanisms for preserving or transferring context between gateways within the Trusted Non-3GPP IP Access is considered out of scope of this specification and should be handled within standards external to 3GPP.

In both the case of PMIPv6 and MIP v4 FACoA on S2a, the Gateway Control Session for the target gateway of the relocation is established before the intra-non-3GPP handover occurs. After the handover, the Gateway Control Session in the source gateway of the handover is terminated.

The mobility management and policy control signalling are both shown as optional messages. This is to allow flexibility depending on the requirements of the trusted non-3GPP IP access system. This allows a policy control signalling relocation (on Gxa) or a relocation of the local mobility anchor (S2a) or both (Gxa and S2a).

E.1 Gateway Relocation with PMIPv6 on S2a

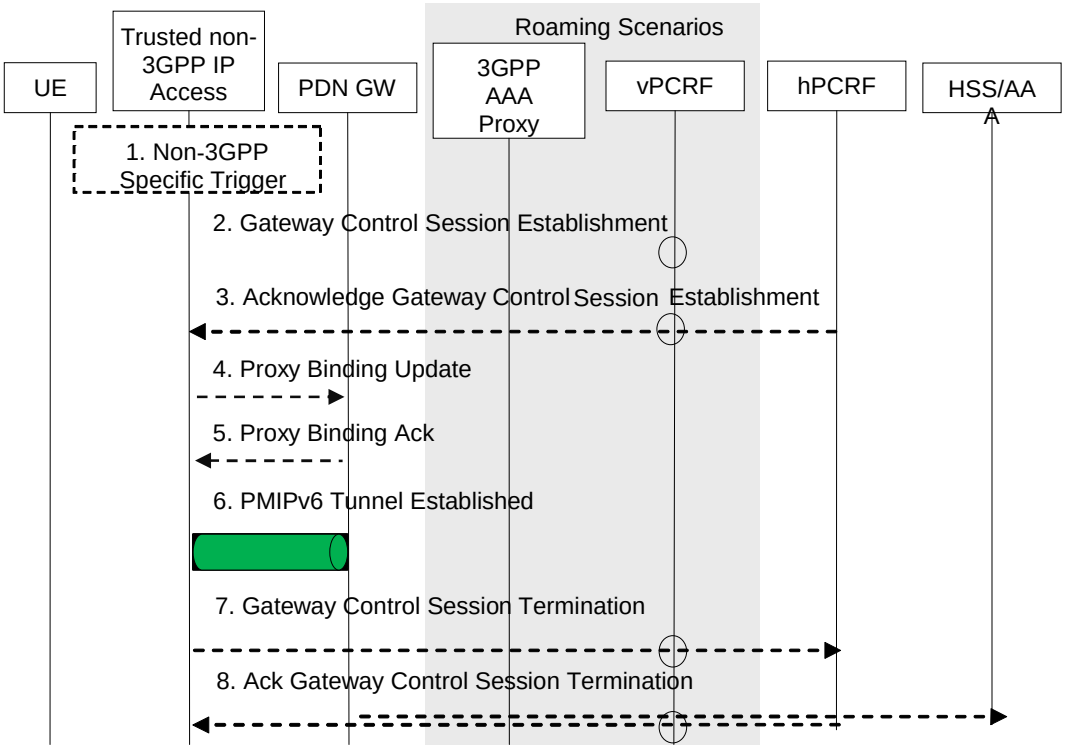


Figure E.1-1: Gateway Relocation when PMIPv6 MM mechanism is used over S2a

When the Gateway Relocation procedure occurs in the Non-Roaming case (Figure 4.2.2-1), the vPCRF is not involved.

In the case of Roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-4), the vPCRF is employed to forward messages from the hPCRF in the home PLMN, by way of the vPCRF in the VPLMN to the non-3GPP access.

1) A gateway relocation is triggered, to be initiated by the Trusted Non-3GPP IP Access. These trigger is outside the scope of 3GPP standardization.

2) The target Gateway in the Trusted Non-3GPP IP Access sends a Gateway Control Session Establishment message to the hPCRF.

3) The PCRF responds to the target Gateway an Ack Gateway Control Session Establishment (QoS Rules, Event Triggers) message. The PCC rules provide the PDN GW with information required to enforce the dedicated bearer policy. The event triggers indicate to the PDN GW when to report an event back to the PCRF related to the dedicated bearer.

4) The target Gateway sends a Proxy Binding Update (MN NAI) message to the PDN GW to register the UE at the PDN-GW. The MN NAI identifies the UE.

5) After creating the binding cache entry for the UE, the PDN GW responds with a Proxy Binding Acknowledgement (MN NAI, Lifetime, UE Address Info) message to the MAG. The MN NAI repeats the UE identity sent previously. The Lifetime expresses the duration of validity of the binding. The UE Address info includes the allocated IP Address(es) corresponding to the IP CAN session.

6) The PMIP tunnel from the target gateway to the PDN GW is established.

7) The source Gateway in the Trusted Non-3GPP IP Access system sends a Gateway Control Session Termination to the PCRF. This gateway ceases to perform Bearer Binding and associated policy controlled functions.

8) The PCRF sends an Acknowledge Gateway Control Session Termination message to the Trusted Non-3GPP IP Access acknowledging the termination of the control session.

E.2 Gateway Relocation with MIPv4 FACoA on S2a

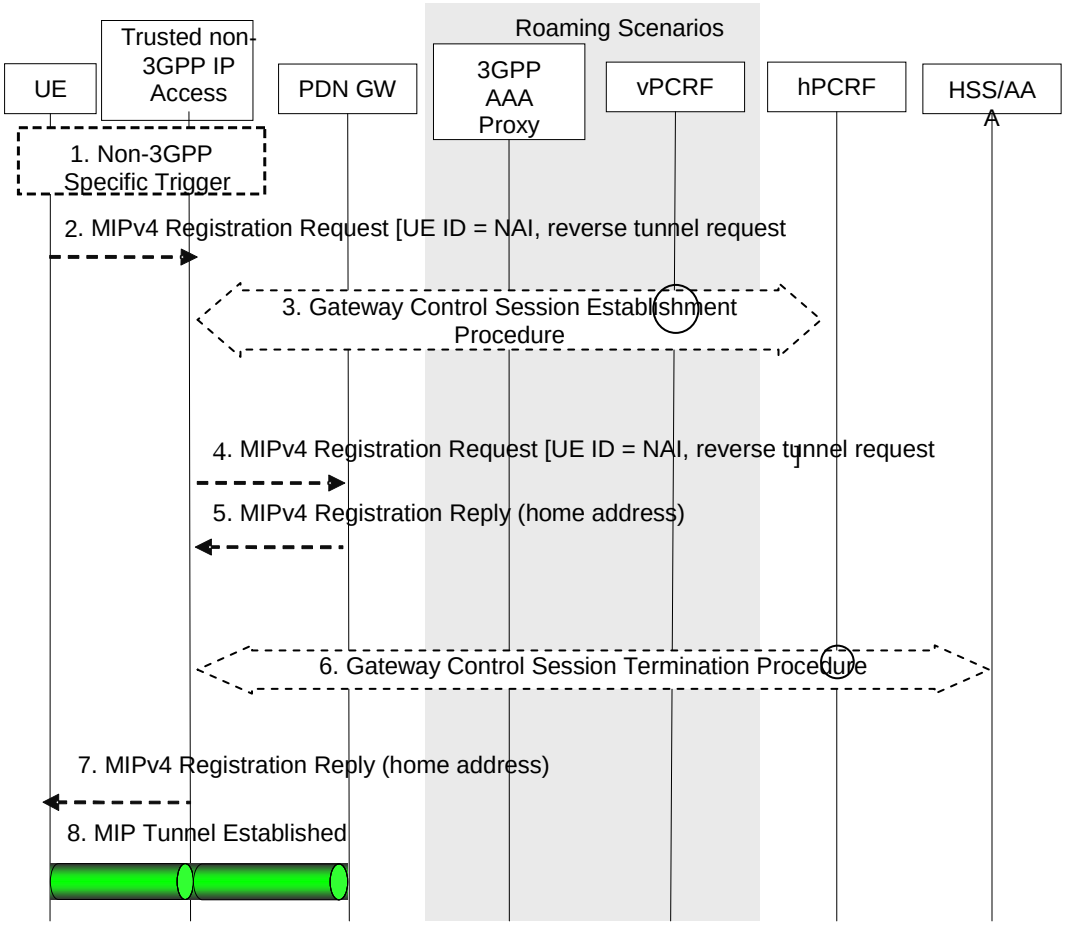


Figure E.2-1: Gateway Relocation when MIPv4 FACoA mode MM mechanism is used over S2a

When the Gateway Relocation procedure occurs in the Non-Roaming case (Figure 4.2.2-1), the vPCRF is not involved.

In the case of Roaming (Figure 4.2.3-1) and Local Breakout (Figure 4.2.3-4), the vPCRF is employed to forward messages from the hPCRF in the home PLMN, by way of the vPCRF in the VPLMN to the non-3GPP access.

1) A gateway relocation is triggered, to be initiated by the UE. This trigger is outside the scope of 3GPP standardization.

2) The UE sends a Registration Request (RRQ) RFC 5944 [12] message to the FA. Reverse Tunnelling shall be requested. This ensures that all traffic will go through the PDN GW. The RRQ message shall include the NAI-Extension RFC 2794 [34] and the Home Agent Address.

3) The Trusted non-3GPP access initiates the Gateway Control Session Establishment Procedure with the PCRF, as specified in TS 23.203 [19]. The Trusted non-3GPP access provides the information to the PCRF to correctly associate it with the IP CAN session to be established in Step 9 and also to convey subscription related parameters to the PCRF.

4) The FA processes the message according to RFC 5944 [12] and forwards a corresponding RRQ message to the PDN GW.

5) The PDN GW allocates an IP address for the UE and sends a Registration Reply (RRP) RFC 5944 [12] to the FA, including the IP address allocated for the UE.

6) The Trusted Non-3GPP Access Network initiates the Gateway Control Session Termination Procedure with the PCRF as specified in TS 23.203 [19]. The Trusted Non-3GPP Access Network no longer applies QoS policy to service data flows for this UE.

7) The FA processes the RRP according to RFC 5944 [12] and sends a corresponding RRP message to the UE.

8) IP connectivity from the UE to the PDN GW is now setup. A MIP tunnel is established between the FA in the Trusted Non-3GPP IP Access and the PDN GW.

Annex F (informative): Deployment of Non-3GPP Trusted WLAN Access on S2a

WLAN networks may be deployed such that separate SSIDs are used for EPC-routed and non-seamless WLAN offload, e.g. <ssid_a> and <ssid_b>.

WLAN networks may also be deployed such that the same SSID in a WLAN Access Point provides different type of network access to different users attached to this Access Point. For example, a given SSID <ssid_x> may provide EPC-routed access for subscriber A and only allow non-seamless WLAN offload for subscriber B. In such a deployment it is up to the operator to provide network configuration that supports different user access preferences, subscriptions and UE configurations.

It is recommended that the UE can be configured to apply different behavior when connected to different SSIDs, e.g. allow or prevent the usage of certain applications on specific SSIDs. For example, for the SSIDs used for EPC access through S2a over Trusted WLAN, the UE can be configured to disable applications that require local connectivity (e.g. DLNA applications) and enable applications that require EPC connectivity to the default APN used for access through S2a over Trusted WLAN. Such kind of special behavior for SSIDs used for EPC access through S2a over Trusted WLAN can improve the user experience and prolong the UE battery life.

NOTE: A UE can be configured to apply different behavior when connected to different SSIDs by means which are outside the scope of this document. For example, the UE can be configured over-the-air, by means of a downloadable application, or manually.

Annex G (informative): Change History

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**
2014-12	SP-66	SP-140693	1329	2	B	TWAN release cause for Trusted WLAN	12.7.0	**13.0.0**
2015-03	SP-67	SP-150027	1339	1	B	GTP-C overload control from TWAN/ePDG to PGW	13.0.0	13.1.0
2015-03	SP-67	SP-150020	1342	1	A	SPExclusionList in WLANSP	13.0.0	13.1.0
2015-03	SP-67	SP-150027	1343	2	B	Support prefix delegation in PMIP-based S5/S8	13.0.0	13.1.0
2015-03	SP-67	SP-150027	1344	2	F	PMIP Prefix Delegation reference correction	13.0.0	13.1.0
2015-03	SP-67	SP-150016	1346	1	A	Adding description of missing S2a system architecture alternative	13.0.0	13.1.0
2015-03	SP-67	SP-150027	1355	1	F	Removing incorrect references to I-WLAN specifications	13.0.0	13.1.0
2015-03	SP-67	SP-150020	1356	-	A	Prioritized PreferredSSIDList	13.0.0	13.1.0
2015-06	SP-68	SP-150239	1360	1	F	Clarification of Impacts when Gxx is not used for eHRPD Access	13.1.0	13.2.0
2015-06	SP-68	SP-150239	1366	2	F	Session/bearer release cause over S2b	13.1.0	13.2.0
2015-09	SP-69	SP-150503	1368	3	**B**	ePDG selection for emergency bearer services	13.2.0	13.3.0
2015-09	SP-69	SP-150503	1380	2	**B**	Introduction of the Support of Emergency services over WLAN access to EPC	13.2.0	13.3.0
2015-09	SP-69	SP-150505	1376	4	**C**	Revision of ePDG selection procedures	13.2.0	13.3.0
2015-12	SP-70	SP-150613	1391	2	**F**	Corrections to ePDG selection	13.3.0	13.4.0
2015-12	SP-70	SP-150613	2902	-	**F**	Correction to handover between ePDGs	13.3.0	13.4.0
2015-12	SP-70	SP-150613	2906	5	**F**	Supporting Location reporting for IMS sessions over S2b.	13.3.0	13.4.0
2015-12	SP-70	SP-150602	2908	1	**A**	Clarification of S2a architecture	13.3.0	13.4.0
2015-12	SP-70	SP-150617	2909	1	**F**	Conveying to the EPC the IMEI of devices accessing a trusted or untrusted WLAN	13.3.0	13.4.0
2015-12	SP-70	SP-150613	2910	2	**F**	Transfer of User Location Information at Create Session Request over S2b	13.3.0	13.4.0
2015-12	SP-70	SP-150613	2912	2	**F**	ePDG supporting emergency services only	13.3.0	13.4.0
2015-12	SP-70	SP-150613	2916	4	**F**	Keeping WLAN Location Information up to date	13.3.0	13.4.0
2015-12	SP-70	SP-150615	2917	2	**B**	Addition of LWA support	13.3.0	13.4.0
2015-12	SP-70	SP-150615	2918	2	**B**	Addition of CRLWI support	13.3.0	13.4.0
2015-12	SP-70	SP-150615	2920	4	**C**	Corrections to ePDG selection procedure	13.3.0	13.4.0
2015-12	SP-70	SP-150615	2921	1	**F**	Clarifications on the ePDG Delete Session procedure	13.3.0	13.4.0
2016-03	SP-71	SP-160162	2922	4	**F**	Clarification on ANDSF precedence	13.4.0	13.5.0
2016-03	SP-71	SP-160160	2925	1	**F**	Correction to ePDG selection for emergency bearer services	13.4.0	13.5.0
2016-03	SP-71	SP-160160	2926	-	**F**	Sending an Emergency-Indication to the 3GPP AAA Server over S6b	13.4.0	13.5.0
2016-03	SP-71	SP-160162	2933	3	**C**	Updated ePDG Selection Procedure	13.4.0	13.5.0
2016-03	SP-71	SP-160162	2934	3	**F**	Coexistence between ANDSF and LWA	13.4.0	13.5.0
2016-06	SP-72	SP-160285	2928	2	**A**	Clarification on TWAN authorization	13.5.0	13.6.0
2016-06	SP-72	SP-160298	2941	1	**F**	Correction of UICC precedence	13.5.0	13.6.0
2016-06	SP-72	SP-160298	2942	2	**F**	Corrections for ePDG selection fallback	13.5.0	13.6.0
2016-06	SP-72	SP-160298	2943	1	**F**	Corrections to ePDG selection procedure for UE determined location	13.5.0	13.6.0

History

Document history		
V13.4.0	March 2016	Publication
V13.5.0	April 2016	Publication
V13.6.0	July 2016	Publication